ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

I PROMOCIÓN

TESIS DE GRADO

"ANÁLISIS, DISEÑO Y EVALUACIÓN DE UNA PROPUESTA TECNOLÓGICA QUE MITIGUE EL ACCESO A PÁGINAS WEB CON CONTENIDO INAPROPIADO"

AUTORES:

ING. TANIA KARINA QUIMBIULCO SOSAPANTA

ING. ERNESTO GERMAN SANGUANO CAIZALUISA

DIRECTOR:

ING. WALTER MARCELO FUERTES PH.D.

SANGOLQUÍ, FEBRERO 2015

CERTIFICACIÓN

Se certifica que el presente trabajo titulado "ANÁLISIS, DISEÑO Y EVALUACIÓN DE UNA PROPUESTA TECNOLÓGICA QUE MITIGUE EL ACCESO A PÁGINAS WEB CON CONTENIDO INAPROPIADO" realizado por los Ing(s). Tania Karina Quimbiulco Sosapanta y Ernesto German Sanguano, ha sido guiado y revisado periódicamente, orientando sus conocimientos y competencias para un eficiente desarrollo del tema y cumple normas estatutarias establecidas por la ESPE, en el reglamento de estudiantes de la Universidad de las Fuerzas Armadas ESPE.

Sangolqui, Febrero de 2015

Ing. Walter Marcelo Fuertes PH.D.
DIRECTOR DE TESIS

Ing. Fernando Galarraga MSc
OPONENTE DE TESIS

DECLARACIÓN DE RESPONSABILIDAD

Nosotros: Ing. Tania Karina Quimbiulco Sosapanta

Ing. Ernesto German Sanguano Caizaluisa

DECLARAMOS QUE:

El proyecto de maestría titulado **"ANÁLISIS, DISEÑO Y EVALUACIÓN DE UNA PROPUESTA TECNOLÓGICA QUE MITIGUE EL ACCESO A PÁGINAS WEB CON CONTENIDO INAPROPIADO."**, ha sido desarrollada metodológicamente respetando los derechos intelectuales cuyas fuentes se presentan en la bibliografía.

En virtud de lo anteriormente expuesto nos responsabilizamos del contenido veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Febrero 2015

Ing. Tania Karina Quimbiulco S.

Ing. Ernesto German Sanguano C.

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros: Ing. Tania Karina Quimbiulco Sosapanta

Ing. Ernesto German Sanguano Caizaluisa

Autorizamos a la universidad de las Fuerzas Armadas ESPE la publicación en la biblioteca virtual de la Institución, el trabajo **"ANÁLISIS, DISEÑO Y EVALUACIÓN DE UNA PROPUESTA TECNOLÓGICA QUE MITIGUE EL ACCESO A PÁGINAS WEB CON CONTENIDO INAPROPIADO."**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría, excepto las publicaciones en congresos o revistas nacionales e internacionales relacionadas a esta investigación.

Sangolquí, Febrero 2015

Ing. Tania Karina Quimbiulco S.

Ing. Ernesto German Sanguano C.

DEDICATORIA

Al ser supremo Dios que en todo momento se encuentra a mi lado, guiándome, cuidándome y permitiéndome seguir adelante en compañía de mi familia.

A mis padres que en todo momento se han encontrado a mi lado brindarme su amor, comprensión y enseñarme a luchar por alcanzar los sueños, hoy en día soy lo que soy gracias a ellos.

A mi hermanita por su incondicional apoyo, compañía y locuras que hacía más llevadera la realización del presente proyecto de tesis.

Tania Karina Quimbiulco S.

El presente trabajo lo dedico a Dios, por darme la vida por medio de mis queridos PADRES quienes con cariño, amor y ejemplo de vida han hecho de mí una persona de bien, a mi ESPOSA la que con mucho amor, apoyo incondicional y confianza permitieron continuar y a mis HIJOS Dieguito y Sofita que son la razón y el motivo para superarme

A todos que me animaron para culminar con éxito una etapa más en mi vida; además dejar una enseñanza que cuando se quiere alcanzar algo en la vida, no hay tiempo ni obstáculo que lo impida lograrlo.

Ernesto German Sanguano C.

AGRADECIMIENTOS

A Dios por sus bendiciones, brindándome salud y vida para culminar este proceso.

A mis padres, hermanita y amigos que de una u otra manera me ayudaron a seguir adelante y no decaer ante las adversidades presentadas.

A nuestro Director de Tesis Ing. Walter Fuertes Ph.D, un especial agradecimiento por su valiosa guía, conocimientos, exigencia y ánimos en seguir adelante.

Tania Karina Quimbiulco S.

Quiero darle gracias a mi ESPOSA, PADRES y SUEGRO por el apoyo brindado; y a mi compañera de tesis Karina por haber apoyado y colaborado en cada momento del desarrollo de la tesis que no pude estar presente por mi situación de trabajo.

A mi estimado Maestro Ing. Walter Fuertes, por la paciencia y la entrega de sus conocimientos y a mi querida Universidad de las Fuerzas Armadas ESPE; todos han contribuido para poder culminar con éxito.

Ernesto German Sanguano C.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Ante el acelerado progreso de la tecnología, las comunicaciones y la falta de control de acceso a Internet en áreas como hogares y colegios, se identificó la necesidad de realizar el presente trabajo de investigación. Se realizaron encuestas a adolescentes, padres de familia y administradores de redes en donde se logra identificar que el porcentaje de control de acceso a Internet es mínimo. A partir de esta premisa se realiza un estudio de la situación actual sobre herramientas de Control Parental, evaluando diferentes herramientas de software tomando en cuenta las características de: funcionalidad, eficiencia, usabilidad, seguridad, y costos de licencias, las cuales demostraron que no todas cumplen con lo requerido. Se determinó una línea base obteniendo requisitos donde se consideran las características principales para desarrollar una aplicación Web. Se diseñó e implementó un mecanismo para el Control Parental, en el que mitiga el riesgo y además se registra todos los accesos efectuados por menores a través del Internet. Se utilizó la metodología de desarrollo OOHDM, integrando Procesamiento de Lenguaje Natural, con la técnica de Recuperación Booleana utilizando algoritmos de búsqueda Boyer-Moore y búsqueda aproximada. Finalmente se procedió a instalar la aplicación en varios lugares, dentro de los primeros quince días se registraron todas las visitas realizadas en Internet, posteriormente se activan las páginas Web y palabras que se deben bloquear por considerarse inadecuadas para los menores. Con la información recopilada se identificó que efectivamente una herramienta de Control Parental reduce el riesgo de acceder a sitios Web con contenido inapropiado.

PALABRAS CLAVE: CONTROL PARENTAL, INTERNET, OOHDM, PROCESAMIENTO DE LENGUAJE NATURAL.

ABSTRACT

Given the fast progress of technology, communications and lack of control over access to the Internet in places such as homes, schools and public areas, it was identified the necessity to develop this research. Surveys to teens, parents and network managers were conducted where it was possible to detect the percentage of Internet access control and it was revealed to be minimal. Following this premise a study over the situation of Parental Control Tools was developed, evaluating different software tools taking into account characteristics such as: functionality, efficiency, usability, security and costs for the use of licenses which have demonstrated that not all of them fulfill all the requirements. In order to obtain the requirements for the main characteristic to develop a web application a baseline was determined. A mechanism for Parental Control was designed and implemented, which mitigates the risk as well as records all the access made by teen through the Internet. OOHDM development methodology was used, integrating the Natural Language Processing, specifically the Boolean Retrieval Model using the Boyer-Moore research algorithms and fuzzy search filter. Finally the application is installed in several places and within the first fifteen days all Internet visits were recorded, subsequently web pages and words that were activated and considered inappropriate for under ages are blocked. With the compiled information it was identified that a tool for Parental Control reduces the risk of accessing web sites with unsuitable content effectively.

KEY WORDS: PARENTAL CONTROL, INTERNET, OOHDM, NATURAL LANGUAGE PROCESSING.

CAPÍTULO I. INTRODUCCIÓN

El avance de la tecnología, la expansión y el acceso a Internet desde cualquier lugar, ha permitido que la sociedad tenga acceso a información de interés en distintos ámbitos como: la educación, investigación, entretenimiento, establecer lazos sociales y realizar varias actividades de comunicación en línea. En la actualidad todas las personas especialmente las nuevas generaciones corren el riesgo de acceder a información con contenido inapropiado como: pornografía, violencia explícita, terrorismo, además puede provocar dependencia o vicio a la moda actual como las redes sociales (Parrini, 2012).

Los peligros que representa el acceso al Internet por parte de niños y adolescentes a nivel mundial ha provocado que empresas y organizaciones establezcan; leyes, políticas, normas y procedimientos, que regulen y controlan el mal uso del Internet, campañas publicitarias en contra del grooming, bullying, pornografía, etc., además el análisis de herramientas tecnológicas que se encuentran disponibles en el mercado, las cuales permitan monitorear y controlar el uso de Internet.

Los escenarios con más riesgo por la falta de control de acceso a páginas Web con contenido inapropiado, son hogares, colegios y servicios públicos de Internet. Este contenido es un tema que no ha sido difundido en el país, ya sea por falta de conocimientos, recursos económicos o concienciación por parte de las personas encargadas en proveer el servicio de Internet, las autoridades de los colegios, y las personas responsables dentro de los hogares.

Con la presente investigación se evalúa diferentes herramientas que controlan el acceso a la navegación y además se identifican cuáles son las técnicas o medidas de control implementadas en colegios hogares y servicios públicos de Internet: verificando cual es el uso que se da al Internet por parte de los niños y adolescentes. Todo esto con el fin de proponer un mecanismo que mitigue el acceso a páginas Web que contengan contenido inapropiado.

La población objetivo para la investigación fueron los colegios públicos y privados que permitió abarcar extractos diferentes de población, estas instituciones se encuentran ubicadas en el Valle de los Chillos.

1.1 Justificación e Importancia

Dentro del país no se han tomado las medidas de control para el filtrado de información en los lugares más vulnerables como son: hogares, colegios y sitios públicos de Internet, de esta manera se ha permitido que todas las personas sin importar su edad accedan a páginas Web que puedan contener información inadecuada afectando principalmente a los más jóvenes.

Los riesgos a los que se exponen los adolescentes pueden ser mitigados por parte de los padres y docentes con herramientas de filtrado de información fáciles de instalar y monitorear, en la actualidad existen este tipo de aplicaciones que son gratuitos y pagados.

1.2 Planteamiento del problema

En los hogares, colegios y servicios públicos de Internet, en el Valle de los Chillos no se cuenta con herramientas informáticas adecuadas para el correcto control de acceso a sitios Web, que deberían ser restringidos para menores por su contenido inapropiado, el cual va provocando que los adolescentes puedan volverse adictos al acceso desenfrenado al Internet permitiendo que caigan en aislamiento social, depresión, ansiedad, u otros.

1.3 Formulación del problema

La presente investigación se enmarca en la problemática existente sobre las amenazas que se encuentran en la Web, al ser los niños y adolescentes las personas más vulnerables a peligros mientras navegan en Internet, ante estos acontecimientos surgen las siguientes interrogantes:

- ¿Cuáles son las herramientas informáticas para la instalación, administración y adquisición, en el control del acceso a información inapropiada?
- ¿Cuál es la factibilidad de aplicar herramientas para controlar el acceso páginas Web con contenido inapropiado?

- ¿Qué medidas pueden tomarse para eliminar o mitigar el impacto del uso inadecuado del Internet por parte de los adolescentes?
- ¿Cuáles son las métricas para medir el acceso a páginas con información no apropiada?

Para responder estas interrogantes se realiza la investigación en niños y adolescentes que tiene las edades de 11 a 17 años, evaluando como es el uso de Internet y su seguridad en lugares como son hogares, colegios.

1.4 Hipótesis

La aplicación de herramientas de filtrado de contenido Web disminuye significativamente el acceso a páginas con información no apropiada.

1.5 Objetivo general

Diseñar e implementar un mecanismo aplicando Procesamiento de Lenguaje Natural (PLN) que mitigue el acceso a páginas Web con contenido inapropiado, mediante la evaluación cuantitativa de herramientas que la controlen.

1.6 Objetivos específicos

- Analizar el marco teórico referencial y el estado del arte de la problemática existente.
- Definir y evaluar las herramientas informáticas de filtrado de contenido para realizar el análisis con relación a las vulnerabilidades que presentan en el control al acceso de información no adecuada.
- Diseñar e implementar un mecanismo para mitigar el acceso páginas Web que contengan contenido inapropiado.
- Verificar, evaluar y validar los resultados estadísticos.

CAPÍTULO II. MARCO TEÓRICO REFERENCIAL

2.1 Introducción

Este capítulo presenta una síntesis sobre el Estado del Arte que sustenta la presente investigación. Se inicia indicando cual es el diagnóstico situacional de acuerdo a encuestas internacionales y datos estadísticos presentados por el Instituto Nacional de Estadísticas y Censos a nivel nacional (véase la sección 2.2). Continúa con el estudio de las herramientas de control de acceso a Internet, que han sido reconocidas a nivel internacional por sus características (véase la sección 2.3). Seguidamente se presenta el marco teórico y la definición operacional que se encuentra basada en la presente investigación (véase la sección 2.4 y 2.5).

2.2 Diagnóstico Situacional

La Fundación Pfizer como aporte a la comunidad, realizó encuestas y análisis sobre los hábitos, usos y comportamientos frente al Internet por parte de los adolescentes en Madrid España, tomando como muestra a mil (1000) jóvenes. Adicionalmente fueron entrevistados los padres y docentes de los jóvenes encuestados, para conocer cuáles son las medidas de seguridad implementadas en casa o instituciones educativas. El informe presenta una visión completa y detallada, partiendo de que en la disponibilidad de internet en los hogares es de un 87.3%, del cual el 73% es utilizado por los jóvenes (Pfizer, 2009).

En Ecuador los datos estadísticos de TIC, realizados por el INSTITUTO NACIONAL DE ESTÁDISTICA Y CENSOS (INEC), en 21.768 viviendas, 579 centros poblados urbanos y rurales obteniendo los resultados siguientes: ((INEC), 2011).

- El 24,7 % de los hogares tienen computadores de escritorio y el 9.8 % de los hogares tienen computadores portátiles.
- El 31,4% de la población de Ecuador ha utilizado Internet en los últimos 12 meses.
- El 32% de los hombres en los últimos 12 meses ha usado Internet frente al 30,8% de las mujeres.

- El grupo etario con mayor uso de Internet es la población que se encuentra entre 16 y 24 años con el 59,4%, seguido de las personas de 25 a 34 años con el 39,6%. Los que menos utilizan son las personas de 65 a 74 años con el 3,3%.
- En los últimos 12 meses se ha incrementado en el número de personas que han usado internet en el quintil 1 pasando del 13,2% en diciembre 2010 a 15,5% en diciembre 2011.
- La provincia con mayor número de personas que utiliza Internet es Pichincha con 44,5%, seguida de Azuay con 36,9%, la que menos tiene es Santa Elena con 18,8%.
- El 38,3% de la población lo usa en el hogar, seguido del 22,0% que lo usó en las instituciones públicas.
- El 32,6% de la población utiliza Internet para comunicarse, seguido del 31,1% que la utiliza para obtener información.

2.3 Herramientas de control de acceso a Internet

Debido al crecimiento de la tecnología y el acceso libre al Internet, la cual no es controlada adecuadamente por las entidades que facilitan este servicio, la Sociedad de Información Europea (Europes's Information Society), realizó una evaluación comparativa de las herramientas para la protección en línea de los niños y adolescentes, con el objetivo de ayudar a los padres en elegir la herramienta de control en el acceso a Internet adecuada,

"Self-regulation is one of the instruments of the European Strategy to create a better Internet for Children.

They way children use the Internet and mobile technologies has changed dramatically in the past years. At the same time, the Internet can open a wide range of opportunities for youngsters when used safely and responsibly. In order to ensure that children, parents and teachers have access to the right tools and information for a safe use of the Internet and new technologies, we support industry self-regulation.

Some self-regulatory initiatives have already been taken, with our support, by the industry at European level."(Society, 2009).

2.4 Marco conceptual

En la figura 1 muestra en capas los elementos teóricos que apalancan esta investigación, ha sido divido en base a los ambientes por el cual atraviesan los mecanismos de Control Parental.

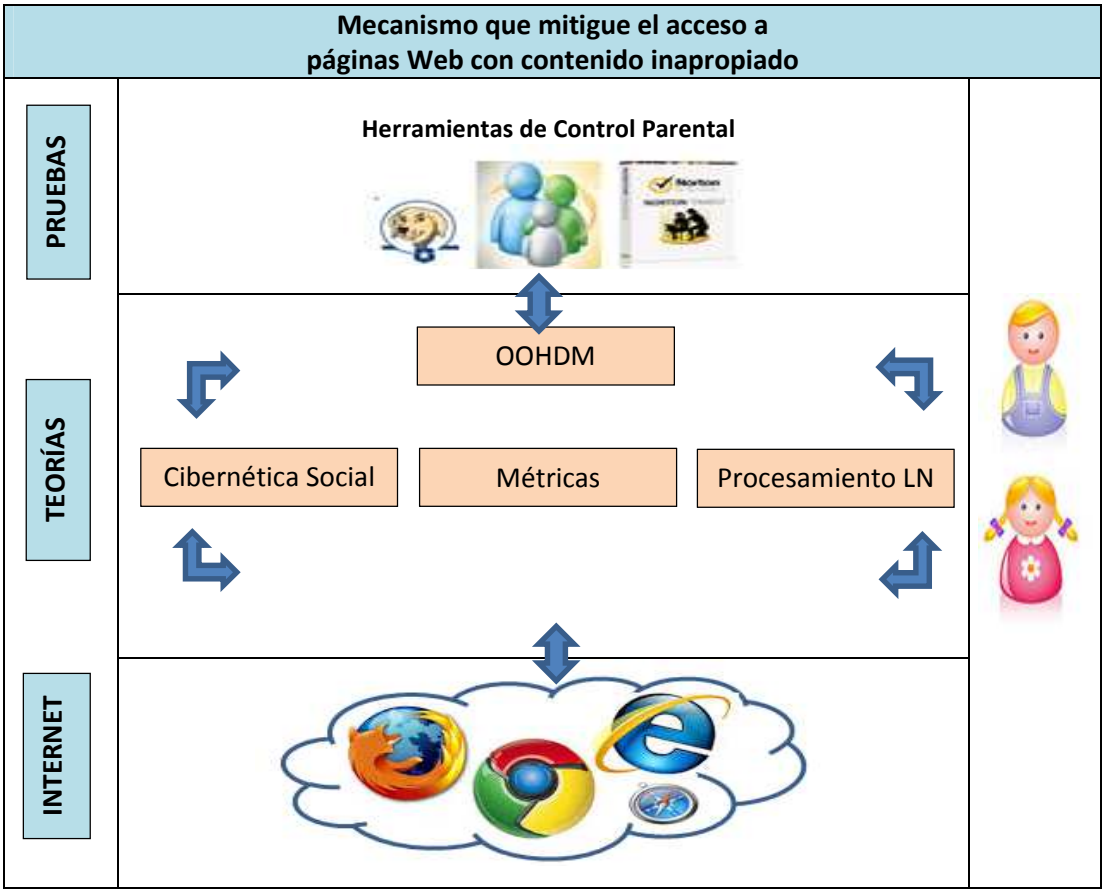


Figura 1. Estructura de Investigación de Control de Acceso a Internet
Fuente: Ilustración Propia

2.4.1 Cibernética Social

Es una teoría interdisciplinaria que integra las ciencias sociales y humanas en un solo bloque, tiene como objetivo estudiar a la persona quien está directamente ligada a los sistemas. También se le puede denominar Cibernética de segundo orden, que ha sido el análisis de las redes sociales y de los adolescentes que hacen uso constante de estas herramientas (Velandia Mora, 2005, pág. 14)

Se puede señalar que la Cibernética social es un método práctico que abarca las ciencias humanas y sociales en su totalidad, manejando una visión sistémica y triádica donde la sociedad es movida en tres partes y tres fuerzas dando lugar a los juegos triádicos, estos juegos están representados por tres sub-grupos direccionados por:

- La Inteligencia Racional que abarca. Método Científico, Método Cualitativo y Método Administrativo.
- La Inteligencia Emocional utiliza: Método Creativo, Trabaja Mediante Imágenes y tiene Visión del Futuro.
- Inteligencia Operacional del Cerebro que mantiene activo: La Planificación, La Gestión, La Supervisión y El Feedback.

Dentro de este enfoque los juegos triádicos energéticamente presentan una red por canales de Input (Necesidades, Insumos Consumos y Demandas) y de un Output (Satisfacción, Vienes y Productos). A raíz de esta energía el hombre presenta diferentes tipos de visión:

- Unítriádicas: que lo abarca todo.
- Monádica: que mira un solo lado.
- Diática: que mira dos lados, con visión de competencia.
- Feedback, que tiene como funcionalidad la retroalimentación de un proceso que tiene la capacidad de influir en el aprendizaje, sin embargo el simple hecho de entregar un resultado no conduce necesariamente a una mejora.

2.4.2 Métricas

El desarrollo de las tecnologías de la información y las comunicaciones ofrece nuevos escenarios para la realización de los estudios métricos de la información, sobre todo de aquella que circula por Internet. La Cibermetría se presenta como la disciplina dedicada a la descripción cuantitativa de los contenidos y procesos de comunicación que se producen en el ciberespacio, La

figura 2 describe sus componentes y la interrelación entre ellos. (MsC. Martínez Rodriguez, 2006).

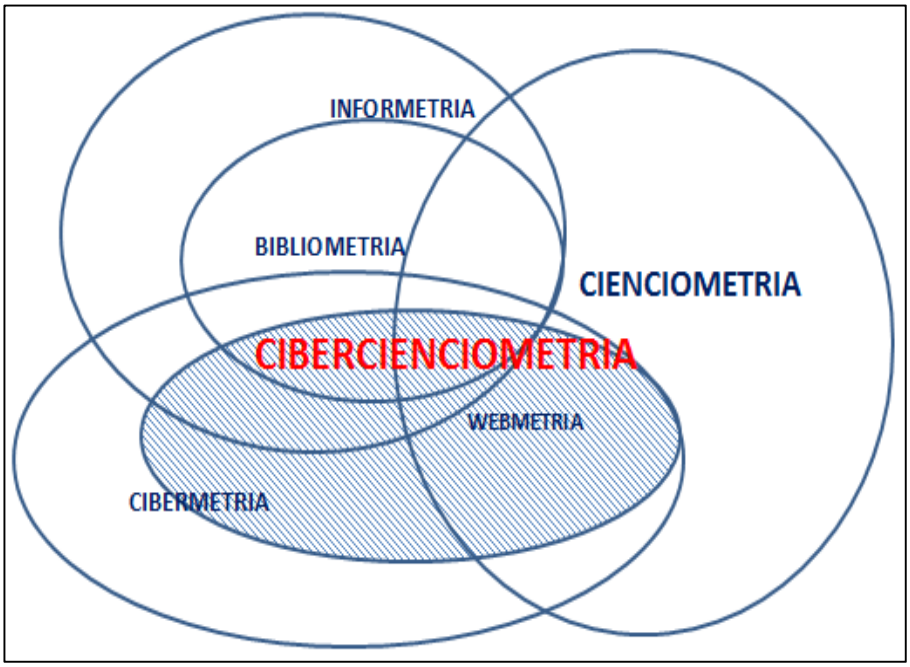


Figura 2. Disciplinas Cuantitativas Cibermetría.
Fuente: Razón y Palabra Revista Electrónica [1]

La Cibermetría trabaja en torno a la información que circula en la Web, obteniendo datos de acuerdo a la necesidad y de igual manera abre la posibilidad de descubrir patrones ocultos existentes en la Red.

2.4.3 Procesamiento del leguaje natural

El Procesamiento del Lenguaje Natural (PLN) tiene como objetivo estudiar e investigar mecanismos computacionales que permitan la comunicación entre personas y máquinas mediante el uso de Lenguajes Naturales (Broncano, Carlos III de Madrid, 2006)

Con el procesamiento del lenguaje natural se busca poder crear programas que puedan analizar, entender y generar lenguajes que los humanos utilizan, de manera que el usuario pueda llegar a comunicarse con el computador de la misma forma que lo haría con un humano.

Se ha demostrado que el lenguaje natural se encuentra organizado a través de un conjunto de reglas, a tal manera que en una oración se asocian para describir

[1] http://www.razonypalabra.org.mx/actual/mlopez.html

objetos y acciones, posiblemente complejas. El objetivo de un analizador sintáctico es precisamente descubrir estas asociaciones entre palabras, lo que se conoce como estructura sintáctica.

El Procesamiento del Lenguaje Natural (PLN) como una subdisciplina de la Inteligencia Artificial y rama de la ingeniería lingüística computacional, pretende lograr que una computadora aprenda a interpretar el lenguaje natural a través de dos caminos, uno epistemológico y otro heurístico (Broncano, Carlos III de Madrid, 2006):

- El epistemológico: define el espacio de conceptos que el programa puede aprender.
- El heurístico: define los algoritmos para el aprendizaje.

Existen algunas aplicaciones del Procesamiento del Lenguaje Natural entre las cuales se encuentran las siguientes:

- Corrección de textos.
- Traducción automática.
- Recuperación de la Información.
- Extracción de información y resúmenes.
- Búsqueda de documentos.
- Sistemas inteligentes para la educación y el entrenamiento.

2.4.4 Recuperación de la información

Existen diversos modelos asociados a la recuperación de información que forman una herramienta que permite diferenciar una consulta previa y una serie de respuestas para dicha consulta. El modelo de recuperación booleana es una de las técnicas que fue utilizada en la realización de este proyecto.

Principales modelos de recuperación de información:

a) **Modelo de recuperación booleano:** Se basa en la teoría de conjuntos y el álgebra booleana de gran simplicidad. El algoritmo de recuperación está fundamentado en un criterio de decisión binaria sin ninguna noción de escala de medida ni ningún emparejamiento parcial en las condiciones de la

consulta. En este modelo el método de representación, consiste en especificar los documentos como un conjunto de términos de indexación o keywords. (Broncano, Carlos III de Madrid, 2006)

b) **Modelo de recuperación vectorial**: Asigna pesos no binarios a los términos índice de las preguntas y de los documentos. Estos pesos de los términos se usan para computar el grado de similitud entre cada documento guardado en el sistema y la pregunta del usuario. Se basa en la construcción de una matriz de términos y documentos, las filas contienen los documentos almacenados en una base de datos y las columnas se corresponden con los términos que se incluye en cada documento. (Broncano, 2006)

c) **Modelo de recuperación probabilístico:** se fundamenta en el cálculo de la probabilidad de que un documento sea relevante a la consulta proporcionada. El cálculo de las probabilidades se toma de la siguiente formula: prob=n/N donde n es el número de documentos que son relevantes a una consulta y N el número de documentos totales del sistema. (Broncano, Carlos III de Madrid, 2006)

2.4.5 Ingeniería de Software

Permitió establecer y usar principios de ingeniería para obtener un producto de software confiable, verificando su funcionamiento en computadoras reales, abarcando el ámbito de programación y análisis, aplicando un método sistemático, disciplinado y cuantificable al desarrollo, operación y mantenimiento de software.

2.4.6 Metodología OOHDM

El modelo OOHDM u Object Oriented Hypermedia Design Method, para diseño de aplicaciones hipermedia y para la Web, es una extensión de HDM (Hypertext Design Model) con orientación a objetos, que se está convirtiendo en una de las metodologías más utilizadas. Ha sido usada para diseñar diferentes

tipos de aplicaciones hipermedia como galerías interactivas, presentaciones multimedia y numerosos sitios web.

Las características principales de las aplicaciones web es la noción de navegación. En OOHDM, se considera a una aplicación web como una vista navegacional del modelo conceptual. OOHDM propone el desarrollo de aplicaciones hipermedia mediante un proceso de 5 etapas:

- Determinación de Requerimientos
- Diseño conceptual
- Diseño navegacional
- Diseño de interfaces abstractas
- Implementación

Cada etapa de la concepción define un esquema objeto específico en el que se introducen nuevos elementos.

a) Determinación de Requerimientos

Permitió la identificación de los actores y las actividades que han sido desarrolladas, tomando en cuenta los requerimientos necesarios, esta fase se fundamenta con los diagramas de casos de usos, los cuales son diseñados con la finalidad de obtener de manera clara los requerimientos y acciones del sistema.

b) Diseño conceptual

Se construye un esquema conceptual representado por los objetos de dominio o clases y las relaciones entre dichos objetos. Se usa un modelo de datos semántico estructural (modelo de entidades y relaciones). El modelo OOHDM propone como esquema conceptual basado en clases, relaciones y subsistemas.

c) Diseño navegacional

Son como nodos, enlaces y estructuras de acceso (índices y visitas guiadas) inducidas del esquema conceptual. Los enlaces derivan de las relaciones y los nodos representan ventanas lógicas sobre las clases conceptuales. Se presentó la estructura navegacional en términos de contextos navegacionales. Un contexto navegacional es un conjunto de nodos, enlaces, clases de contextos y otros contextos navegacionales (contextos anidados) igual que en HDM definen agrupaciones- que pueden ser definidos por comprensión o extensión, o por enumeración de sus miembros. Los nodos se enriquecen con un conjunto de

clases especiales que permiten presentar atributos así como métodos o comportamientos cuando se navega en un contexto particular. Durante esta etapa, es posible adaptar los objetos navegacionales para cada contexto, de forma similar a las perspectivas de HDM.

OOHDM no propone un modelo enriquecido para el dominio de la aplicación, por lo que deja libre al diseñador para elegir el modelo de especificación del dominio. Sin embargo, el modelo hipermedia está definido en dos niveles de abstracción: las clases y los contextos navegacionales.

En el momento de la especificación de las clases navegacionales es cuando el diseñador define las correspondencias y, aunque OOHDM sugiere algunas. Los nodos inducidos de las clases del modelo del dominio y los enlaces inducidos de las relaciones del modelo del dominio se pueden precisar. Como el segundo nivel está consagrado a la especificación de la navegación, expresada exclusivamente sobre los objetos navegacionales (no sobre los elementos del modelo del dominio), constituye un mecanismo que permite enriquecer el modelo hipermedia.

d) Diseño de interfaces abstractas

Se presentó la especificación de la interfaz abstracta definiendo la forma en la cual aparecen los contextos navegacionales. También se incluye el modo en que dichos objetos de interfaz activando la navegación y el resto de funcionalidades de la aplicación. La separación entre el diseño navegacional y el diseño de interfaz abstracta permitirá construir diferentes interfaces para el mismo modelo navegacional.

e) **Implementación**

Dedicada a la puesta en práctica dentro del proyecto, se publicó e instalo el software necesario es donde se hacen corresponder los objetos de interfaz con los objetos de implementación.

2.4.7 Control Parental o Control Paterno

En el contexto de esta investigación, Control Parental son herramientas que permiten a los padres o tutores controlar y/o limitar el acceso a contenido inapropiado por parte de niños y adolescentes al utilizar Internet.

Estas herramientas de Control Parental pueden ser automatizadas o no. Las herramientas automatizadas son aplicaciones para la computadora, mientras las no automatizadas son la educación y la concienciación que se infunda a los jóvenes. (Segu-Kids, 2012)

Técnicas de control (Franco, 2012) :

- Control de navegación: permite controlar a qué sitios es posible o no acceder, se utilizan diferentes técnicas de prevención:
    - Listas blancas/negras
    - Bloqueo por palabras clave
- Bloqueo de aplicaciones: son herramientas que permiten bloquear ciertas páginas web, mensajería, o correo electrónico.
- Control de tiempo: estas herramientas limitan el tiempo o las horas en las que un niño y/o adolescente puede estar utilizando computadora o conectado a Internet.
- Navegadores infantiles: Son herramientas que dan acceso a páginas adecuadas para los niños y adolescentes.
- Herramientas que bloquean la información que sale de la computadora: son aplicaciones que impiden revelar información personal.
- Monitorización: Permite supervisar todas las páginas web visitadas, no son herramientas preventivas.

2.4.8 Benchmarking

"El benchmarking es un proceso continuo de evaluación de los productos, servicios y métodos, con respecto a los de los competidores más eficientes o a las empresas reconocidas como líderes." (Alonso Arévalo & Martín Cerro, 2004)

Toda técnica de Benchmarking comparte una serie de características que le son propias y que se aplican independientemente de su tipo y campo de aplicación, como son:

- El uso de un método de estudio e investigación.
- El desarrollo de un proceso de búsqueda y descubrimiento de información.

- El uso de un método de diseño e implementación.
- La identificación de oportunidades de aprendizaje.
- El desarrollo de un proceso de gestión estratégica sostenida y continua.
- El uso de herramientas para identificar estándares o prácticas de excelencia

2.5 Conclusiones

En este capítulo, se ha abordado en síntesis el marco teórico que sustenta esta Tesis, presentando el listado de las herramientas de control de acceso a Internet categorizadas como las mejores según sus características. De igual manera se expone la técnica de Procesamiento de Lenguaje Natural la cual es tomada para la investigación como base principal en el control de acceso a páginas que contengan información inapropiada. Adicional se indica la metodología OOHDM que fue utilizada en el desarrollo del proyecto.

CAPÍTULO III. DIAGNÓSTICO SITUACIONAL Y HERRAMIENTAS CONTROL PARENTAL

3.1 Introducción

Este capítulo presenta la ubicación geográfica en donde se realiza la investigación (véase la sección 3.2) y las respectivas encuestas, indicando cuales son las variables que se tomaron en cuenta. Adicionalmente presenta el análisis de las encuestas realizadas (véase desde la sección 3.3 hasta la sección 3.5) y el análisis de las herramientas de control de acceso a Internet (véase la sección 3.6).

3.2 Ubicación geográfica del proyecto de investigación.

El análisis sobre el uso de Internet por parte de los menores de edad es realizado en el Valle de los Chillos de la provincia de Pichincha, tomando como referencia a colegios públicos y privados de esta zona. En la figura 3, se puede apreciar el mapa geográfico en donde se realizaron las encuestas del uso del Internet.

Figura 3. Mapa administración zonal Valle de los Chillos

3.3 Identificación de variables a utilizar en el proceso investigativo.

Dentro del proceso investigativo se han identificado variables como son; los niños y adolescentes con acceso al Internet, tomando como muestra a los estudiantes de distintos colegios del Valle de los Chillos. Además las herramientas de filtrado de

contenido Web, como son las herramientas de Control Parental que existen en el mercado y de acuerdo a la encuesta realizada por Sociedad de Información Europea, presenta a las mejores herramientas con este tipo de controles.

3.4 Método de investigación, técnicas e instrumentos de recolección.

La metodología aplicada en el desarrollo de la presente investigación es el Método Científico, con aplicación de los métodos Deductivo e Inductivo, utilizando las técnicas de recopilación de datos como: la encuesta, entrevista, observación, análisis documental y el experimental. En este proceso de investigación se realizan tres tipos de encuestas:

- Encuesta dirigida a los estudiantes entre las edades 11 a 17 años pertenecientes a colegios públicos y privados, teniendo como objetivo: medir la frecuencia de uso, el tipo de información, amenazas y medios de vigilancia en el acceso a contenidos Web de los niños y adolescentes, con el fin de identificar mecanismos de control para mitigar el acceso a contenido inapropiado en el Internet. (Ver Anexo 1)
- Encuesta dirigida a los padres y representantes de los adolescentes, su objetivo: Medir el grado de control y protección que los padres tienen frente al uso de Internet para los niños y adolescentes. (Ver Anexo 2)
- Encuesta dirigida a los técnicos de colegios su objetivo es: Medir las técnicas de control y mitigación que son establecidas por el administrador de red para sus usuarios. (Ver Anexo 3)

3.5 Análisis de las métricas para la evaluación.

Para conocer cuál es el uso que los niños y adolescentes tienen con Internet, se realizaron encuestas en los colegios ubicados dentro del Valle de los Chillos tomando como referencia los datos entregados por el Ministerio de Educación los cuales se encuentran publicados en la Web. (Educación, 2013)

Para determinar el universo, se investiga la cantidad de colegios que existen en el Valle de los Chillos y la cantidad de alumnos que pertenecen a ellos. En la tabla 1 se puede observar la cantidad de alumnos matriculados en el periodo lectivo 2013-2014

en el Valle de los Chillos, de igual manera en el figura 4 se puede apreciar gráficamente estos datos.

Tabla 1.

Colegios en el Valle de los Chillos

Unidades Educativas Los Chillos		
Sostenimiento	**Nro. de colegios**	**Nro. de alumnos**
Fiscal	73	17222
Fiscomisional	10	2027
Municipal	3	486
Particular Laico	71	12668
Particular Religioso	15	5846
Total Unidades Educativas Los Chillos	**172**	**38249**

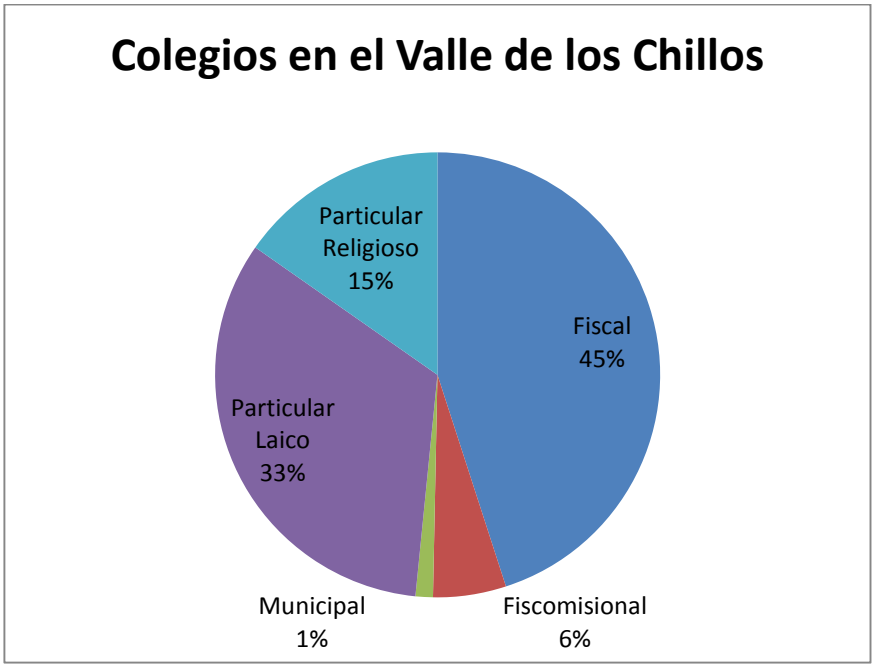


Figura 4. Representación gráfica de colegios en el Valle de los Chillos

Para determinar el número de encuestados en base a los datos adquiridos del Ministerio de Educación se procedió a obtener el cálculo del tamaño de la muestra aplicando la siguiente formula:

$$n = \frac{(k^2) * N * p * q)}{(e^2 * (N-1)) + ((k^2) * p * q)}$$

Ecuación (1)

Dónde:

N: es el tamaño de la población o universo (número total de estudiantes);

k: es una constante que depende del nivel de confianza que sea asignada. El nivel de confianza indica la probabilidad de que los resultados de la investigación sean ciertos;

Los valores k más utilizados y sus niveles de confianza se presentan a continuación:

Tabla 2.
Tabla de niveles confianza

K	1,15	1,28	1,44	1,65	1,96	2	2,58
Nivel de confianza	75%	80%	85%	90%	95%	95,50%	99%

p: es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p = q = 0.5 que es la opción más segura;

q: es la proporción de individuos que no poseen esa característica, es decir, es 1- p;
n: es el tamaño de la muestra (número de encuestas que se realizaron).

Después de la aplicación de la fórmula para obtener la muestra, se presentan los datos a los que deben aplicarse las encuestas, tanto para los adolescentes, representantes y personal técnico de los colegios.

- Encuestas dirigidas a niños y adolescentes entre las edades de 11 a 17 años, los datos después de aplicar la formula se ve representada en la tabla 3.

Tabla 3.
Total de alumnos para encuestas por tipo de colegios

Colegios	Nro. de encuestas
Fiscal	178,2
Fiscomisional	23,76
Municipal	3,96
Particular Laico	130,68
Particular Religioso	59,4
Total	**396**

- Encuestas dirigidas a padres y/o representantes de niños y adolescentes de 11 a 17 años, se realizaron encuestas a los alumnos de maestrías de la Universidad de las Fuerzas Armadas ESPE.
- Encuestas dirigidas a responsables técnicos de los Colegios encuestados.

3.5.1 Indicadores de medición.

En la figura 7 se puede apreciar el número de encuestas que debieron ser aplicados por el tipo de sostenimiento de los colegios.

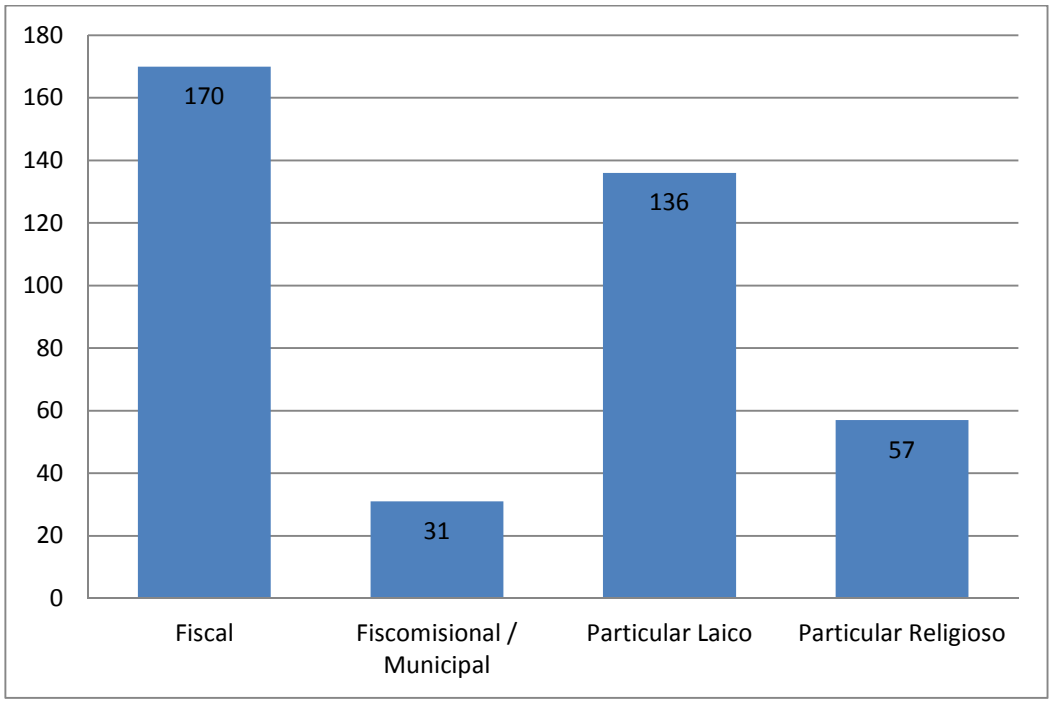


Figura 5. Total de adolescentes encuestados

1. Análisis de las encuesta dirigida a los niños y adolescentes

Pregunta 1. (¿Ha utilizado internet?)

Análisis: Todas las personas encuestadas utilizan Internet sin importar la edad, género y tipo de colegio al que pertenecen (véase figura 6).

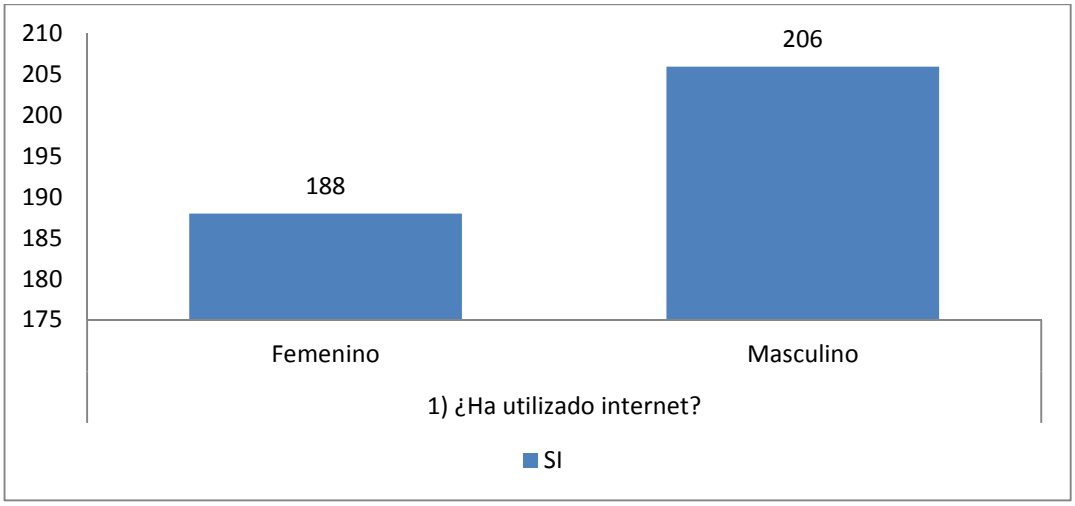


Figura 6. Uso del Internet por genero

- **Pregunta 2** (¿Qué dispositivo utilizas para acceder a Internet?)

Análisis: El dispositivo más utilizado para acceder a Internet es la computadora de escritorio (PC), siendo seguido por la portátil y los celulares (véase figura 7)

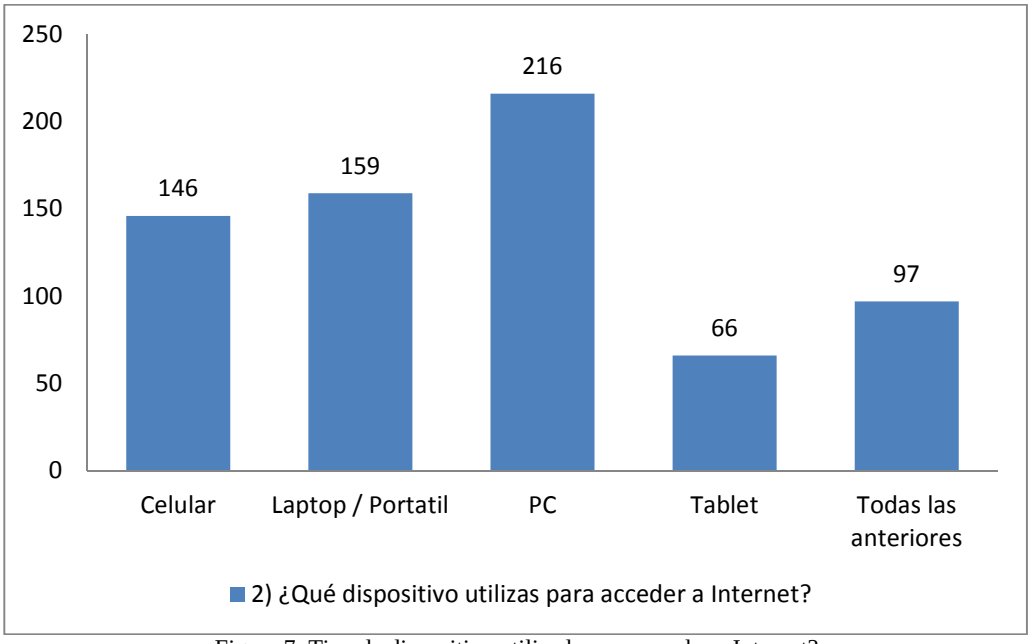


Figura 7. Tipo de dispositivo utilizado para acceder a Internet?

- **Pregunta 3 (¿**Desde qué lugar accedes al Internet**?)**

Análisis: Se demuestra que las adolescentes pertenecientes a colegios particulares Laicos son los que más acceden al Internet y por el contrario los

colegios Fiscomisionales y Municipales. Los lugares de mayor tiempo de acceso son los hogares, por esta razón se debe tomar mayor atención en los domicilios de los niños y adolescentes. En la figura 8 se puede apreciar que efectivamente los colegios Laicos son los que más acceden al Internet dentro del Hogar.

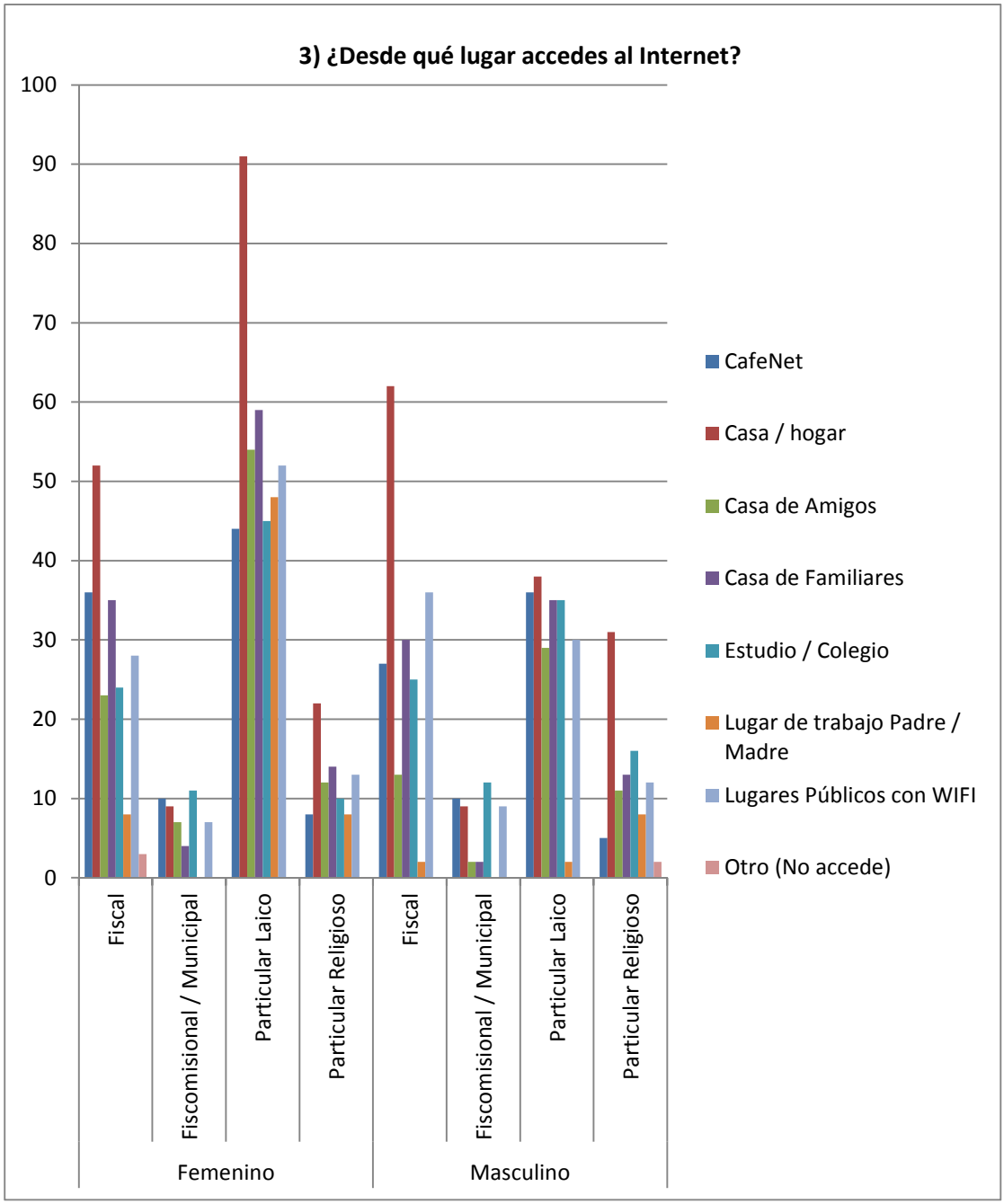


Figura 8. Lugar desde donde acceden al Internet

- **Pregunta 4** (¿Tienes Internet en tu casa / hogar?)

Análisis: Todos los alumnos entrevistados en el colegio Particular Laico tienen acceso a Internet, los alumnos de las demás instituciones también tienen acceso a Internet en menor porcentaje (Véase figura 9). Con esta información se comprobó que la problemática está latente en todos los hogares.

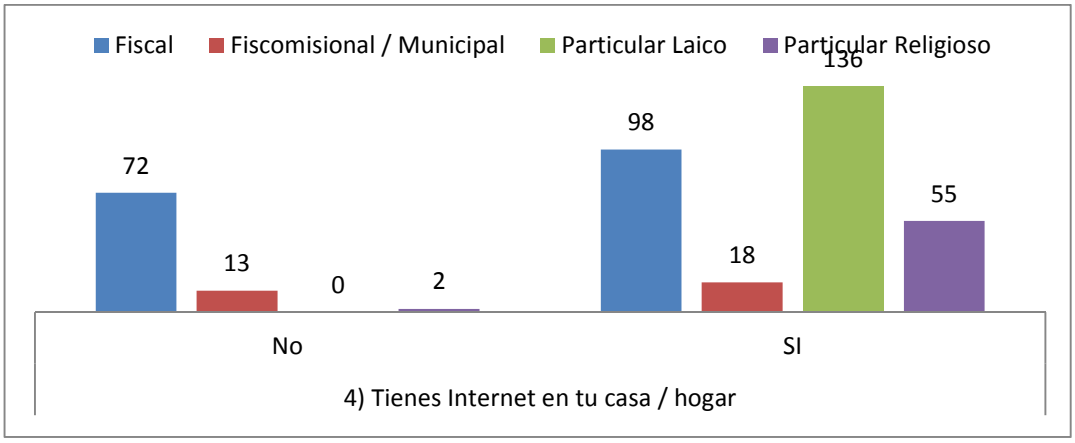


Figura 9. Tiene o no Internet en sus hogares

- **Pregunta 5.** (¿En qué lugar de tu hogar se encuentra ubicado el computador?)

Análisis: Los lugares donde están ubicados el computador con acceso al Internet es la sala de estudios, dormitorios y sala social, hoy en día el avance de la tecnología le ofrece mayor facilidad el acceso inalámbrico de esta manera el acceso a la red es desde cualquier lugar (Véase figura 10).

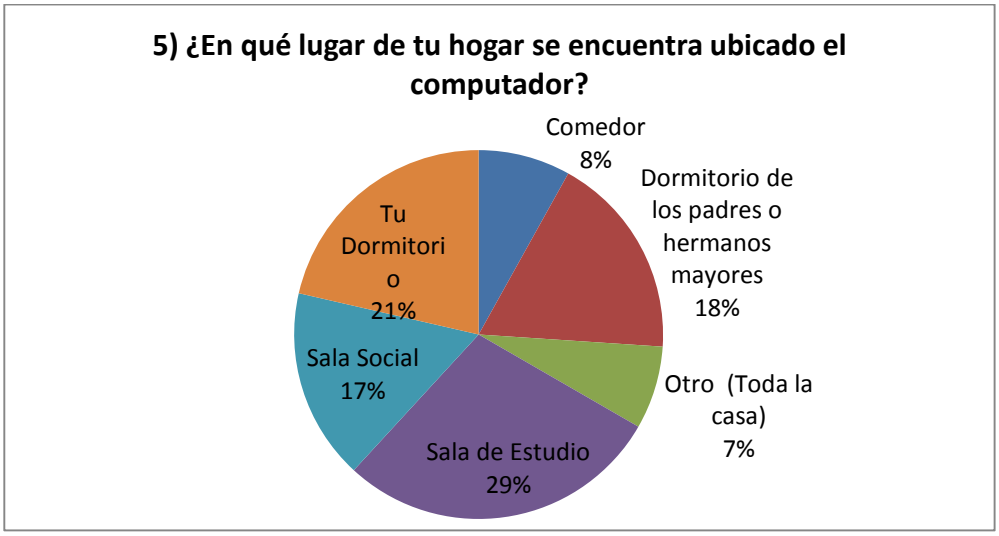


Figura 10. Lugar del hogar donde se encuentra ubicado el computador

- **Pregunta 6** (¿Conoces qué sistema operativo tiene tu computador?)

Análisis: El sistema operativo utilizado por la mayoría de los encuestados es Windows, siendo Windows 7 el más común, es por esta razón que al análisis se enfoca a los Sistema Operativos de Microsoft (Véase figura 11).

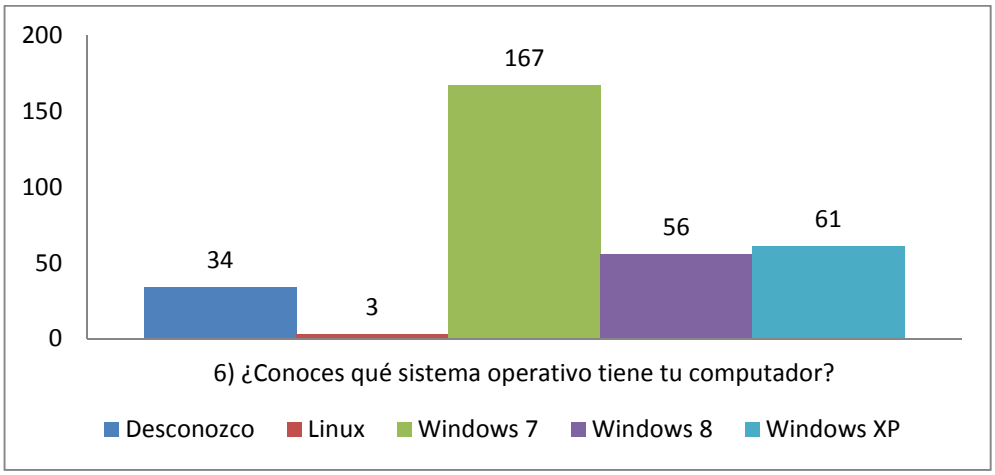


Figura 11. Sistema Operativo que utilizan

- **Pregunta 7** (¿Tienes instalado algún programa de protección o antivirus en tu computador?)

Análisis: La mitad de los adolescentes tanto hombres como mujeres de los colegios particulares seguidos por colegios fiscales si tienen instalado un sistema de protección o antivirus en sus computadores (Véase figura 12).

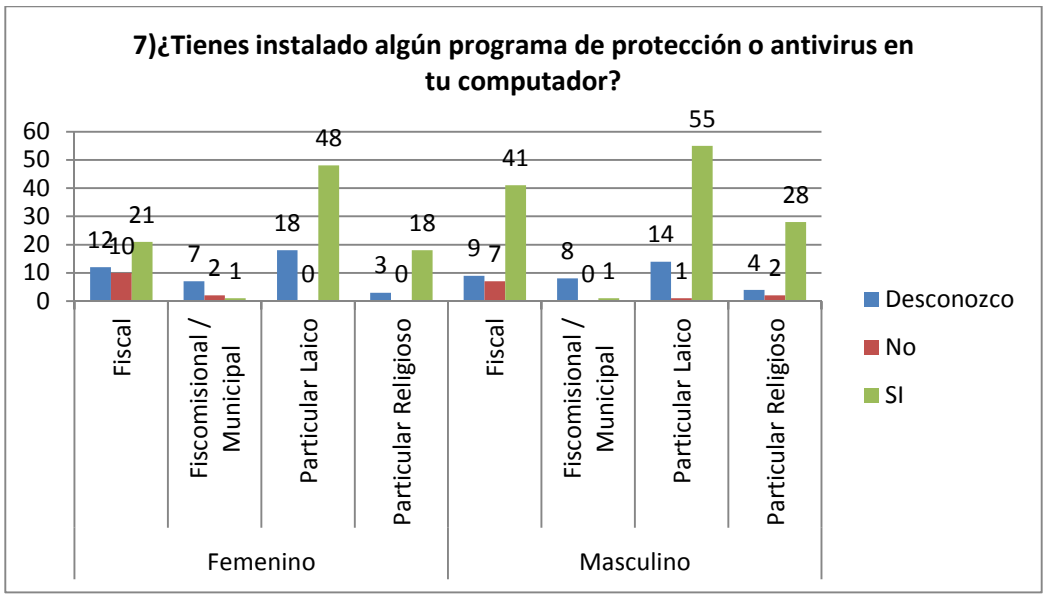


Figura 12. Tiene o no instalado un programa de protección o antivirus en su computador

- **Pregunta 8.** (¿Con que frecuencia accedes a Internet?)

Análisis: Las barras de color verde refleja claramente que estudiantes de todos los tipos de instituciones educativas acceden al Internet todos los días, este debido al avance de la tecnología y a la necesidad de estar comunicados por las diferentes actividades (Véase figura 13).

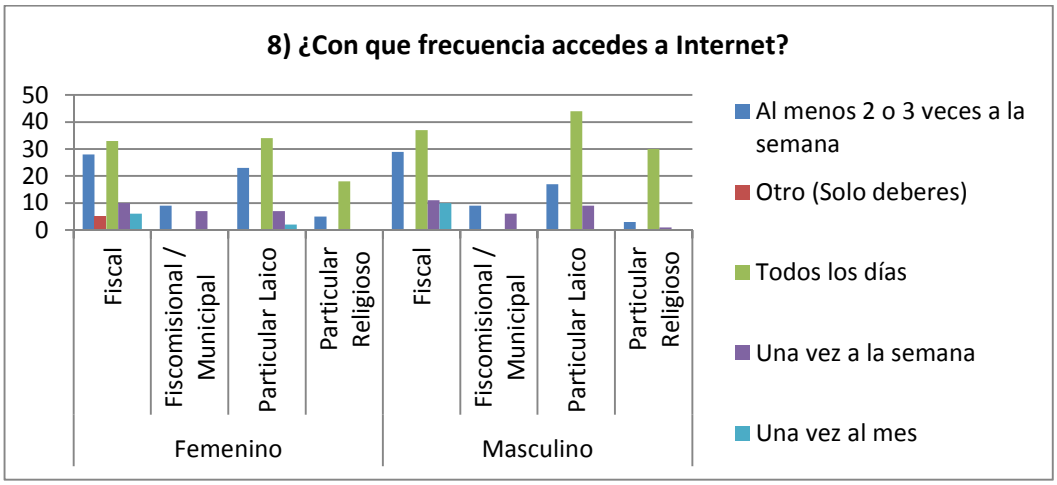


Figura 13. Frecuencia con la que accede al Internet

- **Pregunta 9** (¿A qué hora sueles conectarte a Internet?)

Análisis: La mitad de la población de adolescentes acceden a Internet en la tarde, por lo que los padres de familia no están preparados ante el volumen de información que se presenta en la Web, permitiendo el acceso a sitios inadecuados en Internet durante la ausencia de los padres (Véase figura 14).

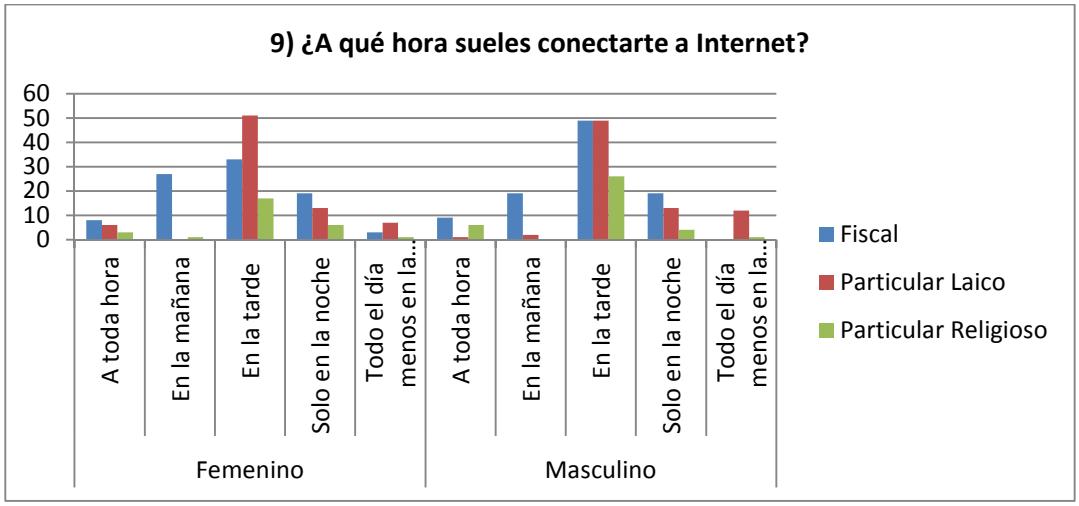


Figura 14. Horario en los que acceden al Internet

- **Pregunta 10** (¿Cuánto tiempo en promedio utilizas el Internet en cada sesión?)

Análisis: Esta pregunta se relaciona con la pregunta 8, por lo que se puede concluir que tanto en hombres como mujeres utilizan todos los días Internet especialmente los adolescentes de instituciones Fiscales y Particulares Laicos (Véase figura 15).

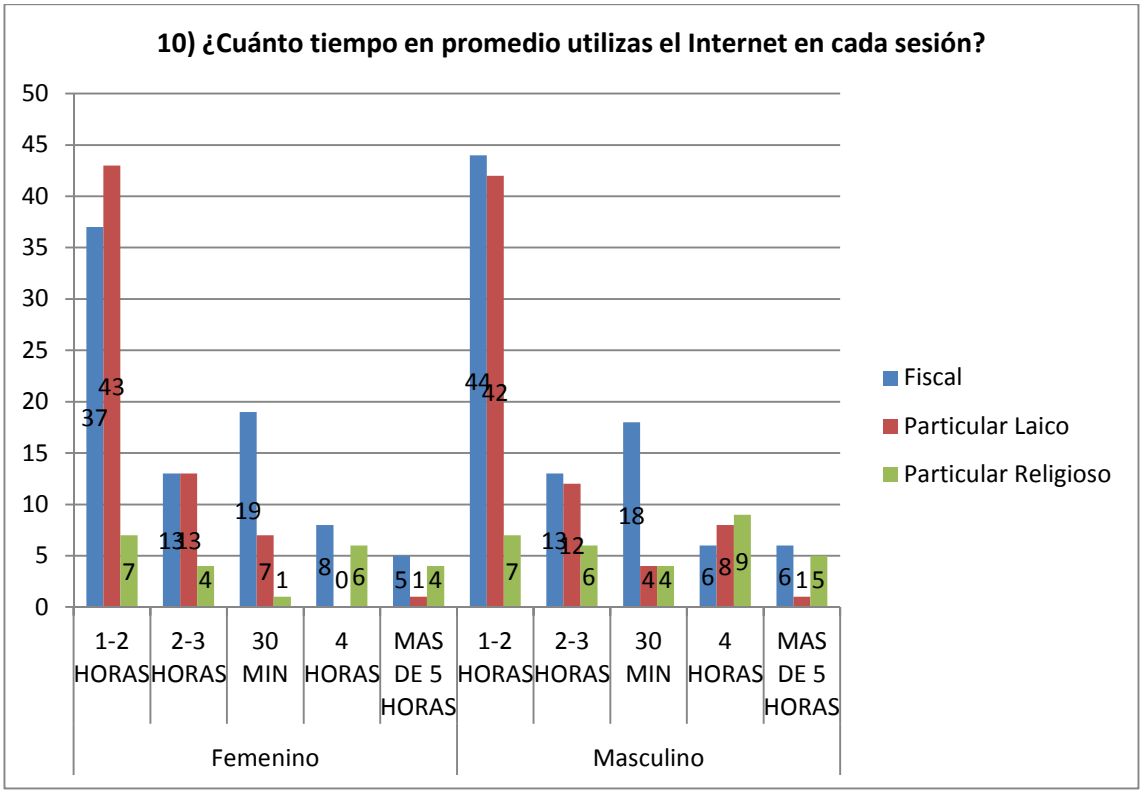


Figura 15. Promedio de uso del Internet por sesión

- **Pregunta 11** (¿Para qué utilizas Internet?)

Análisis: La gran mayoría una parte del tiempo lo utiliza para la búsqueda de información relacionada a los estudios, añadiendo actividades adicionales como el chat y escuchar música online (Véase figura 16).

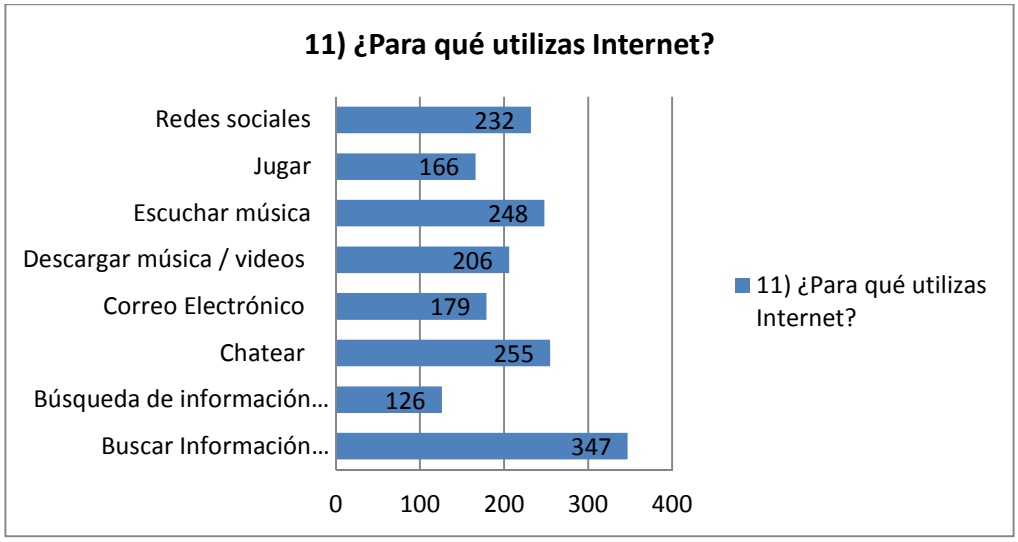


Figura 16. Motivos de uso de Internet

- **Pregunta 12** (¿Tienes creada una o varias cuentas en alguna red social?)

Análisis: La población de adolescentes tanto femenino como masculino de colegios fiscales la mayoría poseen de una cuenta de red social, es necesario disponer de software que permita filtrar el correo basura, de esa manera los menores de edad no reciban correos electrónicos ofensivos (Véase figura 17).

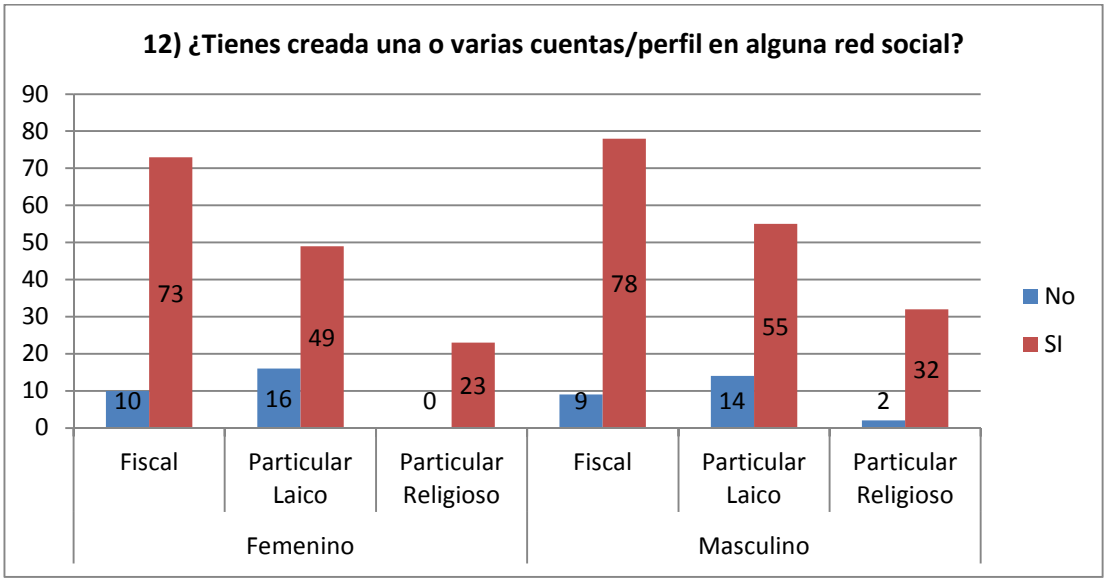


Figura 17. Tiene o no creados cuentas o perfiles en alguna red social

- **Pregunta 13** (¿Cuál es la red social que más utilizas?)

Análisis: Una de las redes sociales más utilizadas a nivel mundial y además en este medio es el Facebook seguida del Twitter tal como lo confirma este estudio (Véase figura 18).

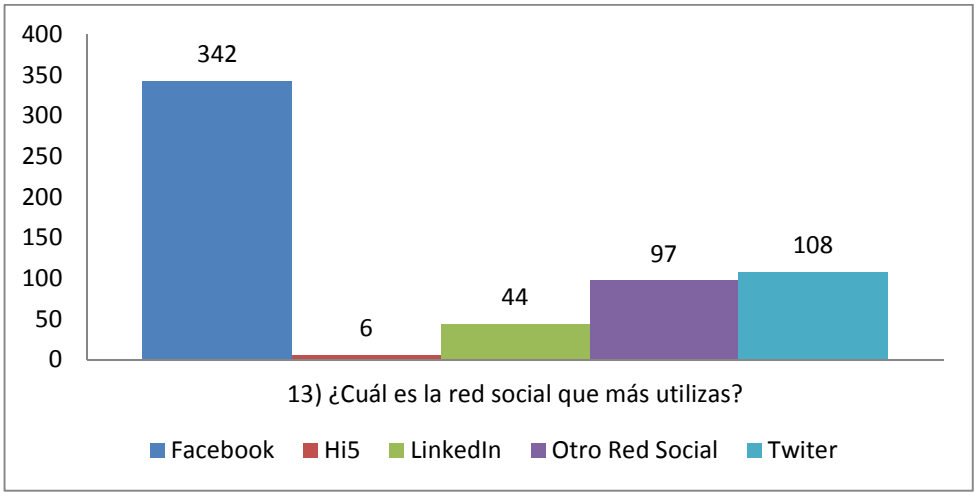


Figura 18. Red social más utilizada

- **Pregunta 14** (¿Cuántos amigos tienes en la red social que más utilizas?)

Análisis: Los valores se encuentra muy variados, se puede señalar que los adolescentes con mayor cantidades de contactos muestran son los de los colegios religiosos tanto en mujeres como hombres (Véase figura 19).

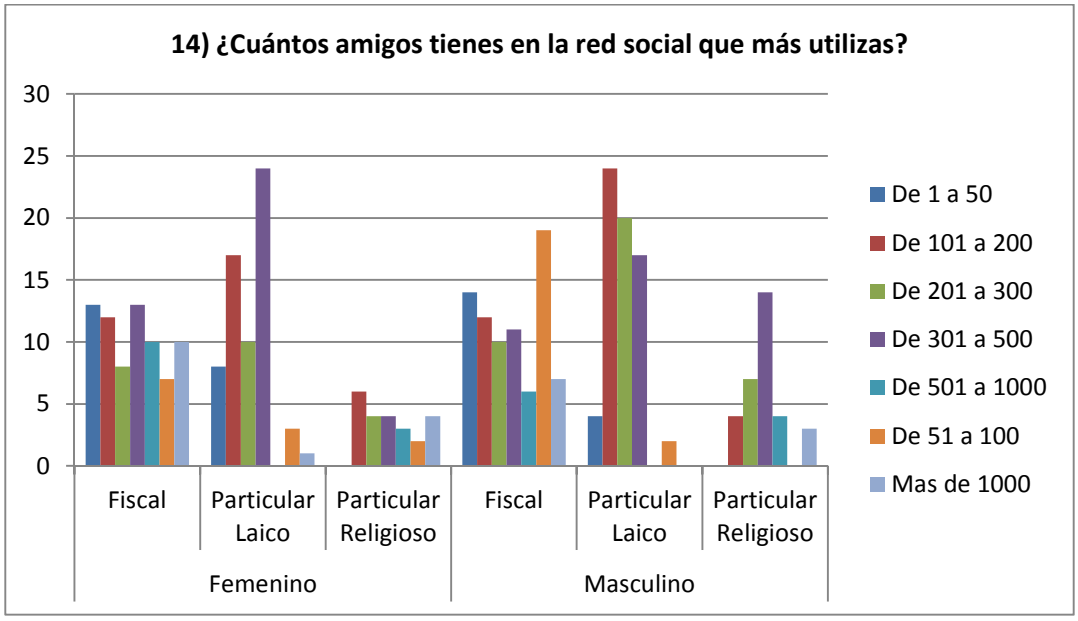


Figura 19. Cantidad de amigos en la red social

- **Pregunta 15** (¿De los amigos que tienes en la red social, aproximadamente a cuantos conoces personalmente?)

Análisis: Tanto en hombres como mujeres de Instituciones Particular Laico sus contactos son personas conocidas en su mayoría muy por lo alto del resto, esta práctica se debería ser replicada a todos los adolescentes ya que de esta manera se puede evitar influencias malas (Véase figura 20).

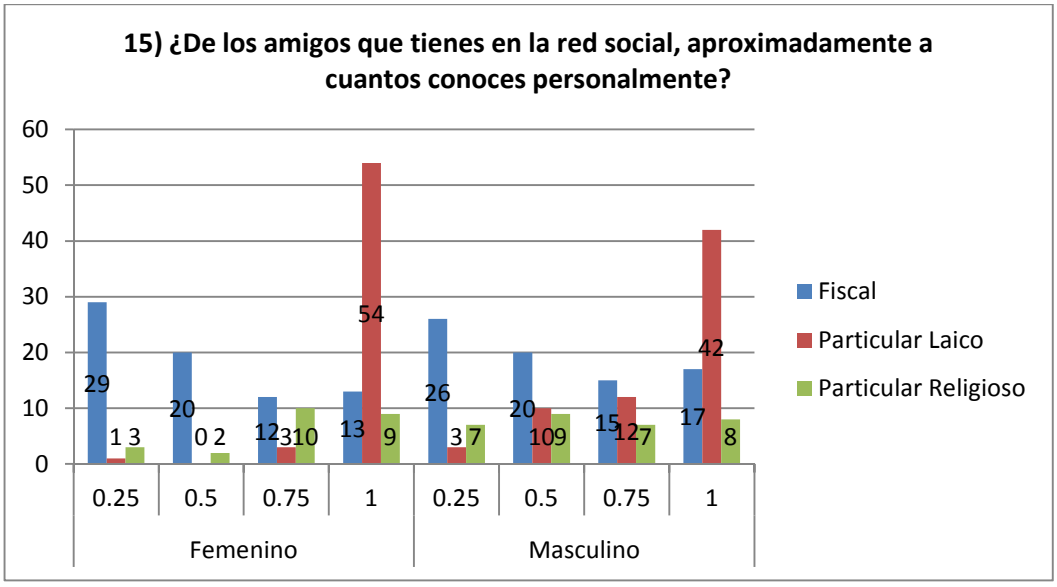


Figura 20. Cantidad de personas conocidas en la red social

- **Pregunta 16** (¿Te comunicas a menudo con personas que NO conoces personalmente?)

Análisis: En la figura 21, representa gráficamente que la comunicación con personas desconocidas en la Web es común entre los menores, el riesgo mediante la comunicación privada con personas de cualquier parte del mundo a través del Internet sin ningún costo, comunicación que puede ser perjudicial para el adolescente generando inseguridad y debilita valores interpersonales, por lo que se requiere software de control y vigilancia por parte de los padres de familia.

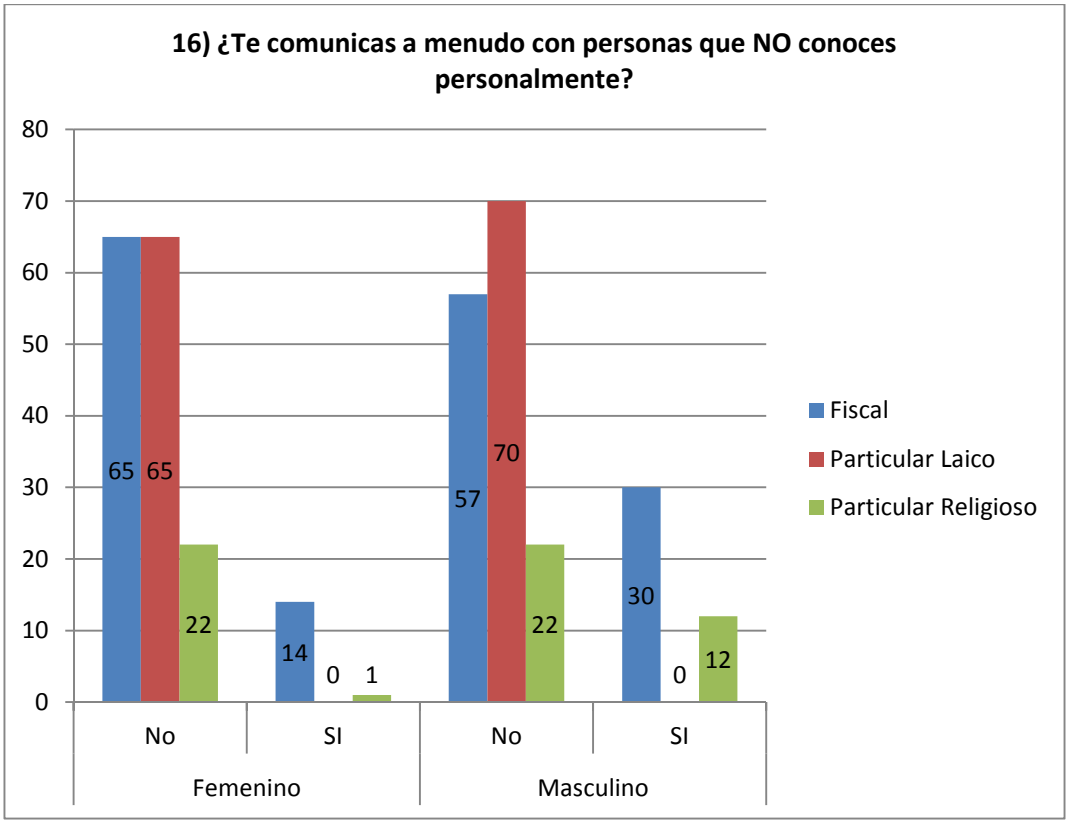


Figura 21. Cantidad de veces se comunica con personas que no conoce

- **Pregunta 17** (¿Para qué usas estas redes o comunidades virtuales?)

Análisis: La mitad de la población usan las redes o comunidades virtuales para estar en contacto con amigos frecuentes seguido por hacer nuevos amigos, debido a que las comunidades virtuales suponen nuevos espacios para la comunicación entre iguales con intereses comunes y objetivos de intercambio, pero crea problemas como el ciberbulliying e incluso una adicción cuando invierten demasiado tiempo, por lo que se debe requerir que los contenidos dados a terceros deben ser autorizadas su publicación y fomentar un canal de denuncia (Véase figura 22).

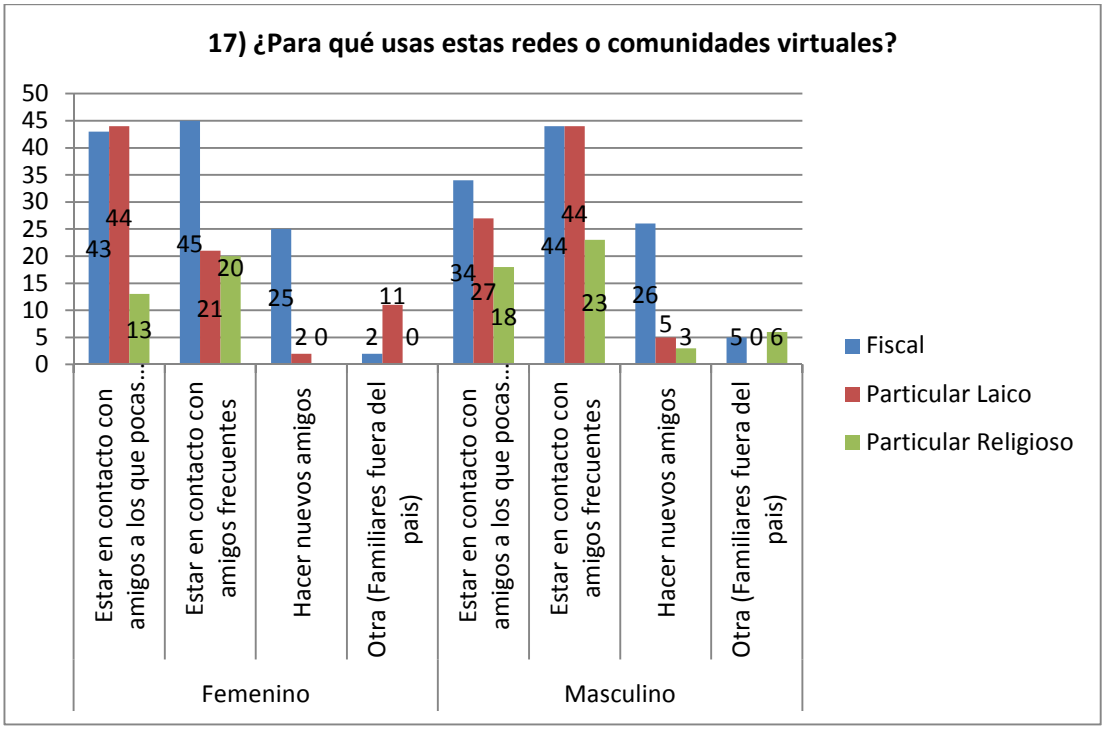


Figura 22. Porque se usa las redes

- **Pregunta 18** (¿Tus padres o algún adulto supervisa mientras estas conectado a Internet?)

Análisis: La supervisión por parte de los padres o representantes es del 26% que siempre está un adulto vigilante sobre el uso del Internet, el 15% reconoce que nunca han sido supervisados, la población restante no siempre están siendo monitoreados por adultos (Véase figura 23).

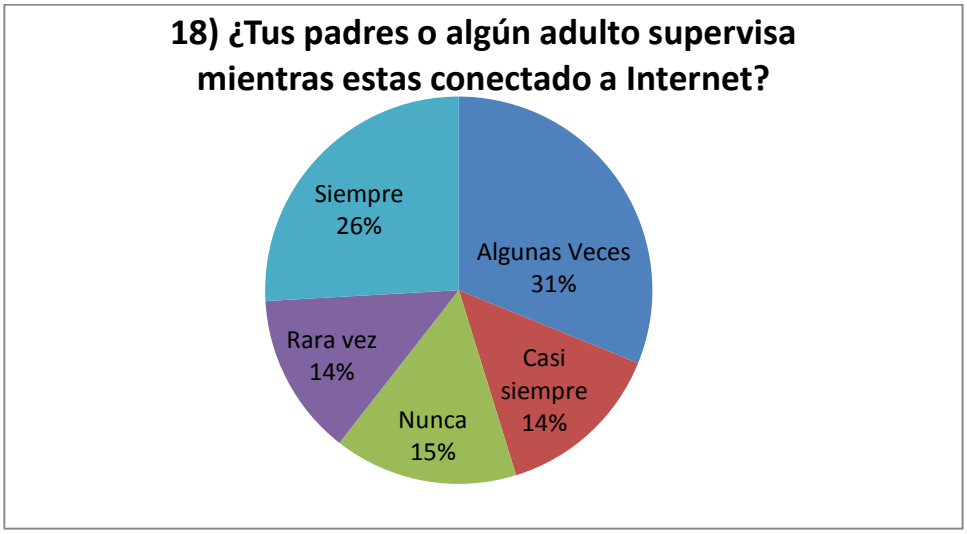


Figura 23. Supervisión cuando se encuentra en el Internet

- **Pregunta 19** (¿Has sufrido alguna clase de peligro o agresión cuando utilizas Internet?)

Análisis**:** La gran mayoría señala que no ha sufrido ninguna agresión o ha estado en peligro, tanto hombre como mujeres y de todo tipo de instituciones, a pesar de ser pocos los de estar en algún peligro no se debe pasar de alto y se debe también establecer controles (Véase figura 24).

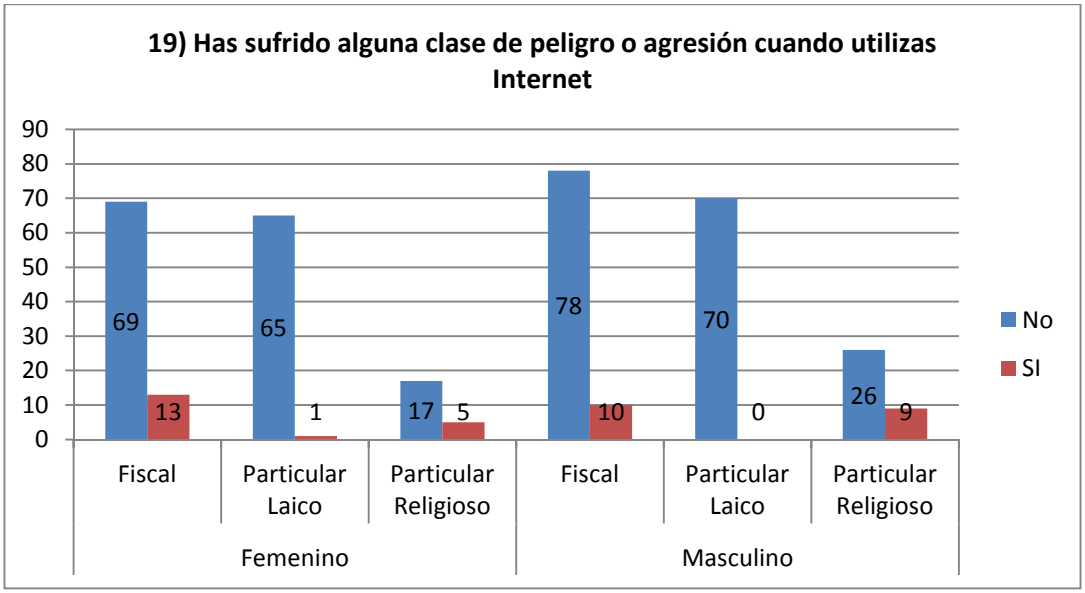


Figura 24. Sufrió o no alguna agresión por Internet

2. Análisis de las encuestas dirigidas a padres y/o representantes de niños y adolescentes.

Se realizaron en total 228 encuestas, las cuales fueron realizadas a un grupo de padres de familia del Colegio Técnico Alangasí y en la Universidad de las Fuerzas Armadas ESPE.

- **Pregunta 1.** (¿En su hogar existen niños y/o adolescentes entre las edades de 10 y 17 años?)

Análisis: Es importante notar que en la mayoría de hogares existen adolecentes dentro del rango de estudio que están más expuestos a sufrir agresiones mediante el Internet (Véase figura 25).

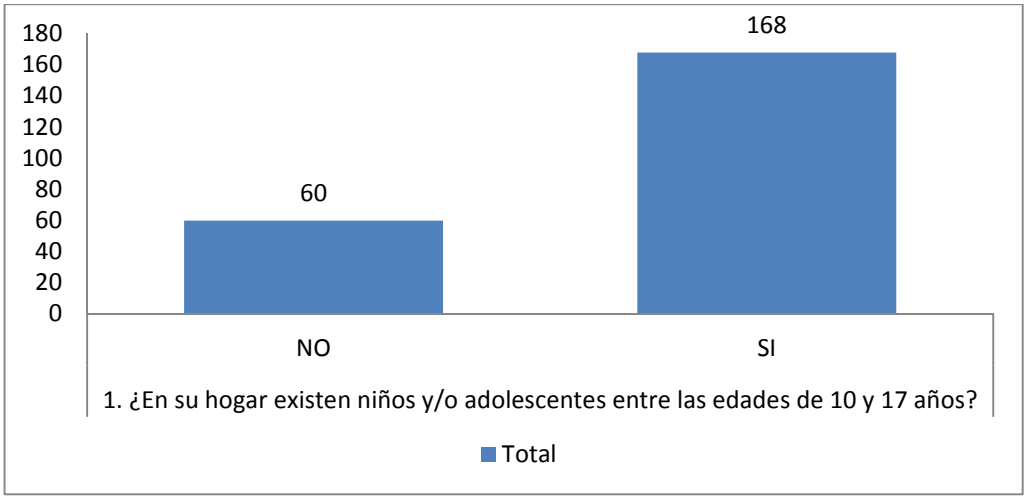


Figura 25. Cantidad de adolescentes en los hogares

- **Pregunta 2.** (¿Posee Internet dentro de su hogar?)

Análisis: Un alto porcentaje de domicilios cuentan con acceso a Internet, con este dato se puede justificar la implementación de controles de navegación para evitar que sus hijos no estén expuestos (Véase figura 26).

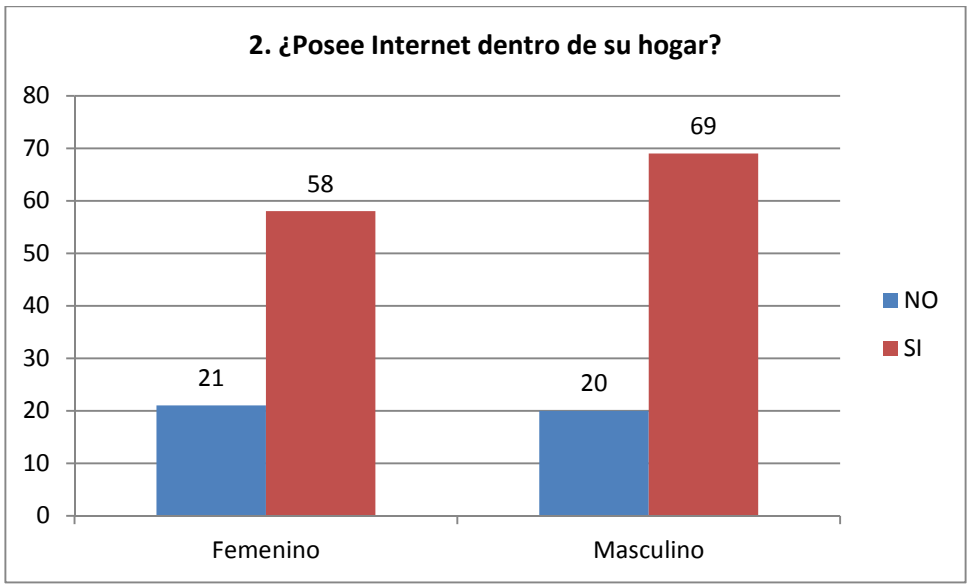


Figura 26. Posee o no Internet en los hogares

- **Pregunta 3.** (¿En qué lugar se encuentran los computadores con acceso a Internet dentro de su hogar?)

Análisis: De acuerdo a la encuesta realizada en la mayoría de hogares el computador se encuentra en la sala de estudio, los porcentajes son similares con el resto, sin embargo hay que recalcar que dentro del dormitorio de los menores también tienen un computador (Véase figura 27).

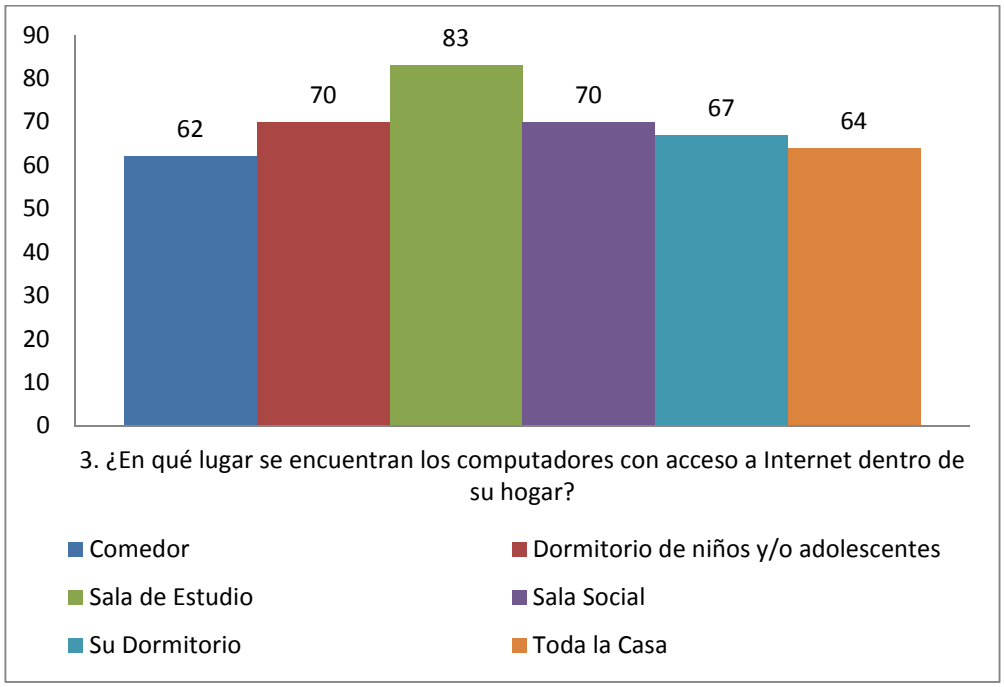


Figura 27. Ubicación de computadores

- **Pregunta 4.** (¿Conoce qué sistema operativo tiene su computador?)

Análisis: Este dato es muy importante, ya que la mayor cantidad de equipos de los hogares utiliza Sistemas Operativos (S.O.) de Microsoft (Windows XP, Windows 7 y Windows 8), es por esta razón se analizará las herramientas compatibles con dichos S.O. (Véase figura 28).

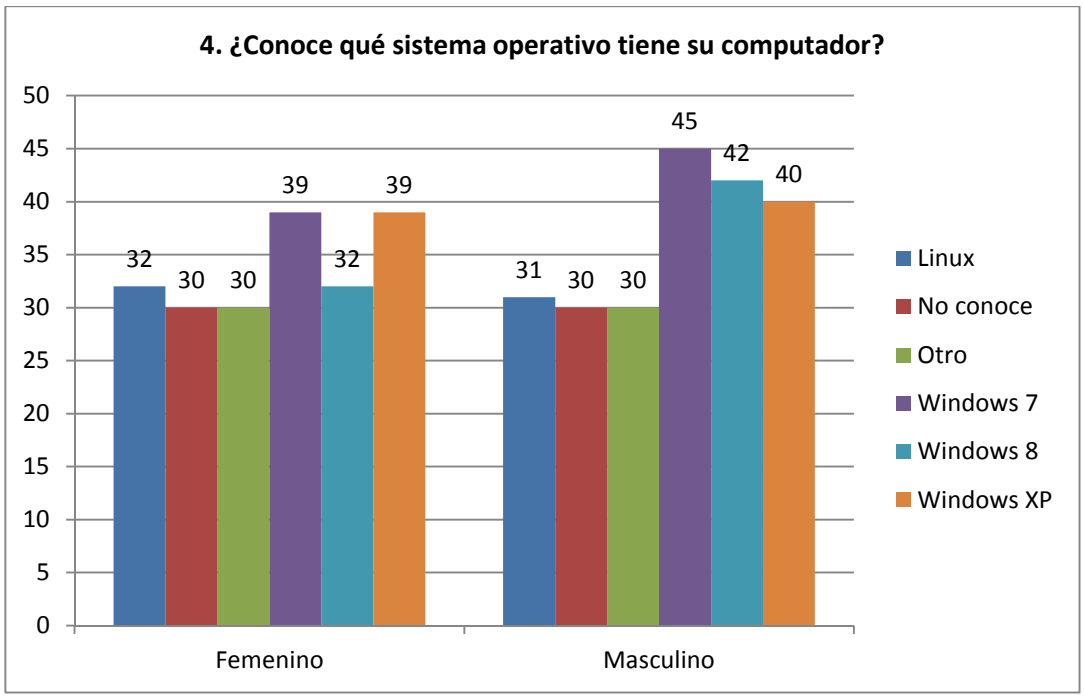


Figura 28. Sistema Operativo más usado

- **Pregunta 5.** (¿Tiene instalado algún programa de protección, monitoreo o control de acceso al Internet?)

Análisis: Mas de la mitad de encuestados señalan que no tienen ningún software que monitoree la navegación, esto puede suceder por el desconocimiento de los padres de la problemática a la que están expuestos sus hijos (Véase figura 29).

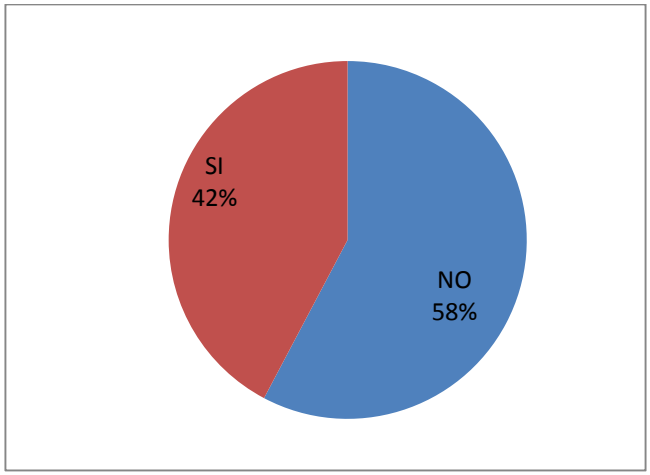


Figura 29. Software de control de acceso a Internet

- **Pregunta 6.** (¿Tiene instalado algún antivirus en su equipo con acceso a Internet?)

Análisis: La mayoría de equipos, tienen instalado algún antivirus, hay que tomar en cuenta que no todos los antivirus controlan el acceso a Internet, más bien su función es proteger de los ataques de virus, gusanos, y otros (Véase figura 30).

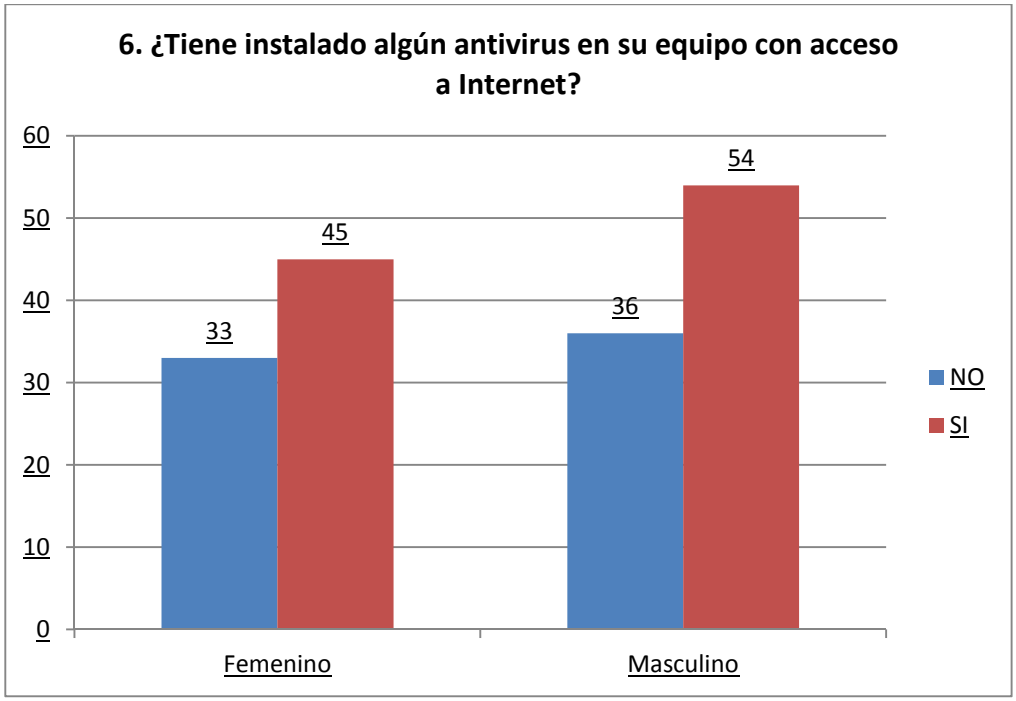


Figura 30. Tiene o no instalado antivirus

- **Pregunta 7.** (¿Ha realizado alguna configuración de Control Parental en su computador?)

Análisis: El menor porcentaje de hogares no han instalado y configuradas herramientas de control parental, esto nos permite buscar y mostrar las mejores alternativas para poder ofrecer las mejores alternativas (Véase figura 31).

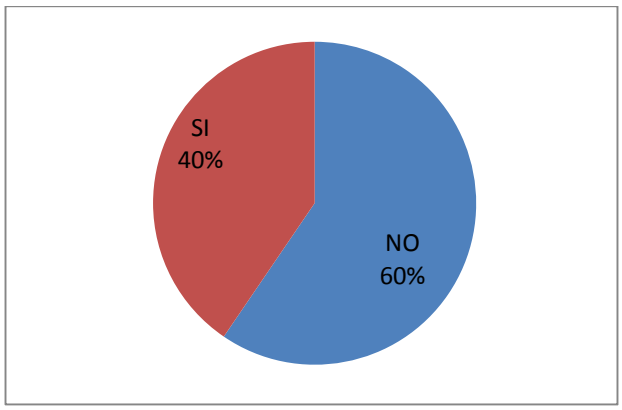


Figura 31. Configuración Control Parental

- **Pregunta 8.** (¿Permite que sus hijos utilicen Internet a cualquier hora?)

Análisis: Los valores obtenidos son semejantes, por esta razón es recomendable que el control de navegación debe ser permanente, de esta manera podremos cubrir todos los horarios del uso del computador (Véase figura 32).

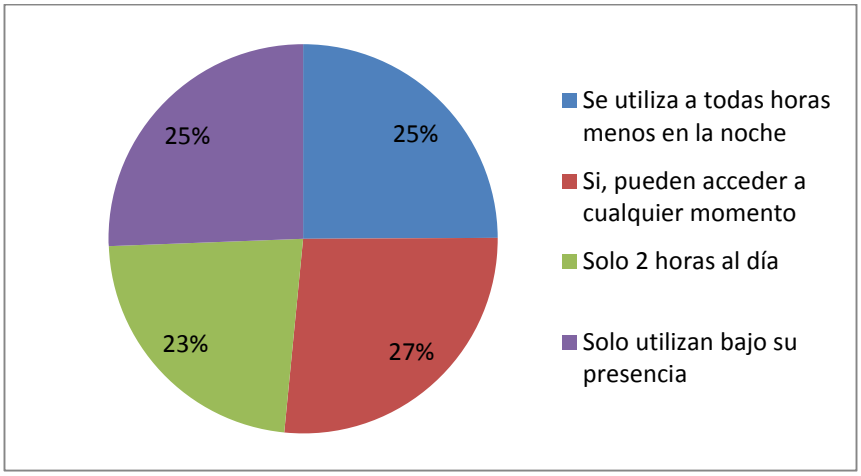


Figura 32. Hora de acceso al Internet

- **Pregunta 9.** (¿Supervisa que hacen su(s) hijo(s) en Internet?)

Análisis: Los resultados obtenidos son muy parecidas, hoy en día es muy complicado vigilar en razón que tanto su madre como padre laboran (Véase figura 33).

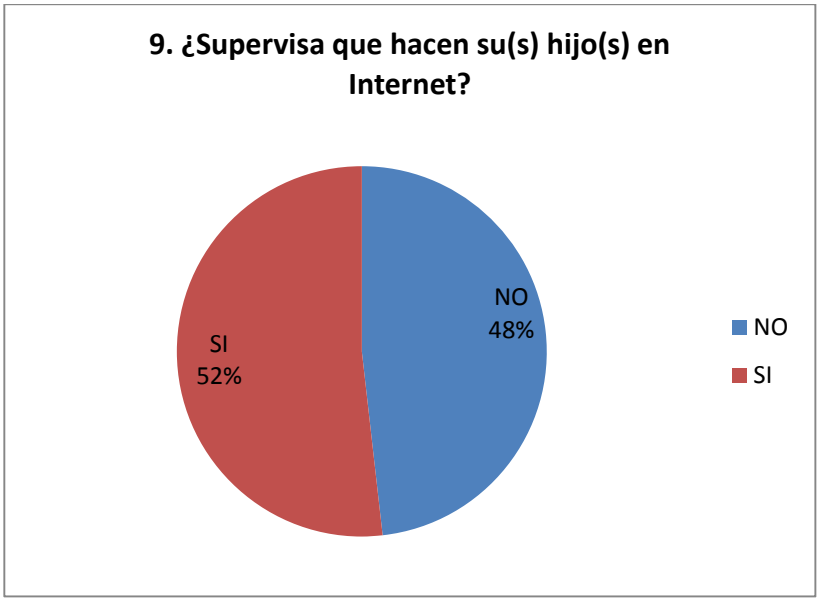


Figura 33. Supervisión de Uso en Internet

- **Pregunta 10.** (¿Conoce cuáles son los peligros a los que está expuesto su hijo en Internet?)

Análisis: El porcentaje entre los que conocen y desconocen de los peligros son bastante cercanos, es muy alto que la mitad de personas desconozcan de la exposición a las cual están expuestas sus hijos (Véase figura 34).

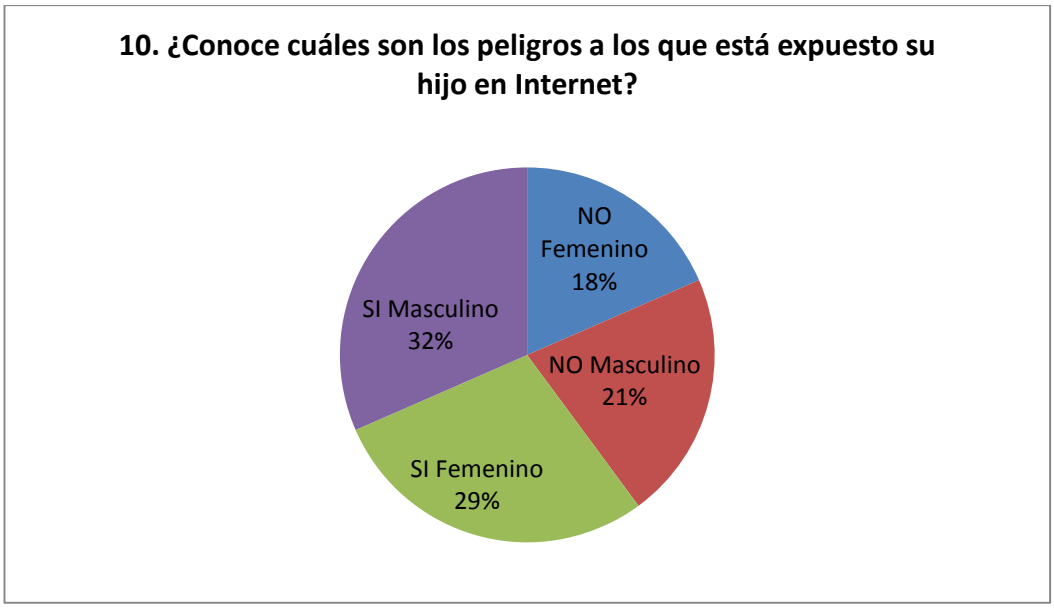


Figura 34. Peligros que están expuestos en Internet

- **Pregunta 11.** (¿Cree que su hijo utiliza responsablemente el Internet?)

Análisis: A pesar que los porcentajes de que los padres creen que sus hijos utilizan responsablemente son altos, esto no puede ser tan real por la exposición que está a todas las amenazas del Internet (Véase figura 35).

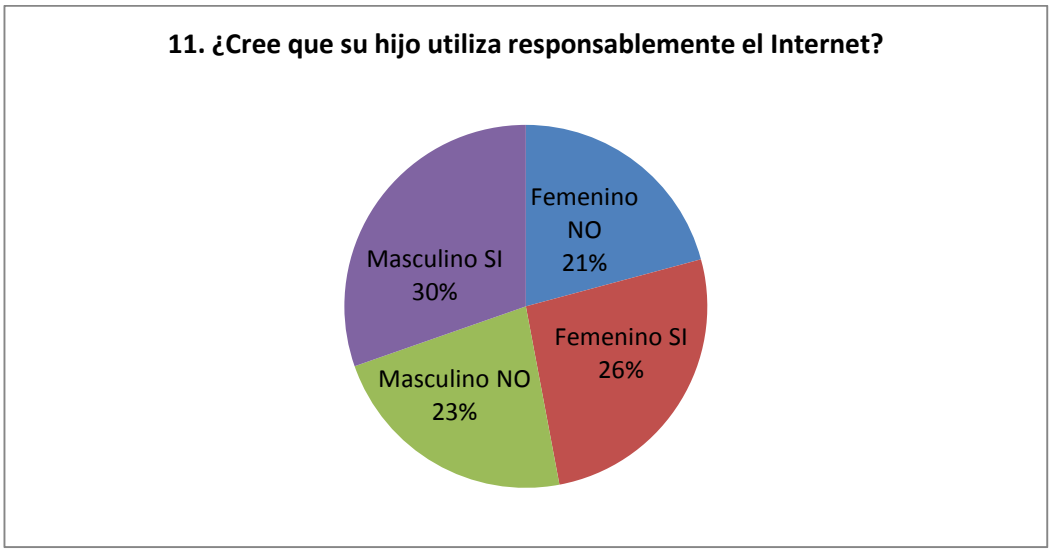


Figura 35. Uso de Internet responsable

3. Análisis de las encuestas dirigidas a responsables técnicos de los Colegios encuestados

La encuesta se realizó a los técnicos encargados de las Instituciones Educativas donde se efectuó las encuestas a los adolescentes; para esto se consideró a establecimientos fiscales, particulares laicos y particulares religioso, como se muestra en la Tabla 4.

Tabla 4.

Técnicos encargados del área de Informática

Técnicos encuestados por Unidad Educativa	
Nombre de la Institución	**Nº. Técnicos**
San Luis Gonzaga	2
Academia Militar del Valle	1
Colegio Nacional Conocoto	2
Colegio Nacional Alangasí	1
Unidad Educativa Gutenberg Schule	1
Total de técnicos encuestados	**7**

- **Pregunta 1** (¿La Institución dispone de servicio de Internet?)

Análisis: La gran cantidad de centros de estudio disponen del acceso al Internet, es por esta razón que es imprescindible instalar software o hardware como barreras para el libre acceso a la red (Véase figura 36).

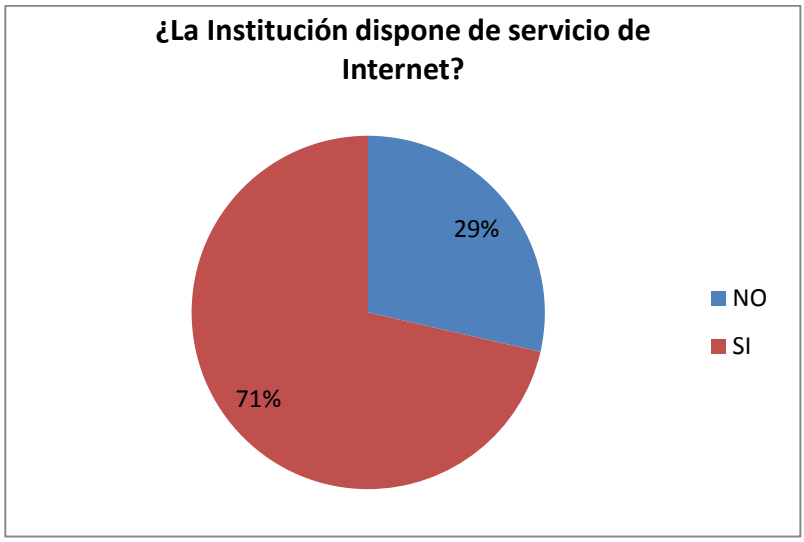


Figura 36. Acceso al Internet

- **Pregunta 2.** (Tipo de Institución)

Análisis: Las instituciones donde se realizó las encuestas fueron en privadas y públicas en su mayoría (Véase figura 37).

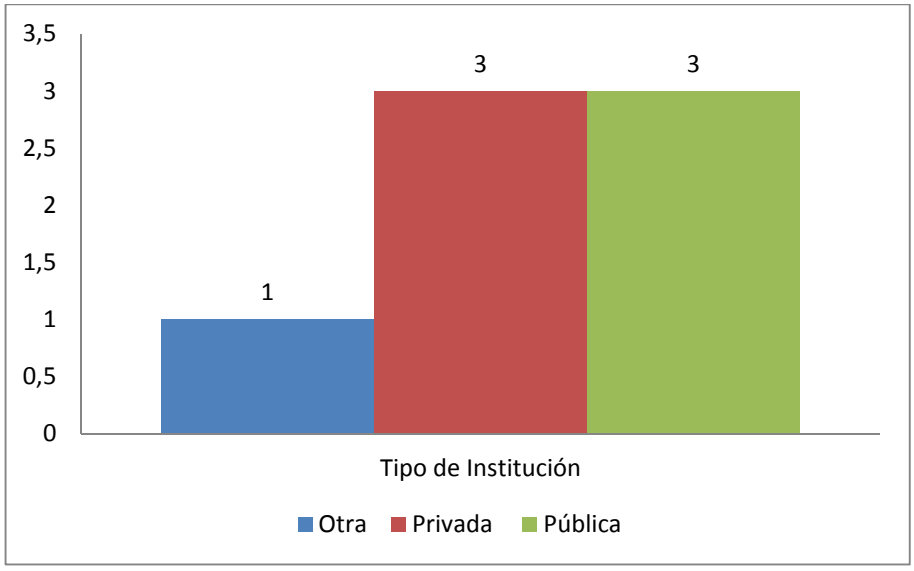


Figura 37. Tipo de Institución

- **Pregunta 3.** (Número de estudiantes en el plantel)

Análisis: Se puede aducir que la mayoría de centros de estudio son de gran afluencia, además de estos colegios analizados existen una gran cantidad con muchos más estudiantes que los mencionados (Véase figura 38).

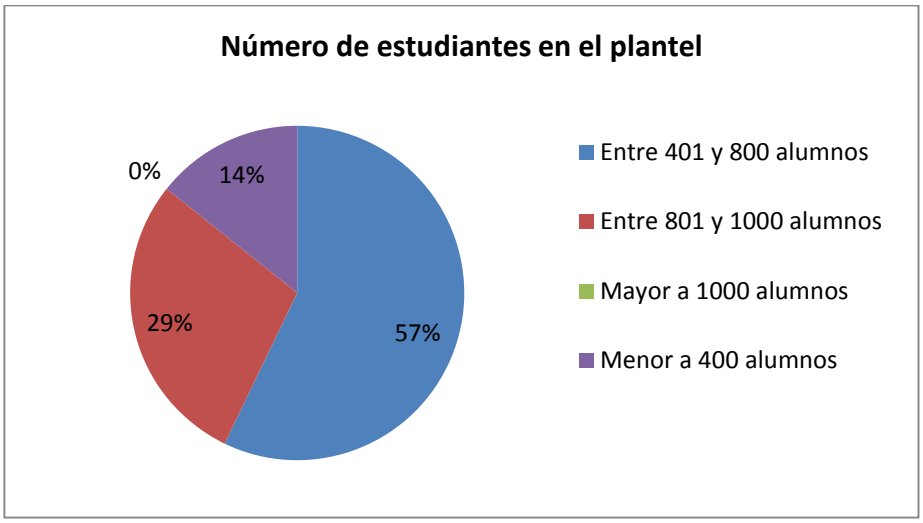


Figura 38. Cantidad de estudiantes

- **Pregunta 4. (**¿Con cuántos laboratorios de computación cuenta?)

Análisis: La mayoría de los colegios al menos tienen un laboratorio de computación, y esto variara de acuerdo a la cantidad de estudiantes con las que cuentan (Véase figura 39).

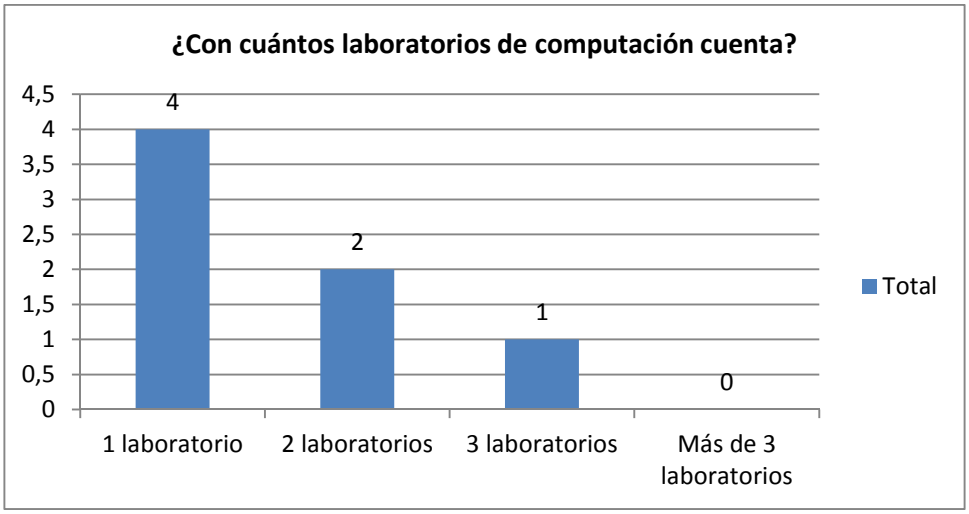


Figura 39. Cantidad de laboratorios

- **Pregunta 5.** (¿Cuántos computadores portátiles funcionales dispone?)

Análisis: Son pocas computadoras portátiles que tienen y en otros casos no disponen de ninguno (Véase figura 40).

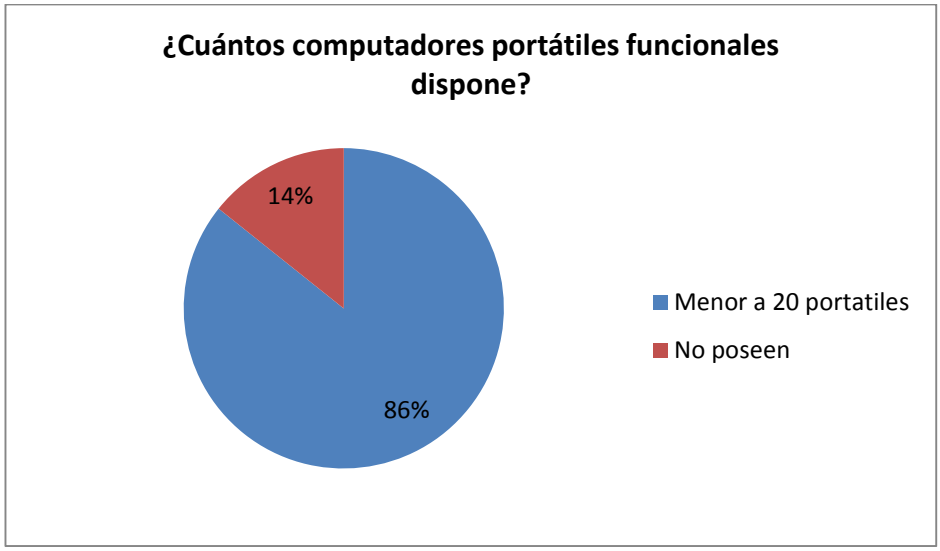


Figura 40. Cantidad de portátiles

- **Pregunta 6.** (¿Cuántos computadores de escritorio funcionales dispone?)

Análisis: La mayor cantidad de equipos que utilizan son los de escritorio, y esto variará de acuerdo a la cantidad de estudiantes (Véase figura 41).

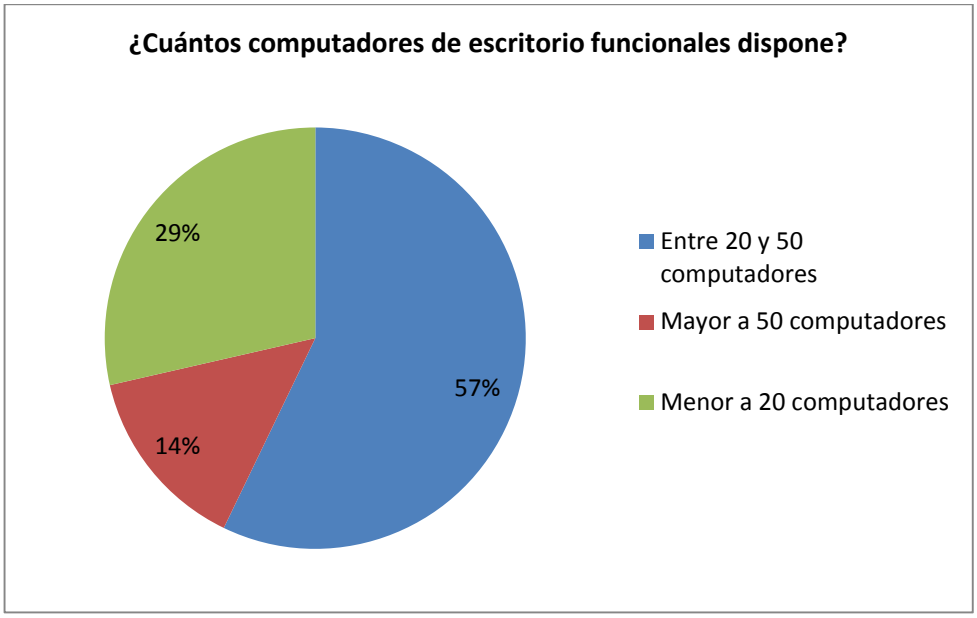


Figura 41. Cantidad de computadores de escritorio

- **Pregunta 7.** (¿Posee políticas de seguridad?)

Análisis: De las instituciones educativas menos de la mitad tiene políticas de seguridad, las cuales hoy en día deberían ser algo primordial para brindar mayor seguridad e los adolescentes (Véase figura 42).

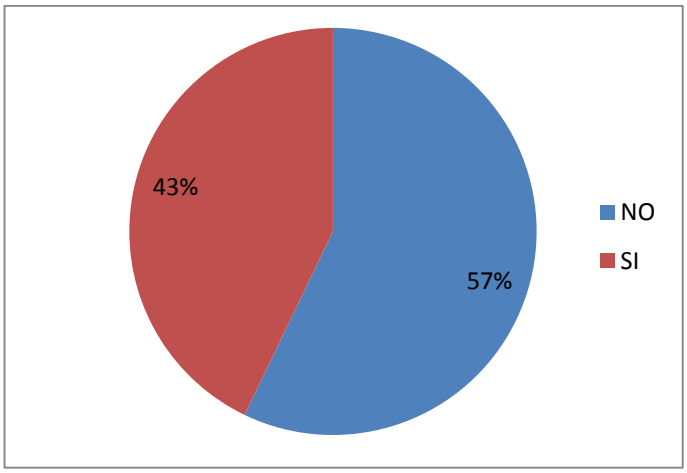


Figura 42. Políticas de Seguridad

- **Pregunta 8.** (¿Qué tipo de herramientas de seguridad tiene implementado?)

Análisis: En las Instituciones encuestadas es bueno saber que ninguna no tiene nada y lo que más se utiliza es Software (Véase figura 43).

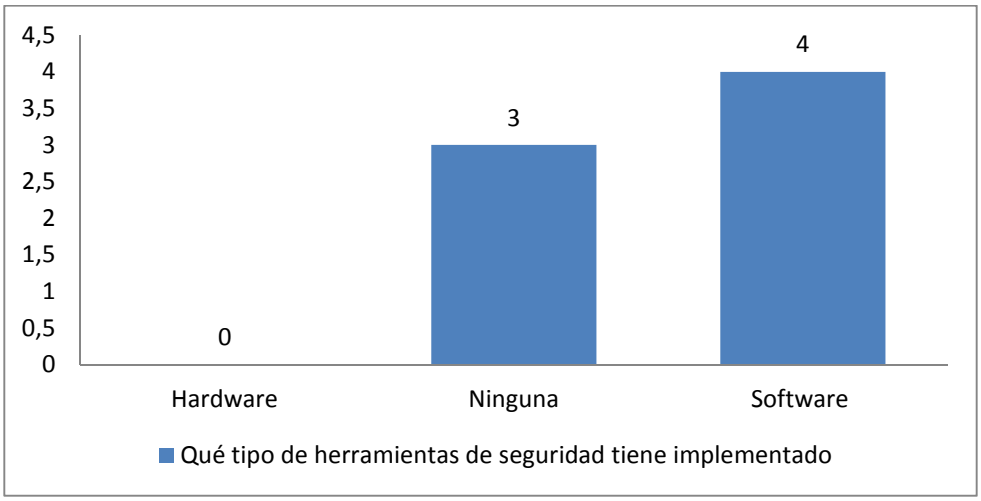


Figura 43. Herramientas de Seguridad

- **Pregunta 9.** (¿Bajo qué Sistema Operativo tiene configurado las seguridades informáticas?)

Análisis: Windows es el sistema Operativo ms utilizado para la configuración de seguridades, serio bueno analizar a nivel de centros de estudios cual opción es la más conveniente (Véase figura 44).

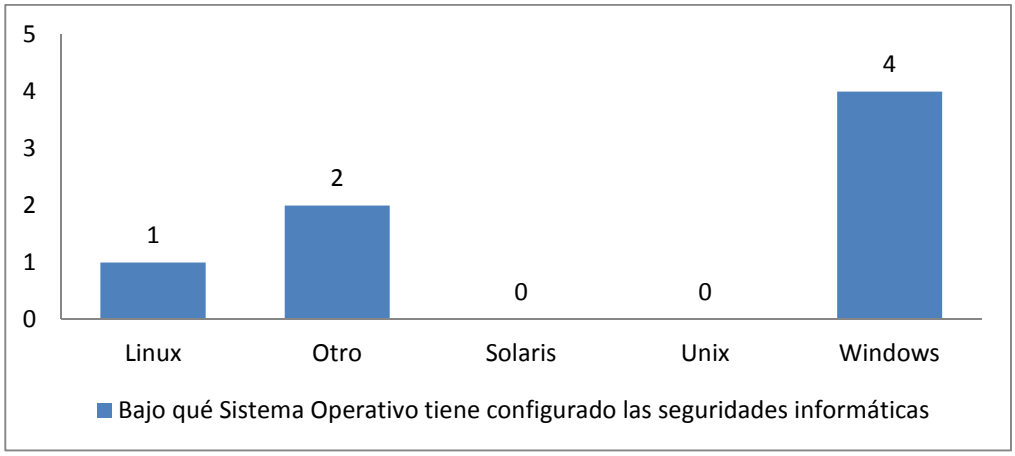


Figura 44. Sistema Operativo

- **Pregunta 10.** ¿Tiene creado perfiles de usuarios para la navegación?)

Análisis: La mayoría de las instituciones encuestadas tiene creados perfiles para acceder a navegar en Internet, es aconsejable de esta manera podemos diferenciar a que pueden acceder tanto los estudiantes, docentes, autoridades y si es posible invitados (Véase figura 45).

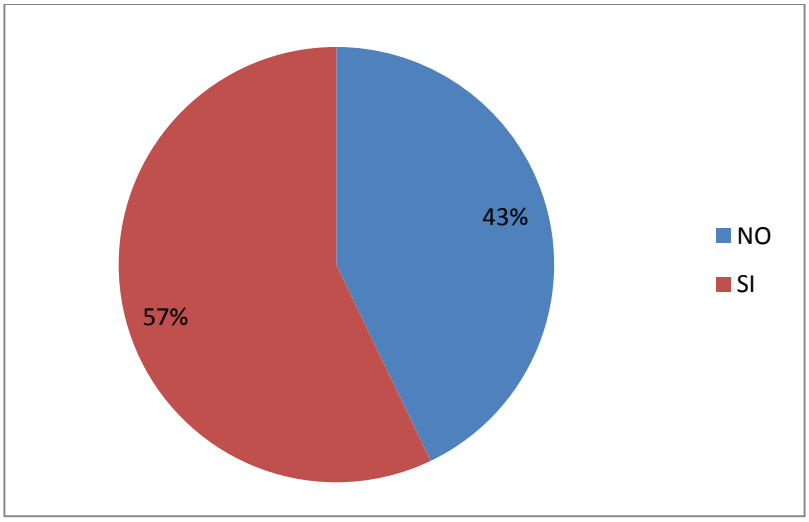


Figura 45. Perfiles de usuarios

- **Pregunta 13.** (¿Qué software, hardware o configuración para el control de seguridades tiene implementado?)

Análisis: Las instituciones pueden utilizar varias opciones para el control de seguridad en este caso una de los utilizados es el Firewall y Antispam. (Véase figura 46)

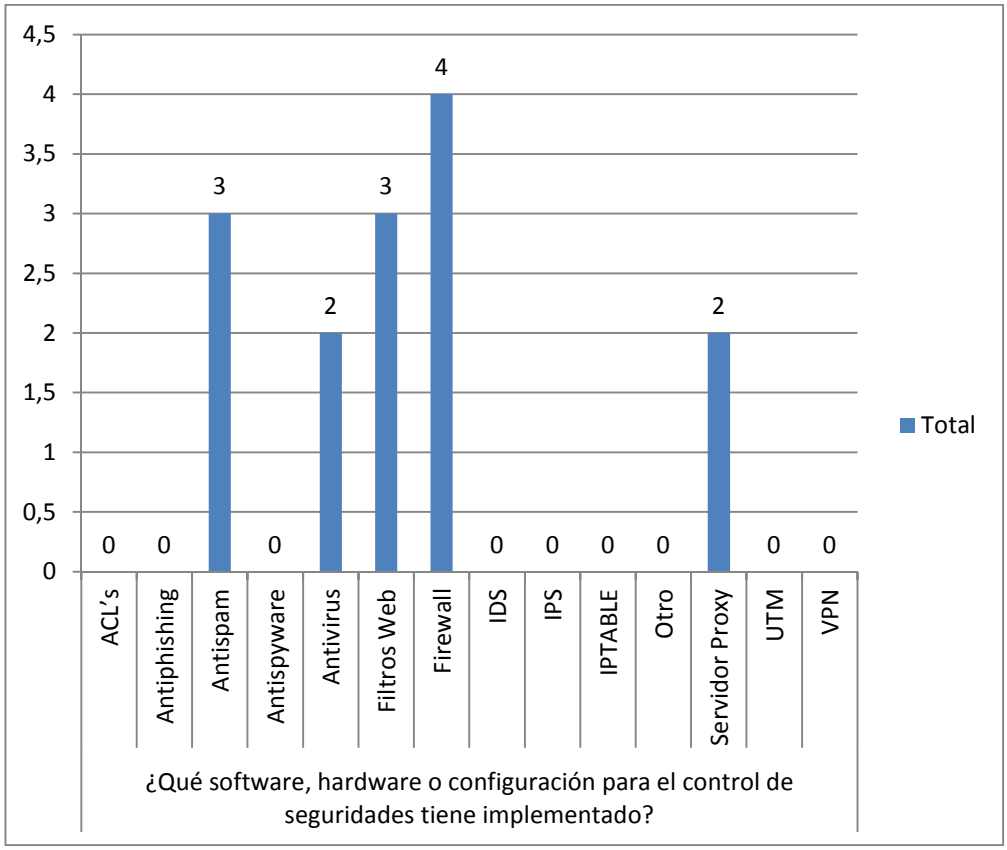


Figura 46. Tipos de control de seguridades

- **Pregunta 15.** (¿Qué tipos de páginas se encuentra bloqueadas?)

Análisis: En una buena cantidad de colegios se centran a bloquear las páginas de Pornografía, pero se debe considerar otros sitios que pueden ser de alto riesgo al cual están expuestos los alumnos (Véase figura 47).

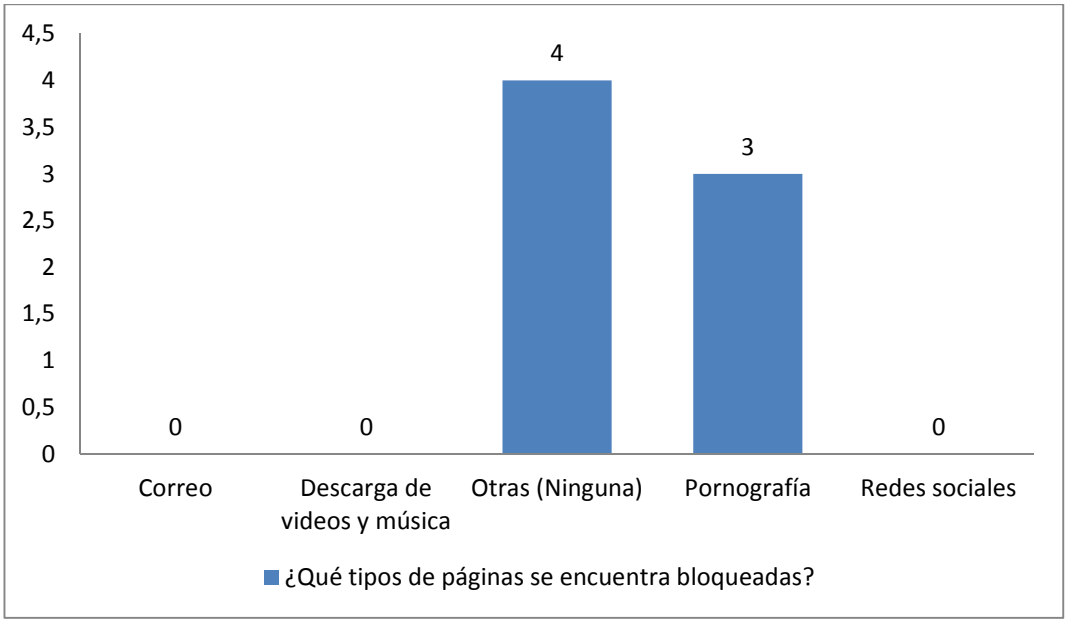


Figura 47. Páginas Bloqueadas

3.6 Evaluación de las herramientas de Control Parental.

El avance de la tecnología a costos accesibles ha provocado la proliferación del acceso al Internet en todos los lugares, vía cable y principalmente inalámbrica. Esto ha permitido el libre a acceso a cualquier tipo de información, sin ninguna restricción. En razón de esto existen muchas personas y organizaciones ya sean privadas o gubernamentales a nivel mundial se ha visto la necesidad de realizar el estudio, obteniendo como resultado varias herramientas (programas), que permiten el control de la navegación.

Luego de realizar un análisis de las diferentes herramientas, y la investigación de varios estudios se ha tomado como referencia el benchmarking efectuado por la Unión Europea sobre las aplicaciones de Control Parental, este estudio está basado en características como (funcionalidad, efectividad, usabilidad, seguridad, precio entre otros.). Además presenta un completo estudio con sus respectivas características de cada herramienta, el Ranking de las mejores aplicaciones en diferentes edades, se tomó como referencia el análisis de adolescentes de 13 años en adelante como muestra la siguiente figura 48.

La calificación que le otorga es dentro del rango de cero (0) a cuatro (4), donde el valor de 4 es cuando cumple la característica con mayor efectividad.

PARENTAL CONTROL TOOLS: GLOBAL RANKINGS for PC TOOLS

PC Tools ranking assessed for ≥ 13 years old users

Rank/21	Tool	Functionality	Effectiveness	Usabiliy	Security	Rating		Price € *
	Average across 21 tools	2,31	1,40	2,51	2,81	1,95		
	Best values	3,4	2,1	3,05	4,0	2,74		
1	PURESIGHT OWL	3,4	2,1	3,04	4	2,74		46,00
2	NORTON ONLINE FAMILY	1,8	1,9	3,05	4	2,43		FREE
3	TELEKOM KINDERSCHUTZ SOFTWARE	2,1	1,9	2,50	4	2,36		FREE**
4	NET NANNY	2,7	1,5	2,46	4	2,22		30,00
5	KASPERSKY PURE	3,4	1,5	2,69	3	2,21		60,00
6	TREND MICRO ONLINE GUARDIAN FOR FAMILIES	1,9	1,7	2,86	3	2,16		23,00
7	K9 WEB PROTECTION	1,6	1,6	2,56	4	2,16		FREE
8	PROFIL PARENTAL FILTER 2	3,4	1,4	2,44	3	2,11		39,99
9	SAFE EYES	3,0	1,2	2,39	4	2,09		38,00
10	MCAFEE FAMILY PROTECTION	2,7	1,2	2,30	4	2,03		36,95
11	F-SECURE INTERNET SECURITY 2012	1,3	1,7	2,52	3	2,01		49,95
12	WINDOWS LIVE FAMILY SAFETY	2,8	1,7	2,68	1	1,94		FREE
13	CYBERSIEVE	2,8	1,0	2,17	4	1,92		27,00
14	MAC OS X PARENTAL CONTROLS	2,4	1,0	2,60	3	1,80		FREE
15	AVG FAMILY SAFETY	2,5	1,3	2,83	1	1,72		14,95
16	MOBICIP	2,1	0,8	2,15	4	1,72		7,75
17	ENOLOGIC NET FILTER	1,5	1,5	2,23	1	1,57		40,00
18	CYBERSITTER	2,4	1,2	2,28	1	1,54		30,00
19	XOOLOO	1,5	1,3	2,47	1	1,51		29,99
20	CYBERPATROL	2,2	0,7	2,58	2	1,47		30,00
21	WHITENET	1,2	1,1	1,84	1	1,24		24,95

Figura 48. Las mejores herramientas de control parental[2]
Fuente, Benchmarking of parental control tools (SIP-BENCH)

3.6.1 Ranking de las mejores Herramientas

Existen programas de uso libre y privados que se encuentran al alcance del público, sin embargo no existe la cultura de protección en el Internet. Adicionalmente cabe indicar que las herramientas de Control de Acceso a Internet trae incluido un módulo de Control Parental incorporado, lo cual no es conocido por todos los usuarios. A continuación se presentan una leve explicación de las herramientas que han sido analizadas.

a. Puresight Owl:

PureSight Technologies Ltd. fue establecida en 1998 con la misión de proporcionar una herramienta de software en línea para el control de acceso. En la tabla 5 se puede observar sus características, esta herramienta se basa en dos tipos de tecnologías:

- **ACI Inspector de Chat Activo (Active Chat Inspector)** identifica y bloquea los contactos indeseables y discusiones potencialmente dañinos procedentes de acosadores cibernéticos.

[2] http://www.sipbench.eu/transfer/SIP_BENCHII_5th_cycle_ranking.pdf

- **ACR Reconocimiento contenido activo (Active Content Recognition)** clasifica de forma dinámica y bloquea los sitios web no deseados. (PureSight, 2010-2011).

Una investigación completa sobre la herramienta, lo realiza el SIP-BENCH III, en su estudio realizado tomando en cuenta la funcionalidad, Eficacia, Usabilidad y Seguridad.

Tabla 5.

Características de la herramienta Puresight Owl

Sistemas Operativos	**Windows Vista (32/64 bit)** **Windows XP (32/64 bit)** **Windows 7 (32/64 bit)**
Precio (Licencia de un año)	1 equipo: $ 5.99 por mes 2 equipos: $ 3.99 por cada mes y equipo 3 equipos: $ 2.99 por cada mes y equipo 4 equipos: $ 2.29 por cada mes y equipo 10 equipos: $ 0.99 por cada mes y equipo
Funcionalidad	Existen varios tipos de opciones de personalización en el manejo y presentación de reportes, permite bloquear redes sociales, alertas de intentos de violaciones.
Usabilidad	El proceso de instalación es comprensible, con excepción del idioma. Ofrece varias opciones para ser individualizadas y posibilidades de influir en la cantidad de información sobre el proceso.

Además es una herramienta para sistemas operativos de Microsoft, para su adquisición se debe cancel un costo es uno de los mejores renqueados según los estudios de realiza el SIP-BENCH III. (SIP-BENCH, 2013)

b. Norton Online Family

Symantec fundada en 1982, reconocida en seguridad, almacenamiento y soluciones de gestión de sistemas. Norton Online Family, permite supervisar y filtrar contenido web únicamente, en la siguiente tabla 6 se presentan las características de esta herramienta. (Symantec, 2013)

Tabla 6.

Características de la herramienta Norton Online Family

Sistemas Operativos	**Microsoft Windows XP (32 bit)** **Microsoft Windows Vista (32/64 bit)** **Microsoft Windows 7 (32/64bit)** **Mac 10.6, Snow Leopard / 10.7, Lion** **Mac OS X 10.5(PowerPC o Intel)** **Mac OS X 10.6(Intel)** **Mac OS X 10.7**
Precio (Licencia de un año)	Gratuito (Limitado)
Funcionalidad	Rastrea las palabras y las frases que buscan los adolescentes en línea. Presenta informes del contenido inadecuado o bloqueado que ha sido buscado.
Usabilidad	La instalación es corta y sencilla, presenta pocas opciones de configuración en la versión gratuita.

Esta herramienta se la puede instalar bajo Windows y MAC, su distribución es gratuita y en varios idiomas, es una de las mejores según lo describe el SIP-BENCH III. (SIP-BENCH, 2013)

c. Whitenet

WhiteNet SIA, ha sido creado por los programadores de software de Letonia. Está basado en el análisis de la lista negra (sitios web con contenidos nocivos, el filtro compara la dirección de la página web en la "Lista Negra", denegando el acceso) y/o una lista blanca (lista de sitios web sin contenidos nocivos), en la siguiente tabla se puede observar sus características. (SIP-BENCH, 2013)

Tabla 7.

Características de la herramienta WhiteNet

Sistemas Operativos	**Windows XP (32-bit)** **Windows Vista (32-bit)** **Windows 7 (32-bit)***
Precio (Licencia de un año)	$ 29
Funcionalidad	Fácil instalación y no requiere de configuración adicional
Usabilidad	Al ingresar a páginas con contenido indeseado estas se cierran automáticamente.

d. K9 Protectión

Es un software gratuito con el cual permite filtrar la información que ingresa a la PC mediante de 60 categorías en las que tiene clasificado el contenido (no es un antivirus). Su origen es Canadiense.

Además es un software de control parental (bloquea, restringe o filtra el acceso a determinada información no apta para menores de edad), es útil en el computador de casa se lo puede utilizar bajo Windows o Mac OS. K9 le da el control de la Internet para que pueda proteger a los adolescentes, en la tabla 8 se pueden observar las características de esta herramienta. (K9 Web Protection, 2013).

Tabla 8.

Características de la herramienta K9 Protection

Sistemas Operativos	**Microsoft Windows XP (32 bit)** **Microsoft Windows Vista (32/64 bit)** **Microsoft Windows 7 (32/64bit)** **Mac** **Android**
Precio (Licencia de un año)	Gratuito (Limitado)
Funcionalidad	Bloquea sitios con la opción de personalizar un horario, categorizar
Usabilidad	Para su uso se debe solicitar una clave facilitada por la empresa fabricante, dicha clave es gratuita y se le solicitara al instalar el programa.

K9 dentro de su configuración para Control Parental tiene los siguientes aspectos:

- Bloquear sitios web en más de 70 categorías, incluyendo la pornografía, juegos de azar, las drogas, la violencia / odio / racismo, malware / spyware, phishing.
- Fuerza SafeSearch en todos los principales motores de búsqueda.
- Establecer restricciones de tiempo para bloquear el acceso a la web durante horas designadas.
- Configurar listas personalizadas de "permitir siempre".
- Reemplazar un bloque de la página web con contraseña.

- Ver informes fáciles de supervisar y controlar la actividad web.
- Categorización en tiempo real de nuevos adultos y sitios maliciosos.

K9 es una de las herramientas más completas que existen para Windows, MAC y Android, su interfaz es en Ingles, vía Web y si lo utiliza en casa es gratuito. (SIP-BENCH)

e. Amigo

Esta aplicación permite ver el registro de la navegación y las conversaciones, de igual manera también almacena lo que se ve en la pantalla en todo momento para que posteriormente se pueda comprobar cuáles son las actividades que han realizado los niños y adolescentes en el Internet, permitiendo obtener un historial de lo que ha escrito y lo que ha leído. La aplicación permite filtrar aplicaciones y contenidos Web, como característica principal no muestra rastros visibles de su ejecución.

3.6.2 Benchmarking para el grupo de edad trece años y mayores

A continuación se muestra la comparación a partir del análisis cuantitativo de varias herramientas tomando en cuenta su funcionalidad, eficacia, usabilidad, seguridad y precio (SIP-BENCH). Las figuras del 49 al 54 muestran el ranking en los distintos criterios de comparación que se describen:

- **Funcionalidad:** Se evalúa que las funcionalidades de la herramienta con éxito proporcionan. ¿La herramienta tiene la funcionalidad que necesita?; por ejemplo ¿es posible bloquear el acceso a las redes sociales?; es posible tener un filtrado para su hijo de 7 años de edad o de 16 años.
- **Seguridad:** Se evalúa la resistencia a los intentos de las herramientas de los usuarios de by-pass por medio de acciones concretas. ¿Es fácil o difícil para su hijo para desinstalar o pueda pasar por las herramientas y acceder a Internet libremente?
- **Eficacia:** Mide cantidad de contenido nocivo que bloquea la herramienta y cuanto contenido no perjudicial lo permite. ¿Las herramientas bloquean el 50%, 75% o 90% de los sitios web pornográficos/violentos? ¿La herramienta

permita que su hijo visite sitios web aceptables? ¿La herramienta permite que su hijo visite sitios web aceptables?

- **Usabilidad:** Evalúa si puede ser fácilmente instalado, configurado, utilizado y mantenido por un promedio de usuarios ¿Será fácil / difícil / imposible de instalar y configurar la herramienta? La calificación es entre cero (0) y cuatro (4), tomando en cuenta que 4 es de mejor cumplimiento la característica analizada.

POR SU FUNCIONALIDAD

Tool name	Functionality	Effectiveness	Usability	Security	Overallsc	Price(€)
PureSight Owl	3.41	2.1	3.04	4	2.74	46.00
Kaspersky Pure	3.41	1.5	2.69	3	2.21	60.00
Profil Parental Filter 2	3.41	1.4	2.44	3	2.11	39.99
Safe Eyes	2.96	1.2	2.39	4	2.09	38.00
Windows Family Safety	2.81	1.7	2.68	1	1.94	Free
Cybersieve	2.81	1	2.17	4	1.92	27.00
Net Nanny	2.67	1.5	2.46	4	2.22	30.00
McAfee Family Protection	2.67	1.2	2.3	4	2.03	36.95
AVG Family Safety	2.52	1.3	2.83	1	1.72	14.95
Mac OS X Parental Controls	2.37	1	2.6	3	1.80	Free
Cybersitter	2.37	1.2	2.28	1	1.54	30.00
CyberPatrol	2.22	0.7	2.58	2	1.47	30.00
Telekom Kinderschutz Software *	2.07	1.9	2.5	4	2.36	Free
Mobicip	2.07	0.8	2.15	4	1.72	7.75
Trend Micro Online Guardian	1.93	1.7	2.86	3	2.16	23.00
Norton Online Family	1.78	1.9	3.05	4	2.43	Free
K9 Web Protection	1.63	1.6	2.56	4	2.16	Free
Enologic Net Filter	1.48	1.5	2.23	1	1.57	40.00
Xooloo	1.48	1.3	2.47	1	1.51	29.99
F-Secure Internet Security	1.33	1.7	2.52	3	2.01	49.95
Whitenet	1.19	1.1	1.84	1	1.24	24.95

Figura 49. Herramientas de Control por funcionalidad
Fuente, Benchmarking of parental control tools (SIP-BENCH)

POR SU EFICACIA

Tool name	Functionality	Effectiveness	Usability	Security	Overallsc	Price(€)
PureSight Owl	3.41	2.1	3.04	4	2.74	46.00
Norton Online Family	1.78	1.9	3.05	4	2.43	Free
Telekom Kinderschutz Software *	2.07	1.9	2.5	4	2.36	Free
Trend Micro Online Guardian	1.93	1.7	2.86	3	2.16	23.00
F-Secure Internet Security	1.33	1.7	2.52	3	2.01	49.95
Windows Family Safety	2.81	1.7	2.68	1	1.94	Free
K9 Web Protection	1.63	1.6	2.56	4	2.16	Free
Net Nanny	2.67	1.5	2.46	4	2.22	30.00
Kaspersky Pure	3.41	1.5	2.69	3	2.21	60.00
Enologic Net Filter	1.48	1.5	2.23	1	1.57	40.00
Profil Parental Filter 2	3.41	1.4	2.44	3	2.11	39.99
AVG Family Safety	2.52	1.3	2.83	1	1.72	14.95
Xooloo	1.48	1.3	2.47	1	1.51	29.99
Safe Eyes	2.96	1.2	2.39	4	2.09	38.00
McAfee Family Protection	2.67	1.2	2.3	4	2.03	36.95
Cybersitter	2.37	1.2	2.28	1	1.54	30.00
Whitenet	1.19	1.1	1.84	1	1.24	24.95
Cybersieve	2.81	1	2.17	4	1.92	27.00
Mac OS X Parental Controls	2.37	1	2.6	3	1.80	Free
Mobicip	2.07	0.8	2.15	4	1.72	7.75
CyberPatrol	2.22	0.7	2.58	2	1.47	30.00

* Telekom Kinderschutz Software is free for Telekom customers.

Figura 50. Herramientas de Control por eficiencia
Fuente, Benchmarking of parental control tools (SIP-BENCH)

POR SU USABILIDAD

Tool name	Functionality	Effectiveness	Usability	Security	Overallsc	Price(€)
Norton Online Family	1.78	1.9	3.05	4	2.43	Free
PureSight Owl	3.41	2.1	3.04	4	2.74	46.00
Trend Micro Online Guardian	1.93	1.7	2.86	3	2.16	23.00
AVG Family Safety	2.52	1.3	2.83	1	1.72	14.95
Kaspersky Pure	3.41	1.5	2.69	3	2.21	60.00
Windows Family Safety	2.81	1.7	2.68	1	1.94	Free
Mac OS X Parental Controls	2.37	1	2.6	3	1.80	Free
CyberPatrol	2.22	0.7	2.58	2	1.47	30.00
K9 Web Protection	1.63	1.6	2.56	4	2.16	Free
F-Secure Internet Security	1.33	1.7	2.52	3	2.01	49.95
Telekom Kinderschutz Software *	2.07	1.9	2.5	4	2.36	Free
Xooloo	1.48	1.3	2.47	1	1.51	29.99
Net Nanny	2.67	1.5	2.46	4	2.22	30.00
Profil Parental Filter 2	3.41	1.4	2.44	3	2.11	39.99
Safe Eyes	2.96	1.2	2.39	4	2.09	38.00
McAfee Family Protection	2.67	1.2	2.3	4	2.03	36.95
Cybersitter	2.37	1.2	2.28	1	1.54	30.00
Enologic Net Filter	1.48	1.5	2.23	1	1.57	40.00
Cybersieve	2.81	1	2.17	4	1.92	27.00
Mobicip	2.07	0.8	2.15	4	1.72	7.75
Whitenet	1.19	1.1	1.84	1	1.24	24.95

* Telekom Kinderschutz Software is free for Telekom customers.

Figura 51. Herramientas de Control por usabilidad
Fuente, Benchmarking of parental control tools (SIP-BENCH)

POR EL NIVEL DE SEGURIDAD

Tool name	Functionality	Effectiveness	Usability	Security	Overallsc	Price(€)
PureSight Owl	3.41	2.1	3.04	4	2.74	46.00
Norton Online Family	1.78	1.9	3.05	4	2.43	Free
Telekom Kinderschutz Software *	2.07	1.9	2.5	4	2.36	Free
Net Nanny	2.67	1.5	2.46	4	2.22	30.00
K9 Web Protection	1.63	1.6	2.56	4	2.16	Free
Safe Eyes	2.96	1.2	2.39	4	2.09	38.00
McAfee Family Protection	2.67	1.2	2.3	4	2.03	36.95
Cybersieve	2.81	1	2.17	4	1.92	27.00
Mobicip	2.07	0.8	2.15	4	1.72	7.75
Kaspersky Pure	3.41	1.5	2.69	3	2.21	60.00
Trend Micro Online Guardian	1.93	1.7	2.86	3	2.16	23.00
Profil Parental Filter 2	3.41	1.4	2.44	3	2.11	39.99
F-Secure Internet Security	1.33	1.7	2.52	3	2.01	49.95
Mac OS X Parental Controls	2.37	1	2.6	3	1.80	Free
CyberPatrol	2.22	0.7	2.58	2	1.47	30.00
Windows Family Safety	2.81	1.7	2.68	1	1.94	Free
AVG Family Safety	2.52	1.3	2.83	1	1.72	14.95
Enologic Net Filter	1.48	1.5	2.23	1	1.57	40.00
Cybersitter	2.37	1.2	2.28	1	1.54	30.00
Xooloo	1.48	1.3	2.47	1	1.51	29.99
Whitenet	1.19	1.1	1.84	1	1.24	24.95

* Telekom Kinderschutz Software is free for Telekom customers.

Figura 52. Herramientas de Control por seguridad
Fuente, Benchmarking of parental control tools (SIP-BENCH)

POR EL OVERALLSO

Tool name	Functionality	Effectiveness	Usability	Security	Overallsc	Price(€)
AVG Family Safety	2.52	1.3	2.83	1	1.72	14.95
CyberPatrol	2.22	0.7	2.58	2	1.47	30.00
Cybersieve	2.81	1	2.17	4	1.92	27.00
Cybersitter	2.37	1.2	2.28	1	1.54	30.00
Enologic Net Filter	1.48	1.5	2.23	1	1.57	40.00
F-Secure Internet Security	1.33	1.7	2.52	3	2.01	49.95
K9 Web Protection	1.63	1.6	2.56	4	2.16	Free
Kaspersky Pure	3.41	1.5	2.69	3	2.21	60.00
Mac OS X Parental Controls	2.37	1	2.6	3	1.80	Free
McAfee Family Protection	2.67	1.2	2.3	4	2.03	36.95
Mobicip	2.07	0.8	2.15	4	1.72	7.75
Net Nanny	2.67	1.5	2.46	4	2.22	30.00
Norton Online Family	1.78	1.9	3.05	4	2.43	Free
Profil Parental Filter 2	3.41	1.4	2.44	3	2.11	39.99
PureSight Owl	3.41	2.1	3.04	4	2.74	46.00
Safe Eyes	2.96	1.2	2.39	4	2.09	38.00
Telekom Kinderschutz Software *	2.07	1.9	2.5	4	2.36	Free
Trend Micro Online Guardian	1.93	1.7	2.86	3	2.16	23.00
Whitenet	1.19	1.1	1.84	1	1.24	24.95
Windows Family Safety	2.81	1.7	2.68	1	1.94	Free
Xooloo	1.48	1.3	2.47	1	1.51	29.99

* Telekom Kinderschutz Software is free for Telekom customers.

Figura 53. Herramientas de Control por overallso
Fuente, Benchmarking of parental control tools (SIP-BENCH)

POR EL COSTO

Tool name	Functionality	Effectiveness	Usability	Security	Overallsc	Price(€)
Norton Online Family	1.78	1.9	3.05	4	2.43	Free
Telekom Kinderschutz Software *	2.07	1.9	2.5	4	2.36	Free
K9 Web Protection	1.63	1.6	2.56	4	2.16	Free
Windows Family Safety	2.81	1.7	2.68	1	1.94	Free
Mac OS X Parental Controls	2.37	1	2.6	3	1.80	Free
Mobicip	2.07	0.8	2.15	4	1.72	7.75
AVG Family Safety	2.52	1.3	2.83	1	1.72	14.95
Trend Micro Online Guardian	1.93	1.7	2.86	3	2.16	23.00
Whitenet	1.19	1.1	1.84	1	1.24	24.95
Cybersieve	2.81	1	2.17	4	1.92	27.00
Xooloo	1.48	1.3	2.47	1	1.51	29.99
Net Nanny	2.67	1.5	2.46	4	2.22	30.00
Cybersitter	2.37	1.2	2.28	1	1.54	30.00
CyberPatrol	2.22	0.7	2.58	2	1.47	30.00
McAfee Family Protection	2.67	1.2	2.3	4	2.03	36.95
Safe Eyes	2.96	1.2	2.39	4	2.09	38.00
Profil Parental Filter 2	3.41	1.4	2.44	3	2.11	39.99
Enologic Net Filter	1.48	1.5	2.23	1	1.57	40.00
PureSight Owl	3.41	2.1	3.04	4	2.74	46.00
F-Secure Internet Security	1.33	1.7	2.52	3	2.01	49.95
Kaspersky Pure	3.41	1.5	2.69	3	2.21	60.00

* Telekom Kinderschutz Software is free for Telekom customers.

Figura 54. Herramientas de Control por el costo
Fuente, Benchmarking of parental control tools (SIP-BENCH)

3.7 Análisis de la línea base

En la tabla 9 se presentan las 21 herramientas que han sido analizadas indicando su ponderación en las diferentes características.

Tabla 9.

Cuadro de análisis

	Average across 21 tools	2.31	1.4	2.51	2.81	1.95
	Best values	**3.4**	**2.1**	**3.05**	**4**	**2.74**
1	PURESIGHT OWL	3.4	2.1	3.04	4	2.74
2	NORTON ONLINE FAMILY	1.8	1.9	3.05	4	2.43
3	TELEKOM KINDERSCHUTZ SOFTWARE	2.1	1.9	2.5	4	2.36
4	NET NANNY	2.7	1.5	2.46	4	2.22
5	KASPERSKY PURE	3.4	1.5	2.69	3	2.21
6	TREND MICRO ONLINE GUARDIAN FOR FAMILIES	1.9	1.7	2.86	3	2.16
7	K9 WEB PROTECTION	1.6	1.6	2.56	4	2.16
8	PROFIL PARENTAL FILTER 2	3.4	1.4	2.44	3	2.11
9	SAFE EYES	3	1.2	2.39	4	2.09
10	MCAFEE FAMILY PROTECTION	2.7	1.2	2.3	4	2.03
11	F-SECURE INTERNET SECURITY 2012	1.3	1.7	2.52	3	2.01
12	WINDOWS LIVE FAMILY SAFETY	2.8	1.7	2.68	1	1.94
13	CYBERSIEVE	2.8	1	2.17	4	1.92
14	MAC OS X PAENTAL CONTROLS	2.4	1	2.6	3	1.8
15	AVG FAMILY SAFETY	2.5	1.3	2.83	1	1.72
16	MOBICIP	2.1	0.8	2.15	4	1.72
17	ENOLOGIC NET FILTER	1.5	1.5	2.23	1	1.57
18	CYBERSITTER	2.4	1.2	2.28	1	1.54
19	XOOLOO	1.5	1.3	2.47	1	1.51
20	CIBERPATROL	2.2	0.7	2.58	2	1.47
21	WHITENET	1.2	1.1	1.84	1	1.24

Con un rango establecido de 1 a 4 para la calificación, se establece que ninguna de las 21 herramientas probadas alcanza la cobertura de la funcionalidad completa. La más completa tiene 3,4; 7 herramientas están clasificadas bajo 2. Los 3 productos de más alta puntuación son: KASPERSKY PURE (3,4), Profil Parental Filter 2 (3,4) y PureSight OWL (3,4). La figura 55 presenta gráficamente cada herramienta y su ponderación por cada característica evaluada. La tabla 10 presenta un análisis basado en las características para el control de accesos.

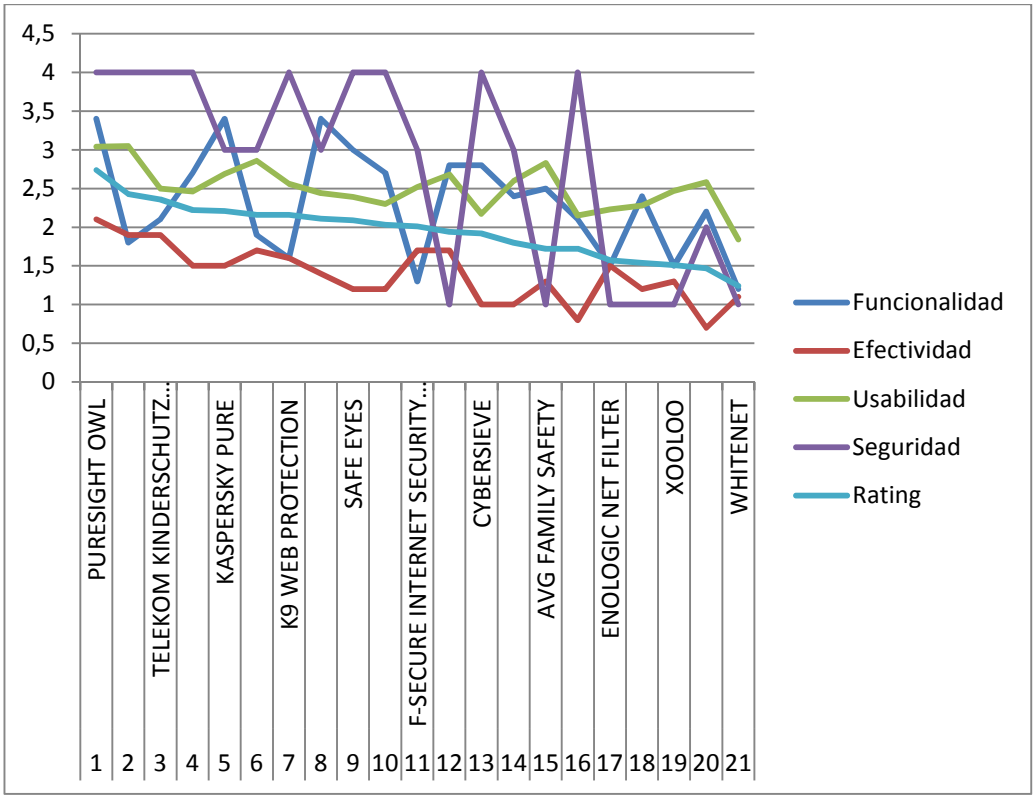


Figura 55. Análisis gráfico

Tabla 10.

Análisis de Control de acceso

CUADRO DE ANALISIS PARA CONTROL DE ACCESO	
Personalización de filtrado de contenidos Web	La mayor parte de las herramientas que nos proporcionan el control Parental y todas las funcionalidades completas (tema + de URL y listas negras / blancas). 8 de las 21 herramientas ofrecen esta opción. 16 herramientas dan la posibilidad de bloquear el acceso a redes sociales y 12 herramientas dan la posibilidad de obligar al usuario utilizar la funcionalidad de seguridad en los motores de búsqueda
Protocolos y Aplicaciones	Las herramientas rara vez proporcionan la opción de bloquear un protocolo por completo, mientras que las aplicaciones de bloqueo son más comunes.
Gestión de perfiles de usuarios	La mayor parte de las herramientas que permiten a los padres para crear y gestionar diferentes perfiles de usuarios con diferentes necesidades. 2 herramientas se pueden utilizar solamente con un perfil.
La restricción de acceso a la Web	18 herramientas permiten a los padres bloquear el acceso a Internet (ya sea utilizando una funcionalidad específica o el uso de las "restricciones de tiempo").

Continua →

Streaming	La mayoría de las herramientas son capaces de bloquear la transmisión basada en web proporcionado por YouTube, si no con una opción específica, al menos por su inclusión en una lista negra. El bloqueo de la aplicación específica que permite el streaming, como Windows Media Player es posible menos de la mitad de las herramientas.
Las actividades de comunicación	17 herramientas son capaces de bloquear MSN Messenger y 15 son capaces de bloquear de Skype.
	Posibilidad de filtrar los contactos es todavía es escasa: sólo 4 herramientas proporcionan una funcionalidad que funciona correctamente para MSN. Si las herramientas son capaces de bloquear Skype y / o MSN, bloquean con respecto a toda la aplicación y no es posible limitar el bloqueo de Voip o sólo de chat de vídeo.
Monitoreo	La mayoría de las herramientas son capaces de proporcionar a los padres una notificación por lo menos básico de la actividad web de los usuarios (páginas web o violaciones visitados). Algunos de ellos también ofrecen alertas específicas con violaciones y un informe más detallado. Hay pocas herramientas capaces de informar sobre el uso de protocolos / aplicaciones. 10 herramientas son capaces de controlar MSN, sólo 4 herramientas dan la información a los padres sobre la actividad de sus hijos en las redes sociales, mientras que ninguna herramienta es capaz de proporcionar información sobre el número y los nombres de los archivos descargados a través de Peer to Peer aplicaciones (por ejemplo: eMule o BitTorrent).
Interacción	Sólo 8 herramientas dan la posibilidad a los PADRES para personalizar la página de bloqueo. Ninguna de las herramientas redirige el NIÑO / ADOLESCENTE para una investigación segura.
Idioma de la Interfaz	Inglés es el idioma más frecuente, mientras que la elección de las herramientas está limitada para muchos otros idiomas europeos.
Seguridad	Algunas herramientas presentan algunas debilidades de seguridad. El más común es: permitir el acceso a una página no permitida a través de sitios de traducción o Google Cache. Pocas herramientas se pueden desinstalar sin una contraseña.

3.8 Consideraciones generales para el Control Parental

Con el fin de dotar de lineamientos para poder establecer el control parental se detalla a continuación algunas recomendaciones:

1. Educar a los niños desde una edad temprana y además comuniquen a sus padres, tutores o profesores de situaciones que sean extrañas de comportamientos de otras personas.
2. Indicarles a las personas integrantes de los hogares, que no se debe proporcionar información como fotografías, documentos entre otros, sobre la familia.
3. Establecer claramente la diferencia entre la realidad y la fantasía, esto en cuanto a personas que se tiene contacto físico como a personas que se los conoce mediante las redes sociales.
4. Colocar el computador en un lugar que sea de fácil acceso a cualquier miembro de la familia, y se pueda tener un control visual cuando el adolecente este utilizando.
5. Enseñar a los adolescentes de que todo lo que se encuentra en el Internet no es información valida, ya que no existe en su mayoría un responsable y se protegen en el anonimato, es necesario tomar información en el cual tenga una persona o empresa responsable.
6. Indicar a los adolecente que no es una buena práctica descargar programas desconocidos, además cual es sus función, ya que pueden descargarse virus, gusanos que pueden dañarán el equipo y la información del equipo.
7. Se puede realizar un seguimiento de acciones que realiza el adolecente cuando se encuentra en el computador.
8. Cuando los estudiantes ingresan a los laboratorios de computación deben tener claro las normativas que la institución deberá establecer en el buen uso de los equipos y el buen comportamiento, además es imprescindible que se disponga de software de filtrado de contenido.

3.9 Conclusiones

Dentro de este capítulo se presentó el análisis y resultados que se obtuvieron de las encuestas realizadas a niños y adolescentes que se encuentran entre las edades de 11 a 17 años. Se determinó que todos los encuestados tienen acceso a Internet, en donde solo el 26% de los encuestados afirman que son monitoreados por un adulto. Hay que tomar en cuenta que el 100% de las personas que dijeron tener Internet en el hogar tienen el Sistema Operativo Windows en diferentes versiones. Adicionalmente se analizó el benchmarking presentado por la Unión Europea que se basa en funcionalidad, eficacia, usabilidad, seguridad y precio.

CAPÍTULO IV. PROPUESTA PARA MITIGAR EL ACCESO A CONTENIDO INAPROPIADO

4.1 Introducción

El presente capítulo define la propuesta para el control de accesos a páginas Web que se ha venido desarrollando (véase la sección 4.2), explica las fases de diseño e implementación utilizando la metodología OOHDM (véase la sección 4.3, 4.4 y 4.5). Ahí se presenta cada uno de los casos de uso que intervienen en esta propuesta, adicional se presenta el algoritmo Procesamiento Natural (véase la sección 4.7), y finalmente se presenta la obtención de resultados y la contrastación de la hipótesis.

4.2 Propuesta

De acuerdo al estudio realizado se encontró la problemática de acceso a Internet sin restricciones en un alto porcentaje por parte de los niños y adolescentes. Además el mayor número de equipos utilizados tienen el Sistema Operativo Windows de Microsoft tanto en los hogares, centros de cómputo de las instituciones educativas y centros de cómputo públicos.

En base a las encuestas realizadas se determina que la falta de control se debe al desconocimiento de las herramientas existentes en el mercado. De igual manera la configuración de estas herramientas son complejas para los usuarios que no manejan la tecnología, por tal motivo se ve la necesidad de desarrollar una aplicación que ayude al control de la navegación en el sistema operativo Windows que sea de fácil instalación y manejo.

Para el diseño e implementación de este programa se ha escogido la metodología de diseño de hipermedia, orientado a objetos (OOHDM), que usa técnicas de representación gráfica de relaciones entre objetos y de contextos navegacionales. Esta metodología se basa en cinco etapas: determinación de requerimientos, diseño conceptual, diseño navegacional, diseño abstracto de interface e implementación. Adicionalmente se implementa un algoritmo basado en el Procesamiento de Lenguaje Natural para la búsqueda de palabras almacenadas.

La herramienta de desarrollo que se eligió fue Punto Net, por ser compatible con el Sistema Operativo Windows, como base de datos para el servicio entregado fue PostgresSQL, y la conexión entre el servicio Windows (demonio) de cada cliente y la base de datos se realizó a través de Web Service. En la figura 56 se puede observar la arquitectura que se utilizó en el proyecto.

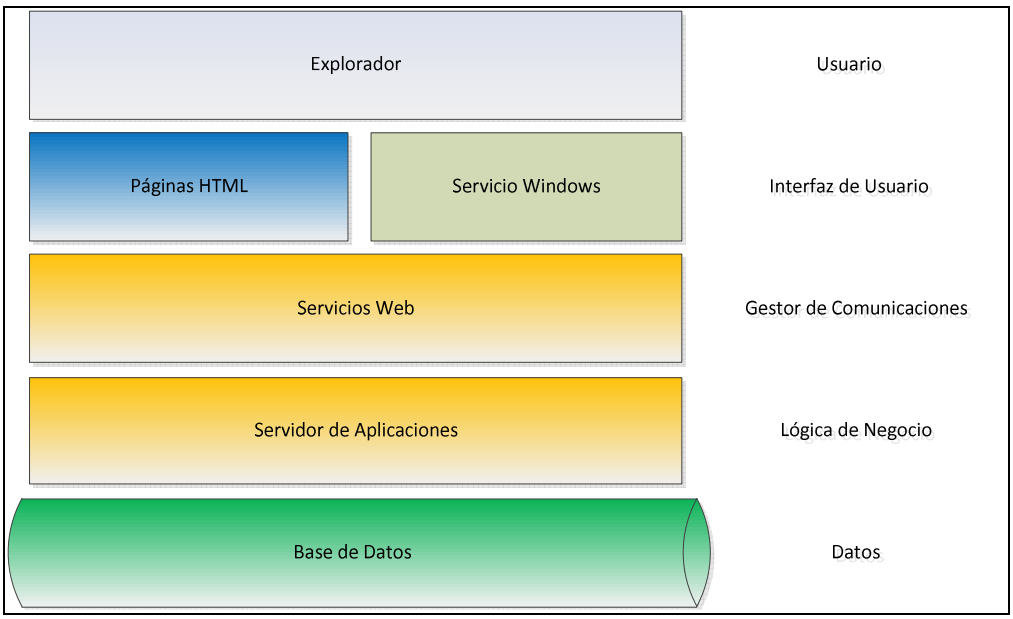


Figura 56. Arquitectura del proyecto Control Parental

4.3 Determinación de requerimientos

De acuerdo a la fase de determinación de requerimientos establecida por OOHDM, la tabla 11 presenta los roles y funcionalidades que existen dentro del proyecto desarrollado, en la tabla 12, 13 se describen los requerimientos funcionales y no funcionales.

Tabla 11.

Roles y funcionalidades

ROLES	TAREAS
Administrador	Realiza la configuración de seguridad que desea colocar en su computador. Puede visualizar las consultas realizadas por parte del Usuario.
Usuario	No tiene acceso a la aplicación, sin embargo se quien visualice las restricciones realizadas con el Usuario Administrador

Tabla 12.

Requerimientos Funcionales

REQUERIMIENTOS FUNCIONALES
• La aplicación debe permitir el ingreso con un usuario y contraseña
• Es necesario permitir registrar restricciones de sitios web a los que los niños y adolescente no puedan ingresar.
• Es necesario permitir el registro de palabras que son consideradas como peligrosas para los menores.
• La aplicación debe restringir el acceso a sitios que han sido registrados anteriormente.
• La aplicación debe restringir el acceso a los sitios web que contengan palabras inapropiadas.

Tabla 13.

Requerimientos no funcionales

REQUERIMIENTOS NO FUNCIONALES
• La aplicación debe contener páginas amigables de fácil navegación.
• Se debe controlar los errores que la aplicación pueda presentar.
• Debe tener tiempos de respuesta razonables en los procesos internos que realiza la aplicación.
• La aplicación debe tener logs sobre los sitios y palabras que han sido habilitadas y deshabilitadas dentro del sitio Web.

4.3.1 Especificación de casos de usos

A continuación se presenta la descripción de los casos de uso que intervienen en el proyecto realizado (Véase tablas 14, 15, 16 y 17).

Tabla 14.

Caso de uso Ingresar al Sistema

Código	001
Nombre	Ingresar al sistema
Actor	Usuario y aplicación
Precondición	Ninguna
Descripción	Página con el formulario que me permite ingresar a la aplicación, al digitar correctamente el usuario y la contraseña
Post-condición	Si el usuario y la contraseña están correctas accede a la aplicación
Fecha	13-12-2013
Versión	1.1

Tabla 15.

Caso de uso Registrar Restricciones

Código	002
Nombre	Registrar Restricciones
Actor	Usuario y aplicación
Precondición	Ingresar a la aplicación logeandose correctamente
Descripción	Al dar click en la pestaña Palabras / Dominio aparece una caja de texto en el que se deberá digitar las palabras que se desea que el navegador bloquee su acceso y se presionar el mouse en el botón Bloquear.
Poscondición	Si el usuario y la contraseña están correctas accede a la aplicación
Fecha	13-12-2013
Versión	1.1

Tabla 16.

Caso de uso Bloquear por palabras

Código	003
Nombre	Bloquear por palabras
Actor	Usuario / Cliente (Explorador)
Precondición	Abrir un Navegador de Internet
Descripción	Desde un navegador o sitio web que contenga una palabra registrada que se encuentre en la lista de bloqueadas, la página no presenta información.
Poscondición	La página no presenta información.
Fecha	13-12-2013
Versión	1.1

Tabla 17.

Caso de uso Bloquear por dominio

Código	004
Nombre	Bloquear por dominio
Actor	Usuario / Cliente (Explorador)
Precondición	Abrir un Navegador de Internet
Descripción	Desde un navegador o sitio web que se coloque el url que se encuentre en la lista de dominios bloqueados, la página no se podrá visualizar.
Poscondición	La página no presenta información.
Fecha	13-12-2013
Versión	1.1

4.3.2 Diagramas de casos de uso

En esta sección se representa gráficamente los casos de uso anteriormente descritos (Véase figuras 57, 58, 59 y 60).

- Caso de Uso Ingresar al sistema

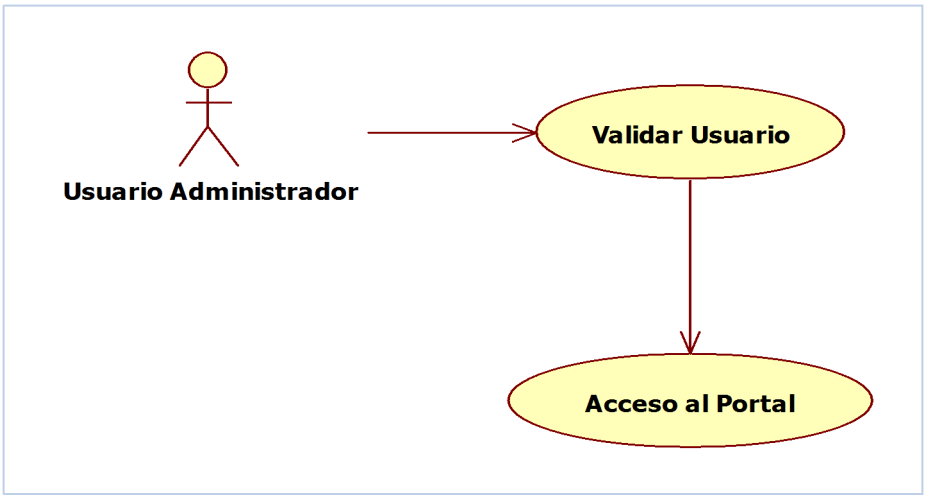


Figura 57. Caso de Uso Ingreso al Sistema

- Caso de Uso Registro de Restricciones

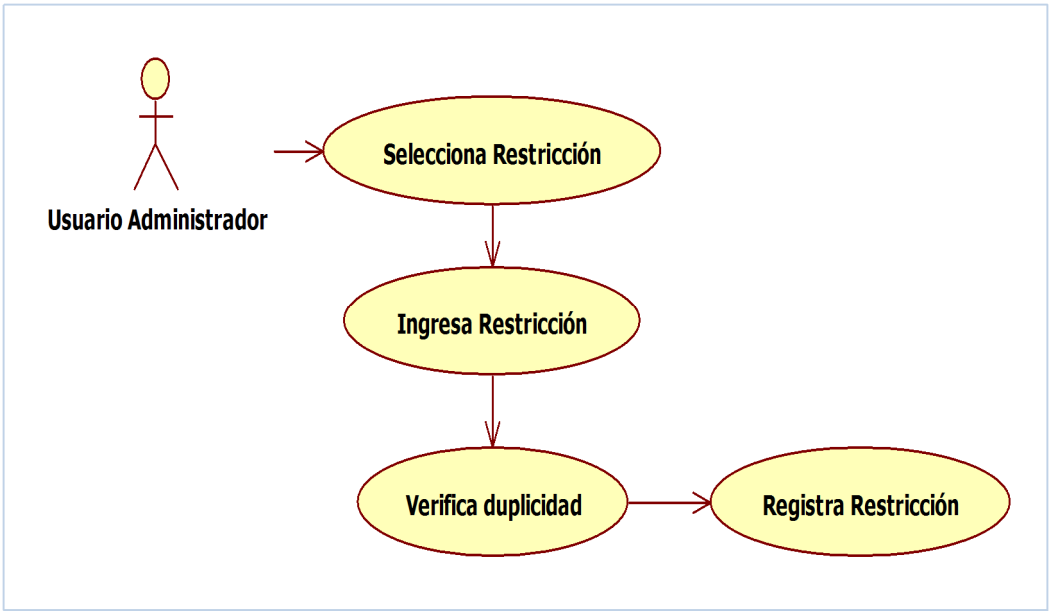


Figura 58. Caso de Uso Registro de Restricciones

- Caso de Uso Bloquear por dominio

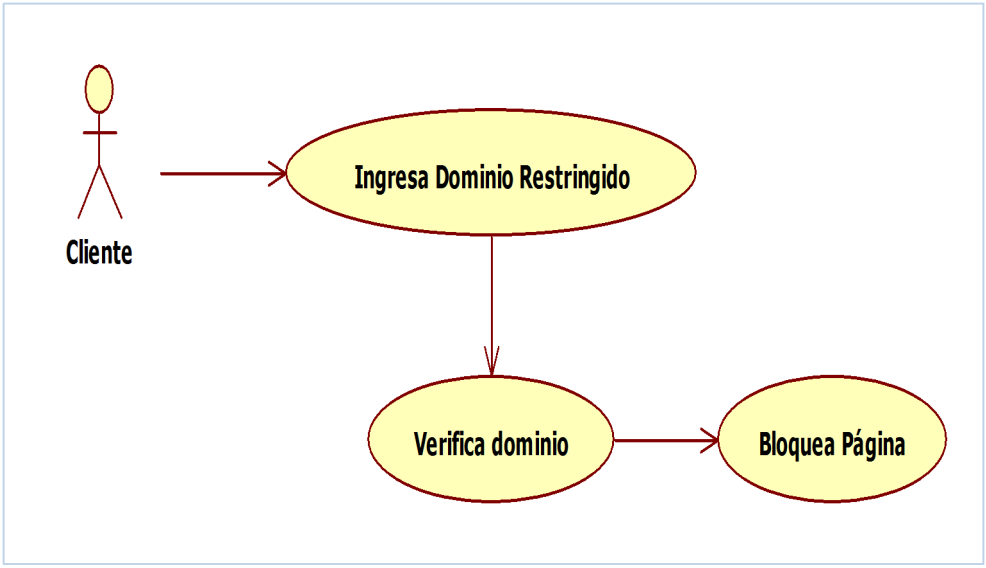


Figura 59. Caso de Uso Bloquear por dominio

- Caso de Uso Bloquear por palabras

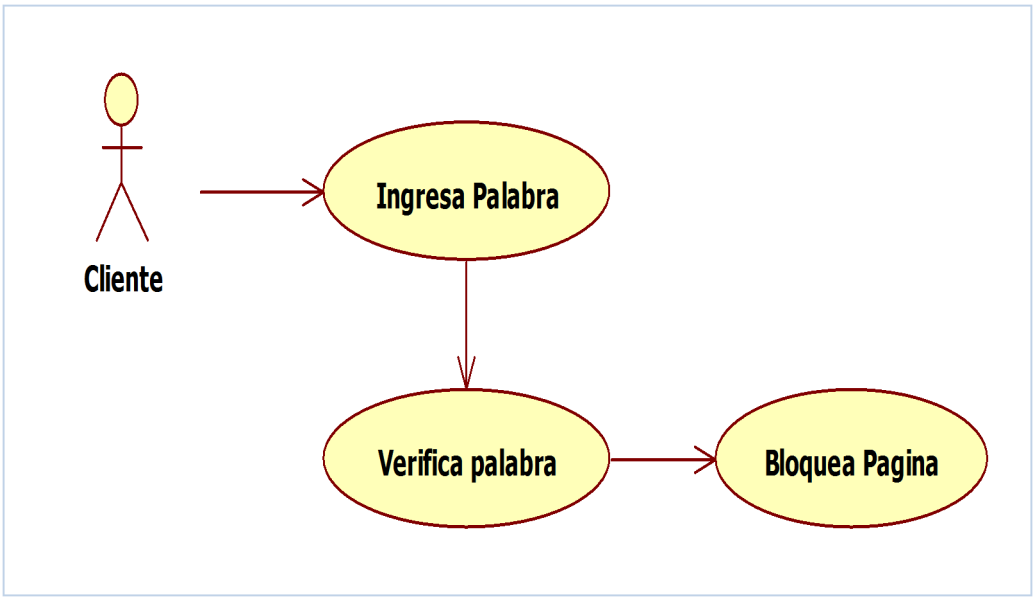


Figura 60. Caso de Uso Bloquear por palabras

4.3.3 Diagramas de secuencia

- Diagrama de Secuencia Ingresar al sistema

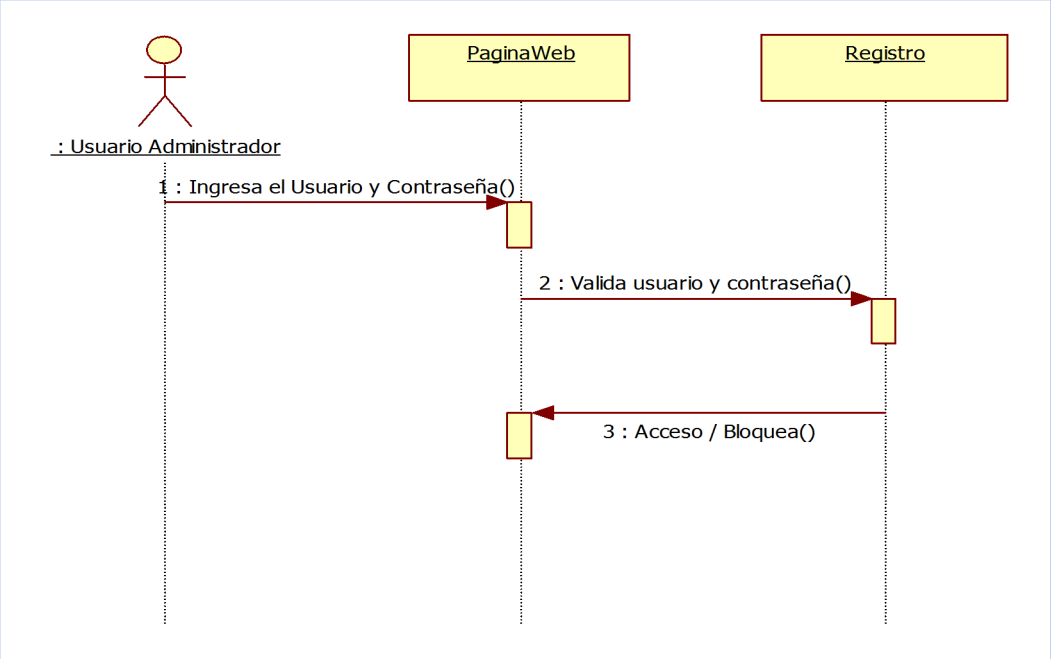


Figura 61. Diagrama de Secuencia Ingresar al Sistema

- Diagrama de Secuencia Registro de Restricciones

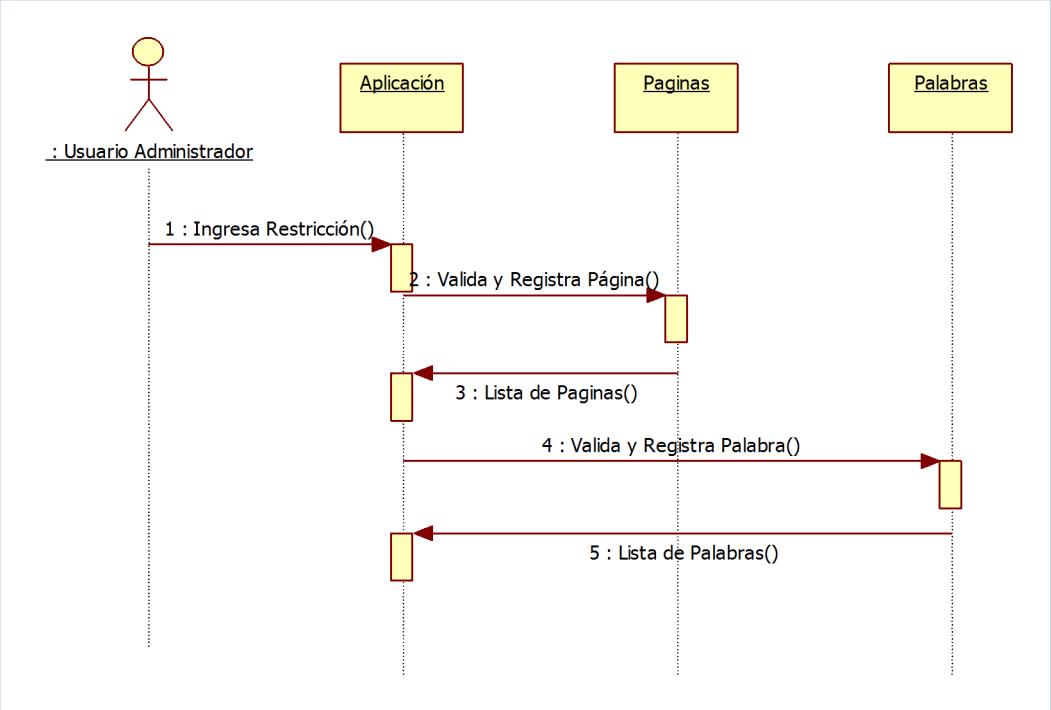


Figura 62. Diagrama de Secuencia Registro de Restricciones

- Bloquear por dominio

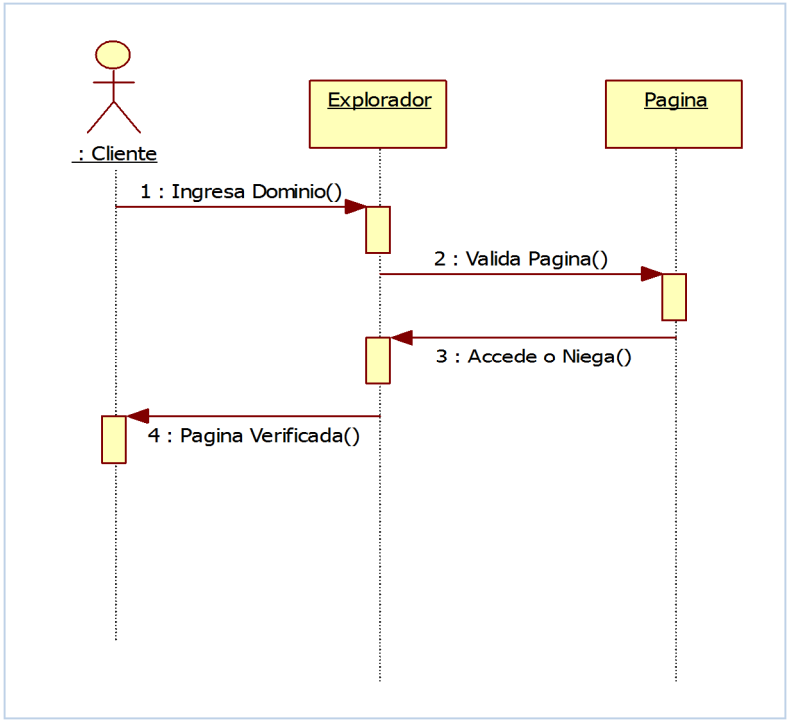


Figura 63. Diagrama de Secuencia Bloquear por dominio

- Bloquear por palabras

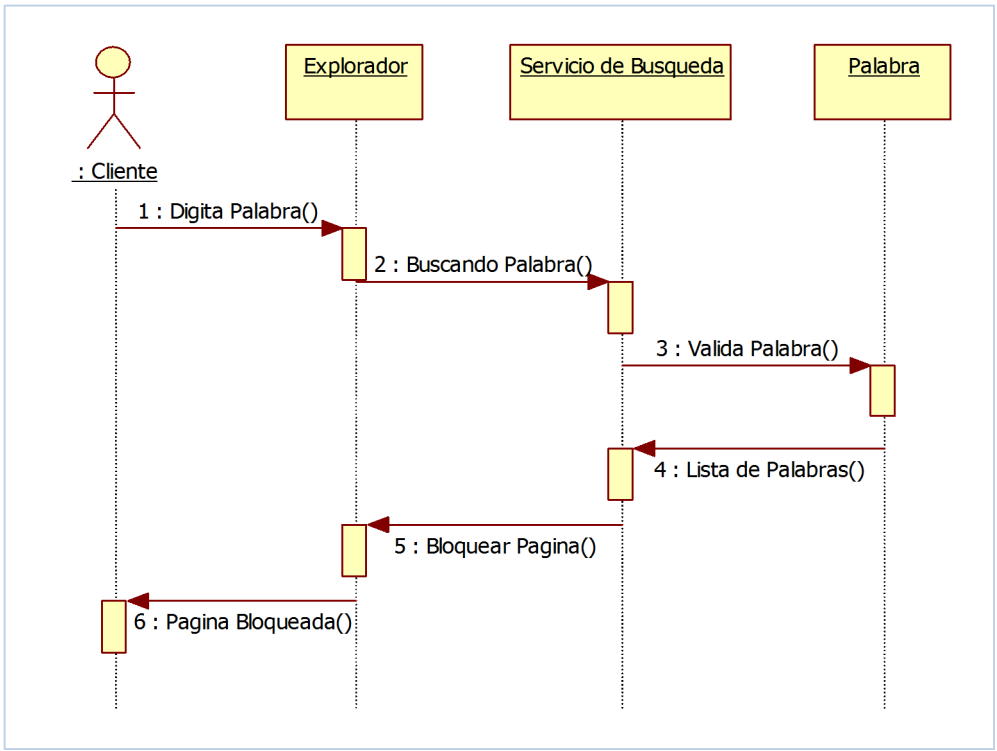


Figura 64. Diagrama de Secuencia Bloquear por palabras

4.4 Diseño conceptual

El modelo conceptual representa la estructura que almacena los datos que son manejados dentro de la aplicación, cada una de las entidades y sus respectivas relaciones permiten registrar datos importantes como palabras y páginas buscadas por los usuarios permitiendo que con estos registros se obtenga información significativa para los padres y o representantes de los menores. En la figura 65 se presentan todas las entidades que fueron utilizadas en el proyecto.

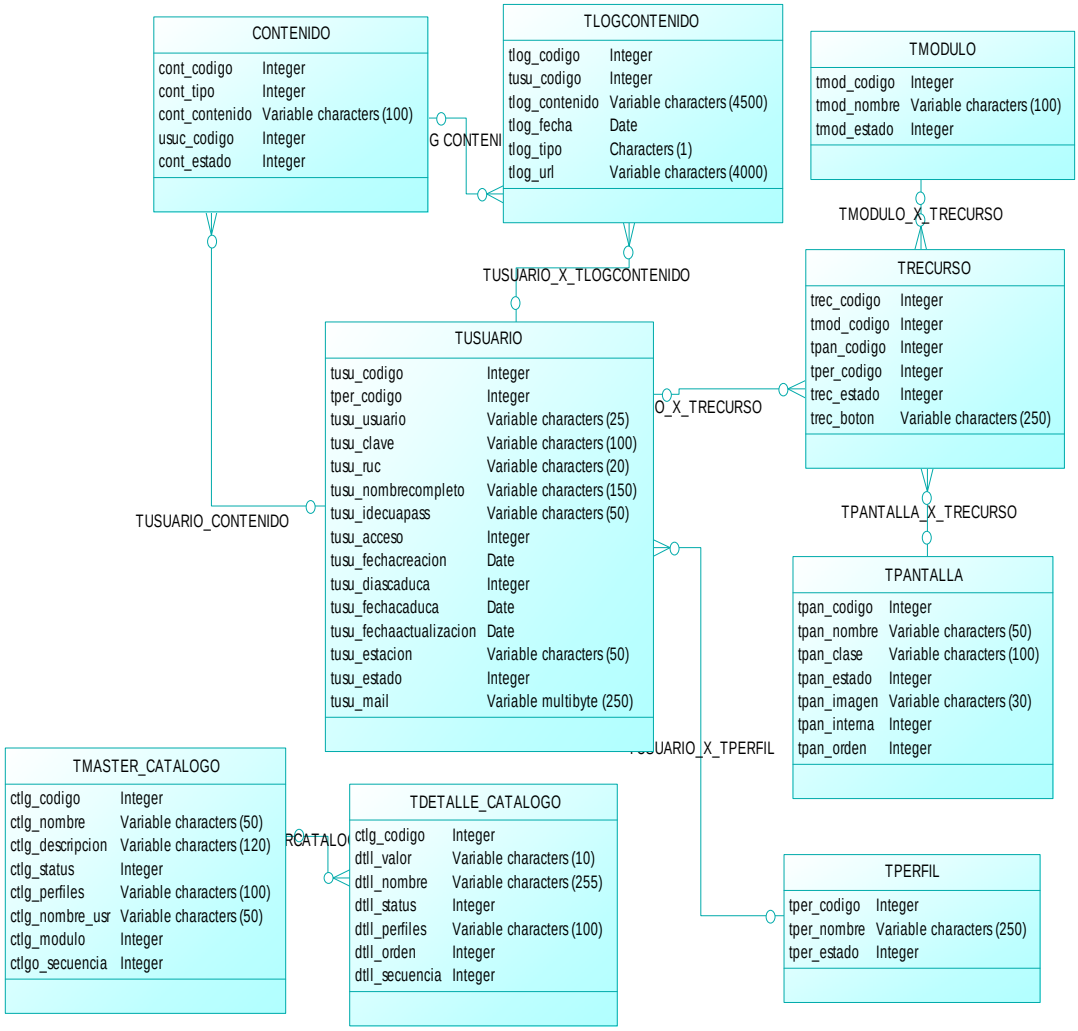


Figura 65. Modelo Conceptual

4.5 Diseño navegacional

Representa el flujo que la aplicación contiene, se presentan en 2 ambientes; el que se encuentra publicado en la Web como administración y el servicio que está instalado en la computadora del cliente monitoreando las visitas realizadas en Internet conectándose a una misma base de datos (Véase la figura 66).

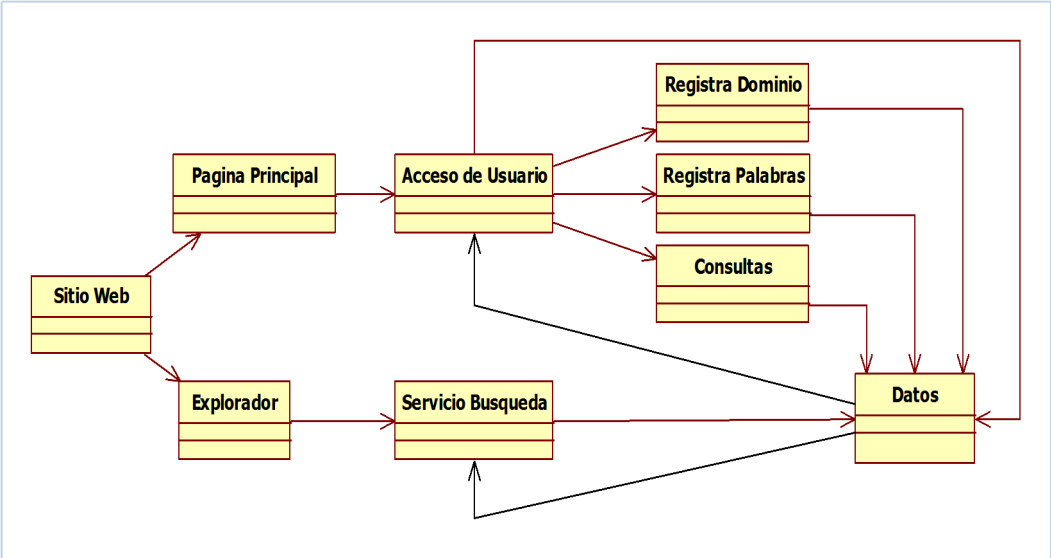


Figura 66. Modelo Navegacional

4.6 Diseño abstracto de interface

El diseño que se realiza para el ingreso a la aplicación, se encuentra dividida en el ingreso de usuario y el contenido, dentro del contenido se puede observar que se divide en dos partes; el menú y su detalle según la opción que se haya seleccionado, (Véase las figuras 67, 68, 69 y 70).

Figura 67. Diseño de Vista abstracta Ingreso al Sistema

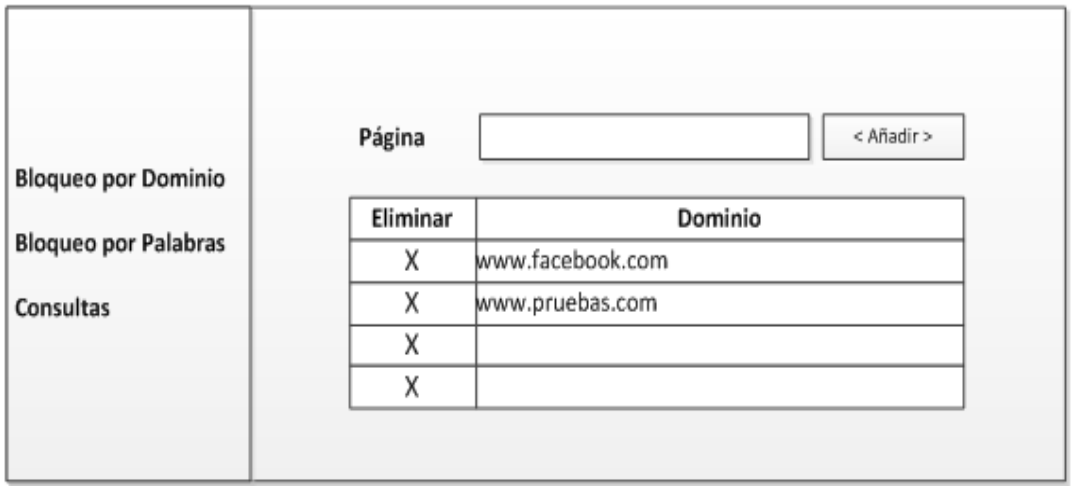


Figura 68. Diseño de Vista abstracta Bloqueo por Dominio

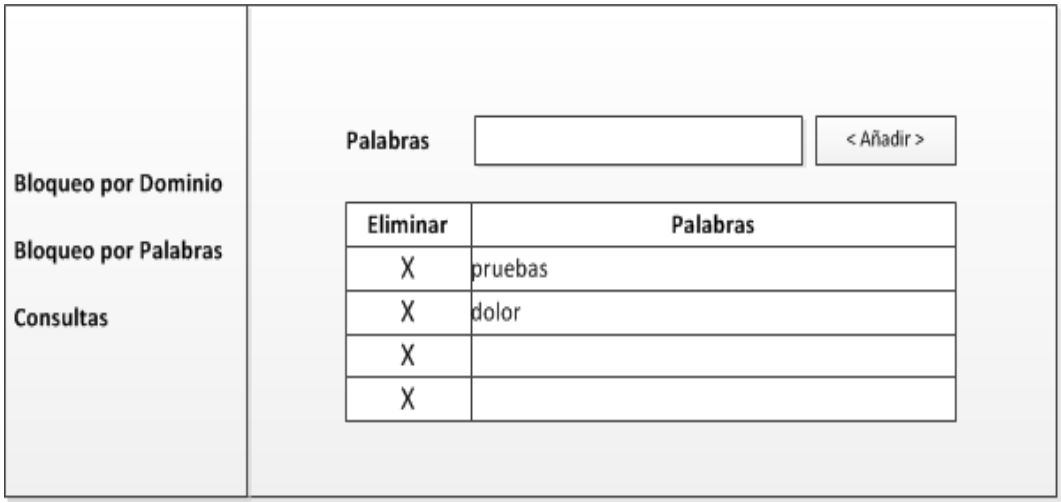


Figura 69. Diseño de Vista abstracta Bloqueo por Palabras

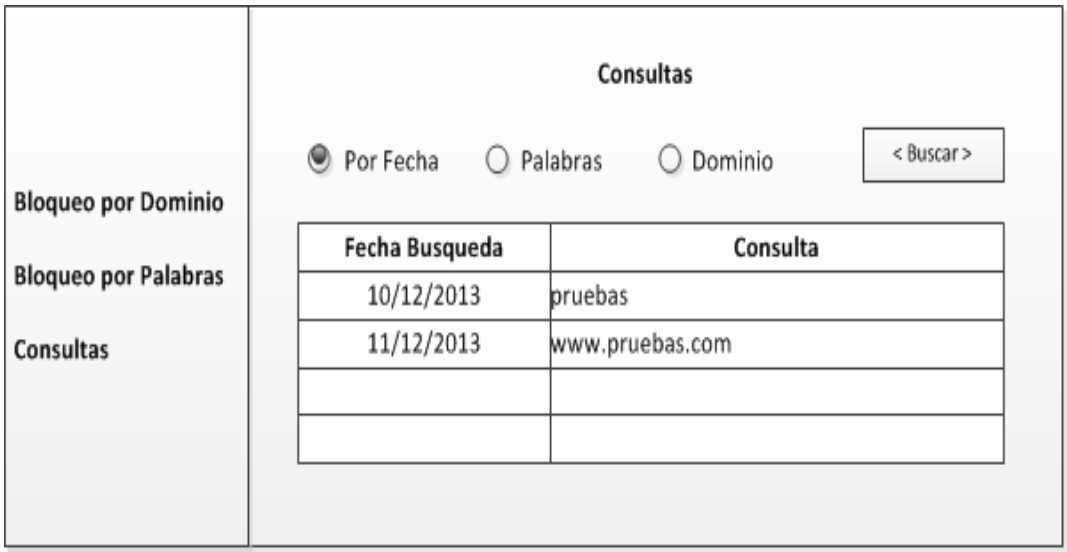


Figura 70. Diseño de Vista abstracta Interfaz de Consultas.

4.7 Diseño e implementación del Mecanismo de Control

Para el control de acceso a páginas Web con contenido inapropiado la aplicación se basó en: el aprendizaje de palabras y sitios Web que pueden ser consideradas peligrosas para los niños y adolescentes las cuales deben ser ingresadas por cada administrador del servicio de Control Parental (padres y/o representantes de los menores). Adicionalmente controla dentro de cada máquina el bloqueo de las páginas Web con palabras restringidas, y el bloqueo de páginas Web que han sido registradas y no deben ser accedidas, en la figura 71, se puede observar el modelo de la aplicación propuesta.

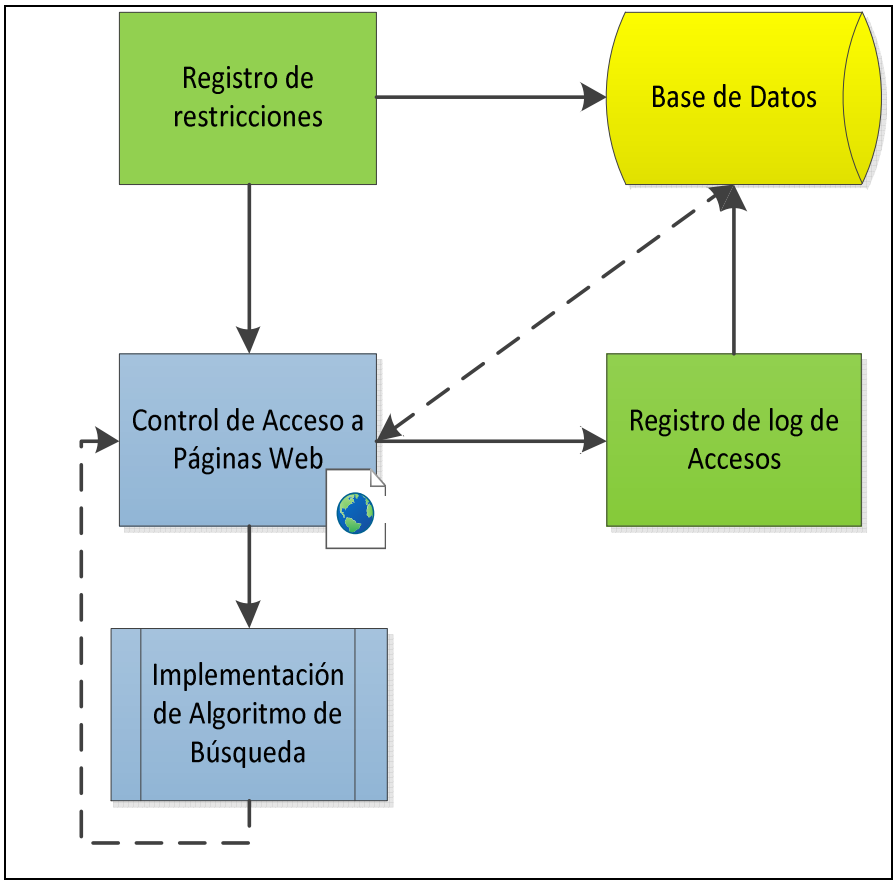


Figura 71. Modelo de Control de Acceso a Páginas Web

Dentro del bloqueo de páginas Web por palabras y dominios registrados, se tomó como pilar fundamental el Procesamiento de Lenguaje Natural utilizando la aplicación Recuperación de Información y el modelo de Recuperación Booleano, se

puede observar en la figura 72, el algoritmo utilizado para el bloqueo de páginas Web por palabras.

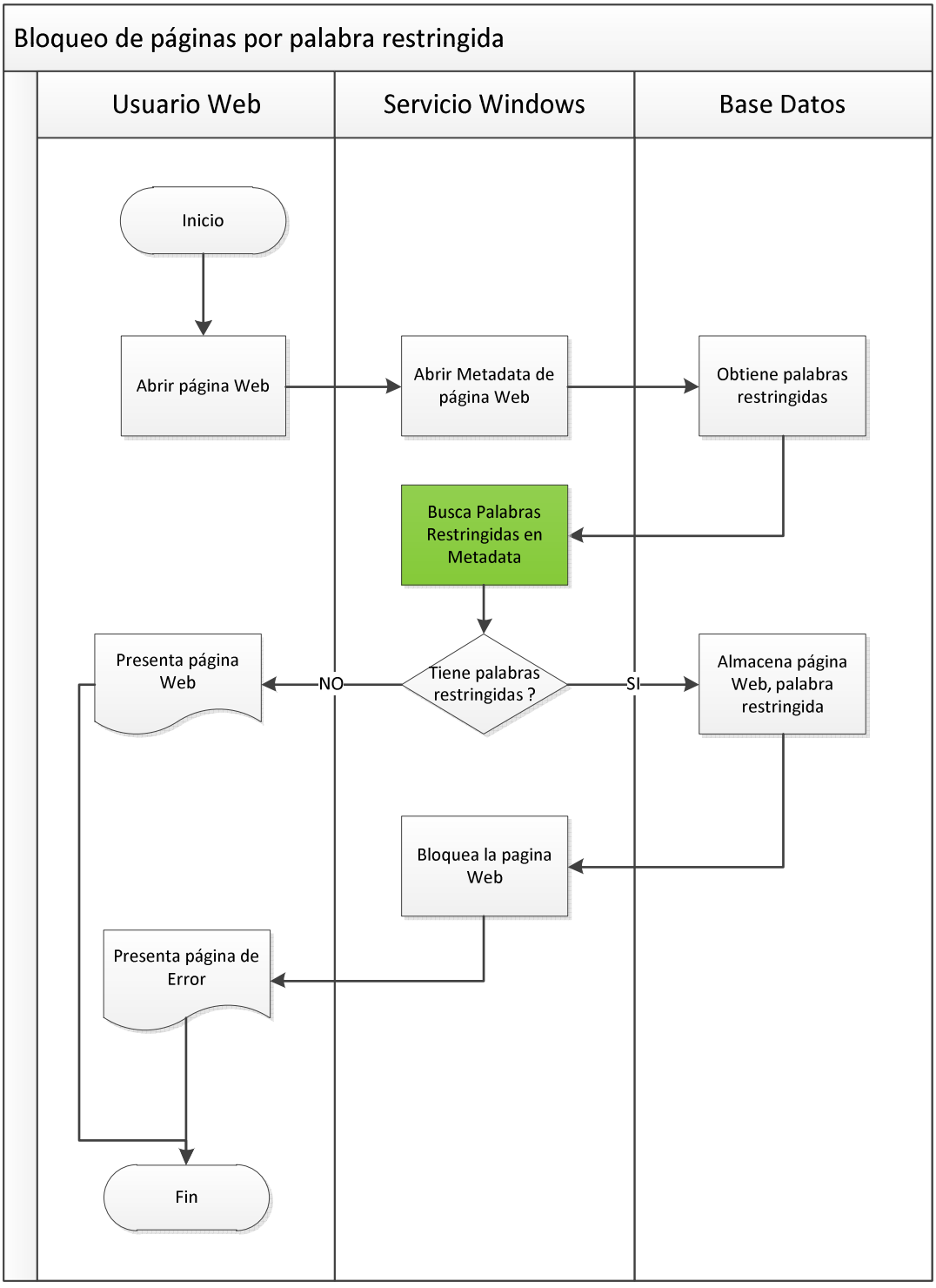


Figura 72. Algoritmo de Bloqueo de páginas Web por palabras restringidas

Cuando se realiza un bloqueo de palabras consideradas como inadecuadas para los menores se utiliza un nuevo diferente. En la figura 73, se puede observar el proceso Busca Palabras Restringidas, el cual está basado en el algoritmo de Boyer-Moore, y el algoritmo de búsqueda aproximada.

El algoritmo inicia dentro de la cadena de búsqueda en este caso dentro de la metadata de la página Web que vendría a ser el conjunto en donde se busca la palabra de izquierda a derecha. Para tener mayor eficiencia se minimiza el número de comparaciones entre palabras, es decir si se encontró una palabra restringida ya no se realizan más búsquedas.

En caso de no tener éxito con la búsqueda de palabras registradas como restringidas, se procede a recortar la palabra en un carácter al final y nuevamente inicia en la cadena de búsqueda, permitiendo así tener palabras aproximadas a las que han sido restringidas. Por ejemplo se registra la palabra ESCUELA al no ser encontrada se procede a recortar en una letra al final quedando como ESCUEL, en caso de no existir se recorta una letra adicional siendo ahora la palabra ESCUE, este proceso continua hasta recortar como 3 caracteres de la palabra original, tomando en cuenta que se realizará en palabras mayores a 7 letras, en caso de ser menores a 7 caracteres se procede a recortar 2 letras.

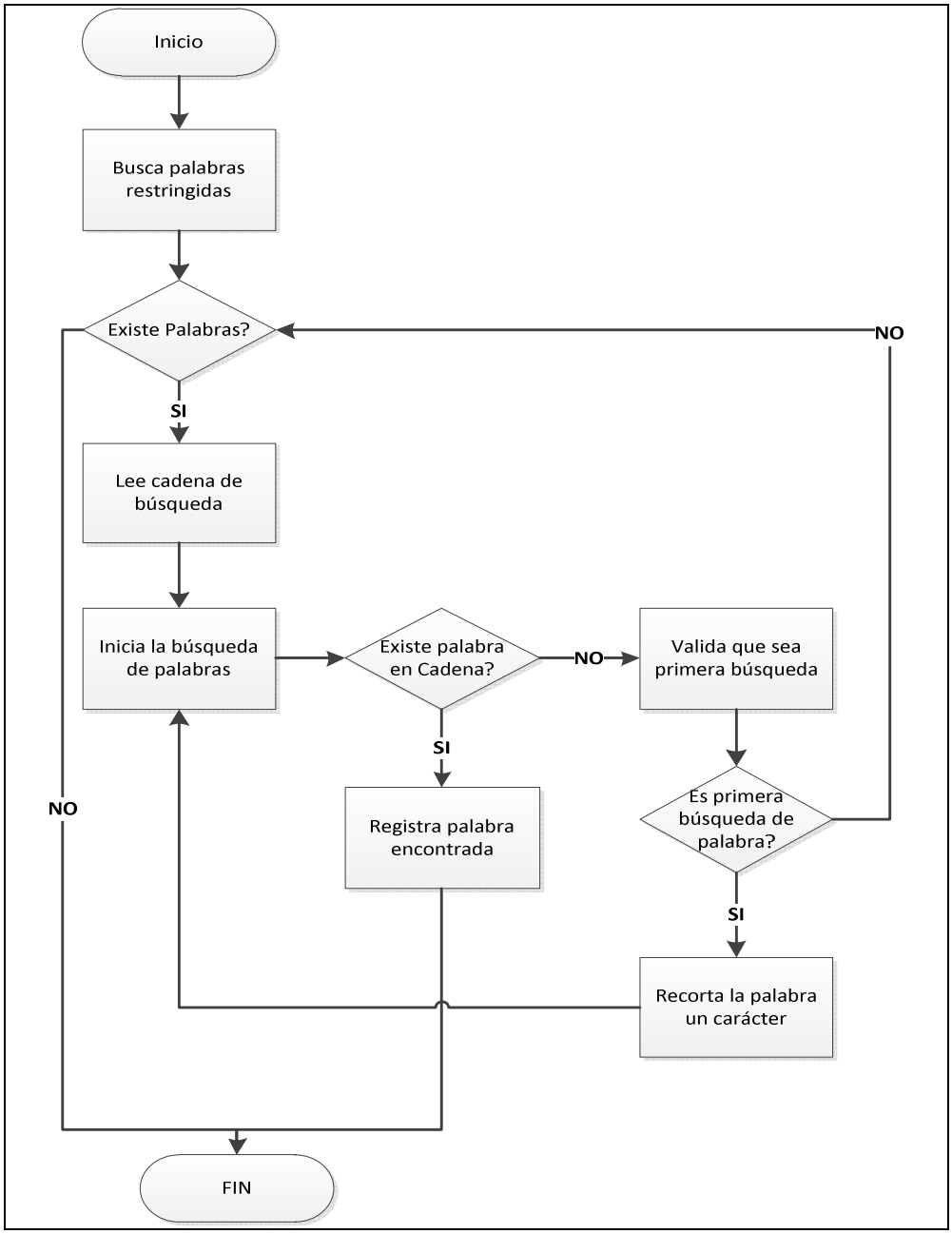


Figura 73. Algoritmo de Búsqueda de Palabra

En la figura 74, se puede observar el algoritmo utilizado para el bloqueo utilizado por dominios registrados.

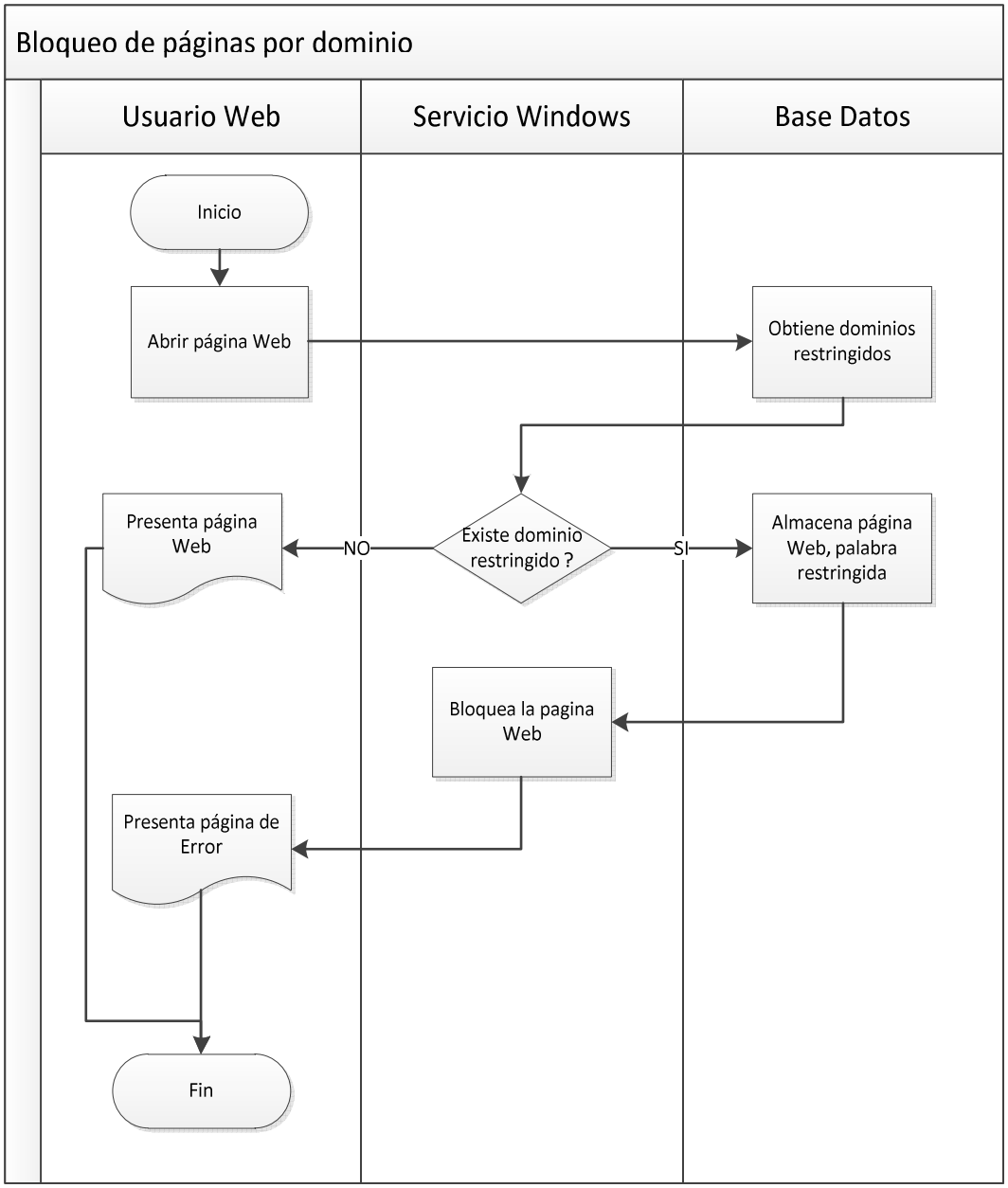


Figura 74. Algoritmo de Bloqueo de páginas Web por dominio restringido

4.8 Implantación, pruebas y evaluación de resultados

Una vez desarrollado el sistema que permite el control de acceso a páginas Web con contenido inapropiado, se procedió a realizar la publicación del sitio Web sobre un servidor Windows 2008 Server, con Internet Information Server, Framework 4.0 y base de datos PostgreSQL.

Para iniciar con las pruebas se registró a 34 usuarios accediendo al sitio Web, ver figura 75. Cabe recalcar que para registrarse dentro del sistema de Control Parental

no es necesario colocar los nombres reales de los usuarios por tal motivo el sistema indica que ingrese un seudónimo ver gráfico 76. Estos usuarios fueron registrados dentro de la base de datos que posteriormente permitirán obtener los resultados de su acceso al Internet.

Figura 75. Página principal sitio Web Control Parental

Figura 76. Página de registro de usuarios

Una vez registrados los usuarios, se ingresa a la aplicación para descargar el Servicio Windows (demonio) que permite realizar el control de contenido. Se instala en las 34 máquinas de los usuarios registrados, (ver Anexo 4 Manual de Registro e Instalación) y durante 20 días los usuarios ingresados inician con el registró de páginas Web que se han visitado, observar en la figura 77.

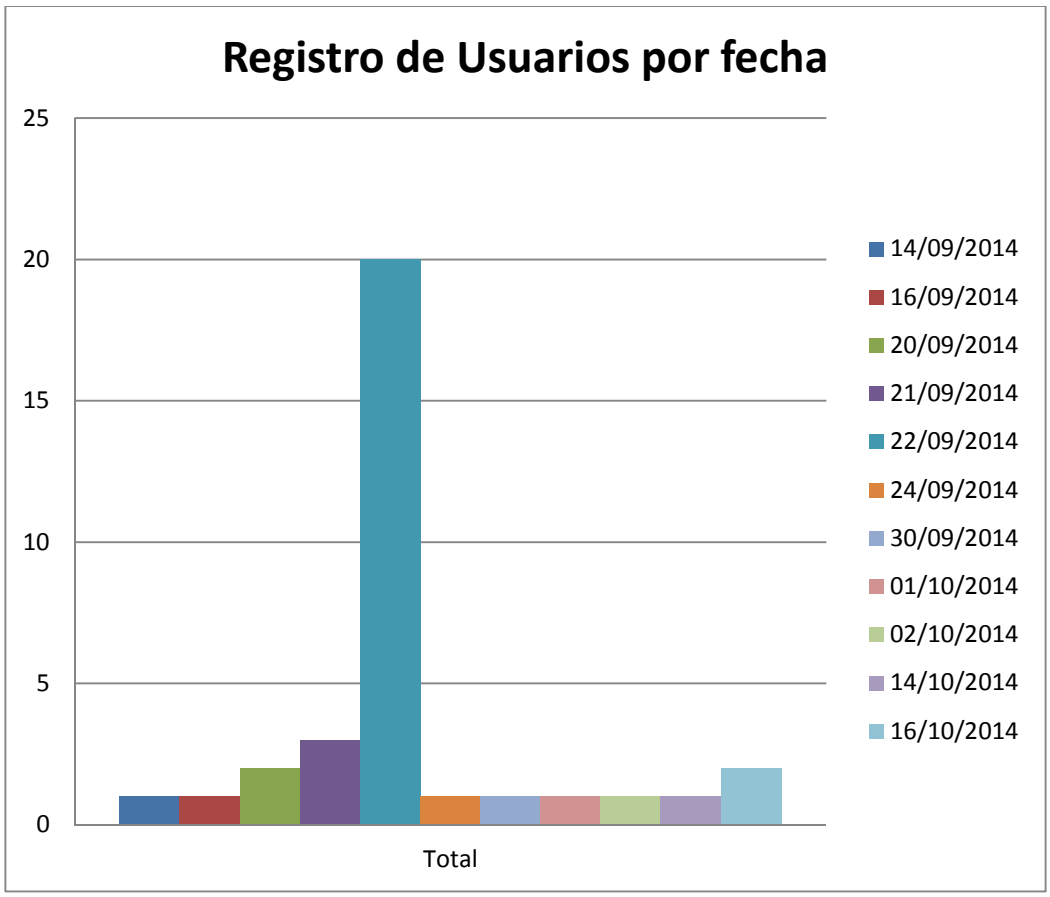


Figura 77. Registro de Usuarios por fecha

Cuando el servicio ha sido instalado el servicio procederá a registrar todos los accesos de páginas Web a las que visitó, este registro contiene la URL, el usuario, la fecha y hora de acceso. En el figura 78 se puede observar el número de accesos a las páginas Web por usuario tomado desde el 14 de septiembre al 24 de Octubre del presente año, el registro total de accesos a páginas Web es de 189655.

.

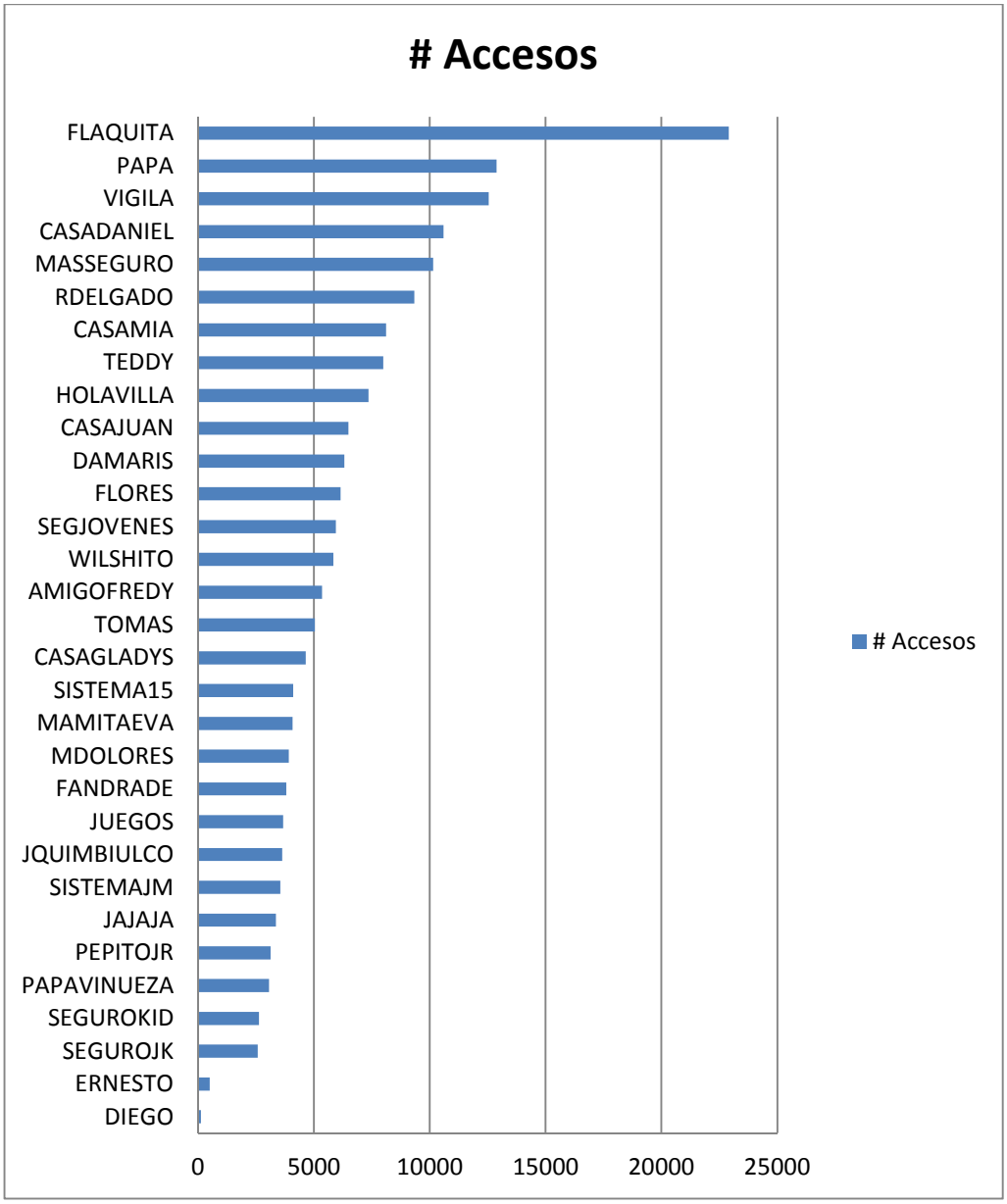


Figura 78. Número de accesos por usuario

En base a los accesos que fueron registrados se puede determinar que accedieron a 1168 páginas Web, las cuales fueron categorizadas de acuerdo al mayor número de accesos. En la figura 79 se puede observar que se categorizaron por Búsqueda, Entretenimiento, Educación, Correo Electrónico, Turismo, Página en Blanco, Deportes, Nueva Pestaña, Cultura, Banca, Salud, Varios, dentro de este último ítem se englobaron diferentes Url puesto que en número de acceso es inferior a 100.

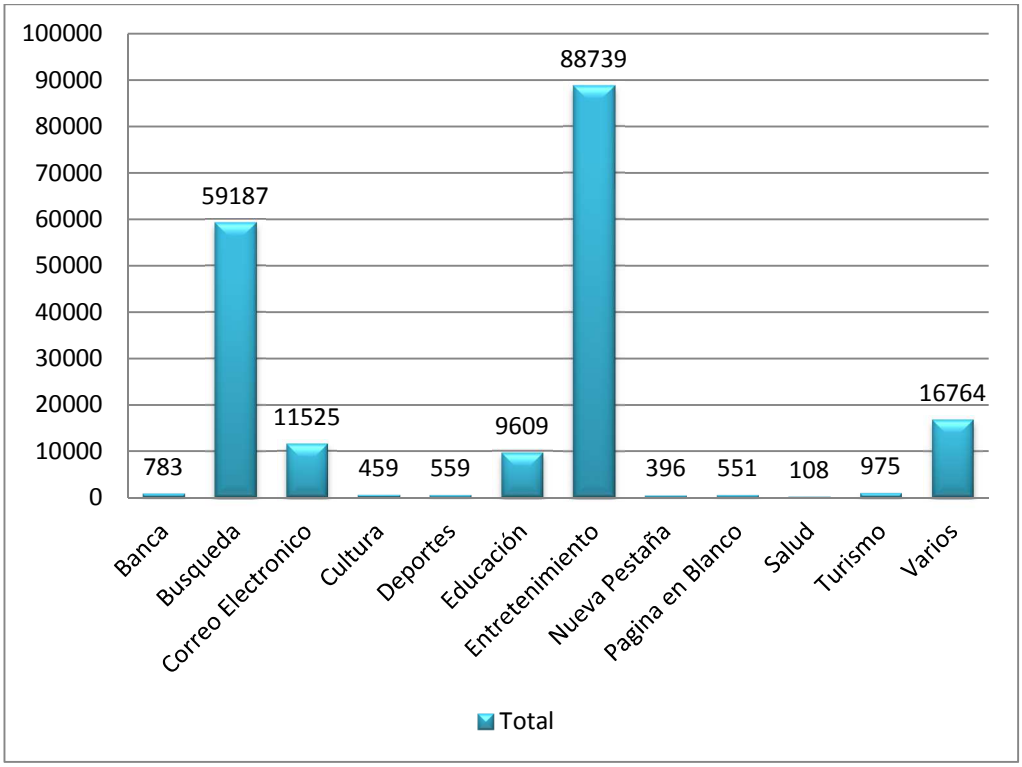


Figura 79. Número de accesos por categoría

En la figura 80 se puede apreciar los 11 sitios Web más visitados, evidenciando que el mayor acceso es en páginas de búsqueda como Google, y seguido por páginas de entretenimiento como Facebook.

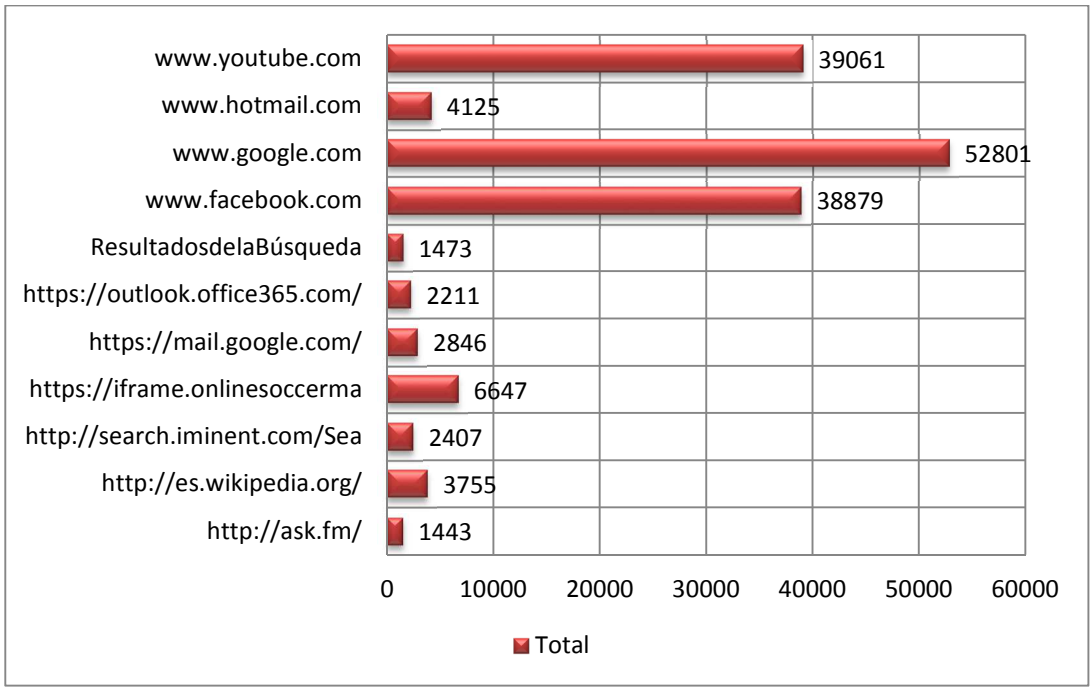


Figura 80. Sitios Web más visitados

A partir del 9 de Octubre se habilita el control de contenido que consiste en registrar palabras y sitios Web que se pueden considerar nocivas para todos los usuarios, (ver Anexo 5 Palabras y Sitios Web inapropiados). Este servicio inicia con el bloqueo de palabras y sitios que se encuentren registrados. En la figura 81 se presenta la cantidad de páginas ingresadas y bloqueadas por usuario, se puede verificar que el usuario que accede con más frecuencia es el usuario flaquita.

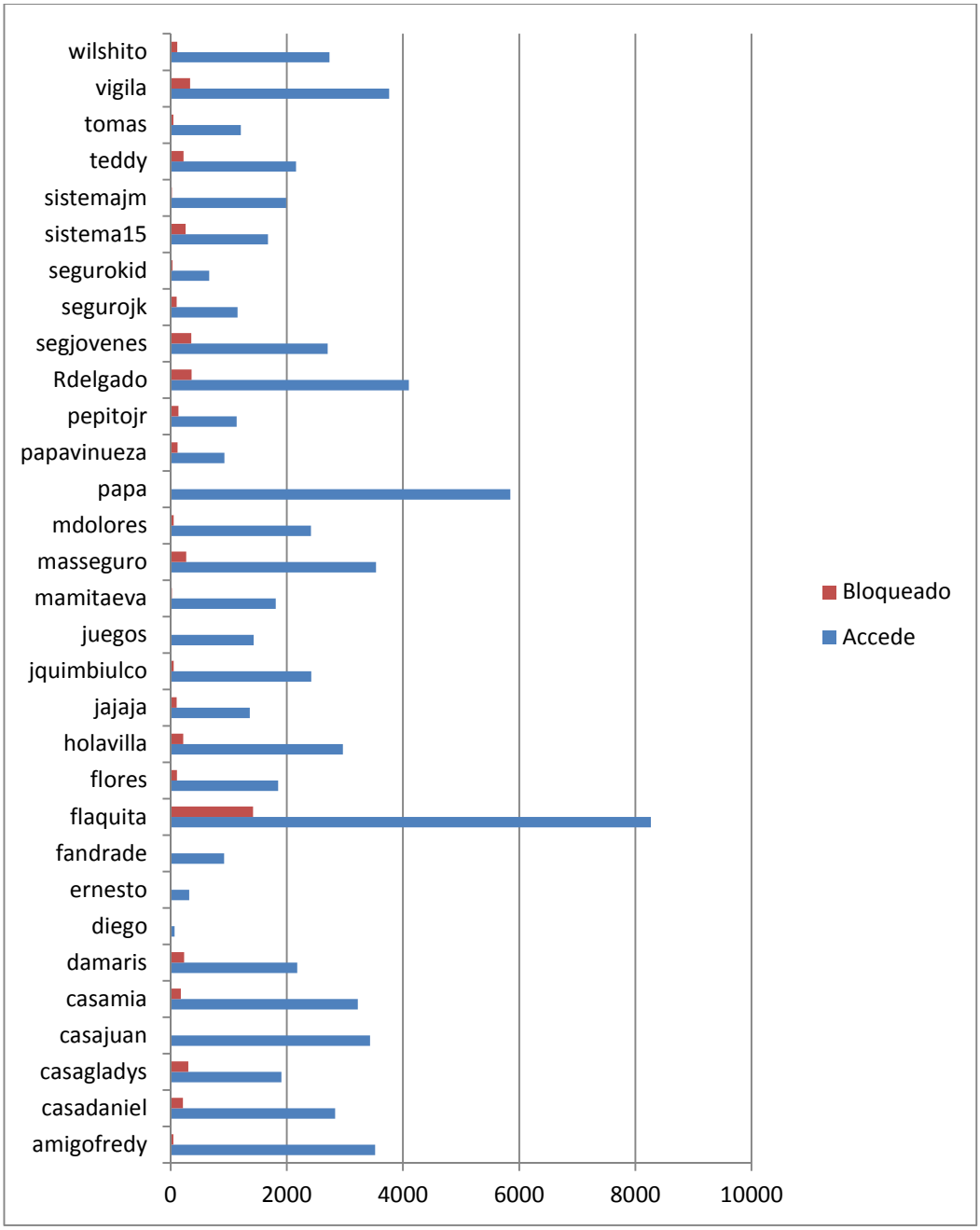


Figura 81. Número de accesos y bloqueos por usuario

En relación a la frecuencia de acceso por fechas se determina que el mayor número de accesos y bloqueos a páginas Web se realizan en el feriado nacional que es celebrado desde el 10 al 12 de Octubre, la figura 82 representa gráficamente el acceso a páginas Web en base a las fechas.

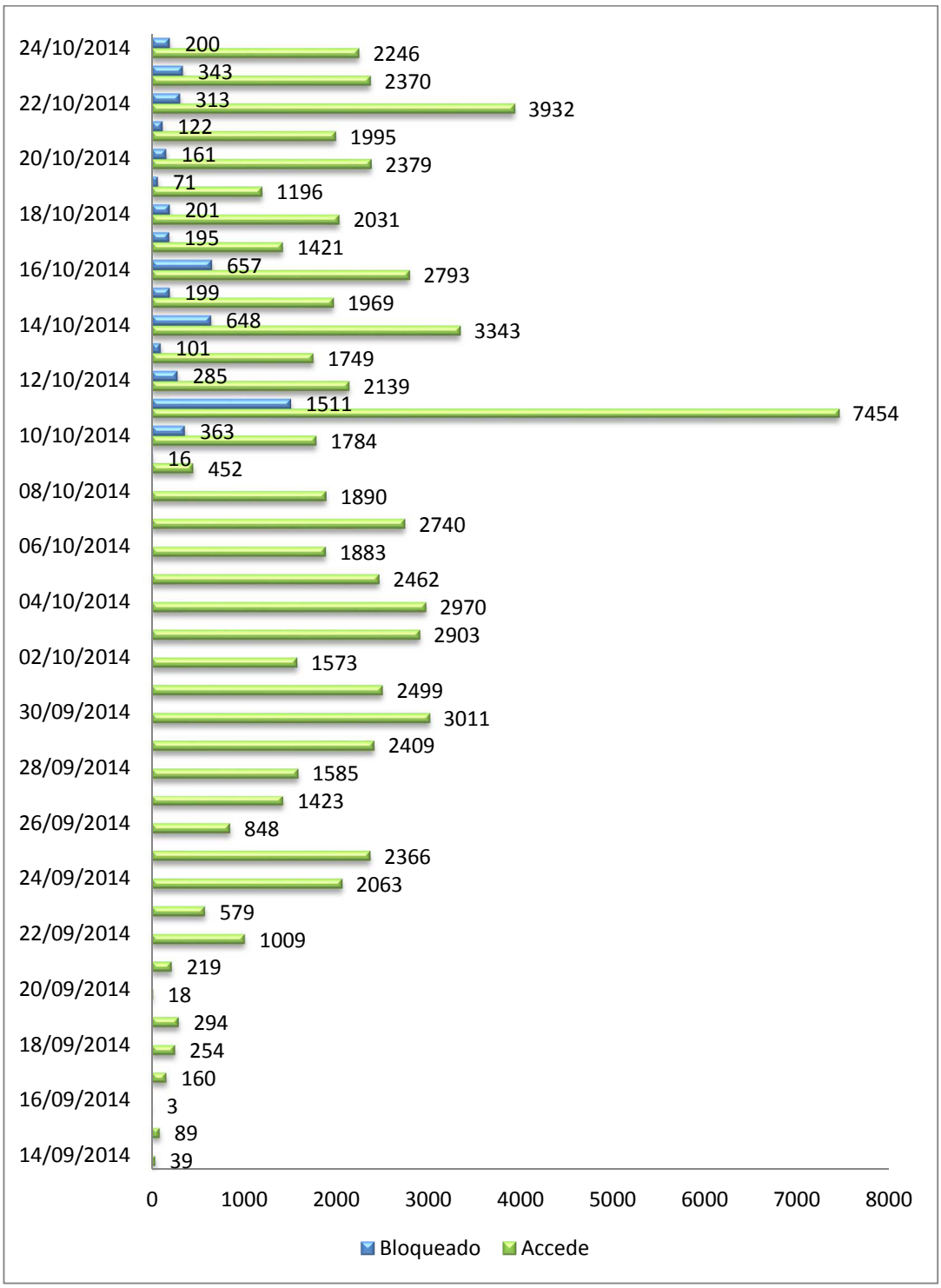


Figura 82. Número de accesos y bloqueos determinados por fecha

En relación al número de accesos por hora en el día se puede determinar que la mayor frecuencia en acceso al Internet es en el transcurso de la tarde tal como se puede observar en la figura 83, en donde se presenta los accesos y bloqueos que el servicio Windows almaceno.

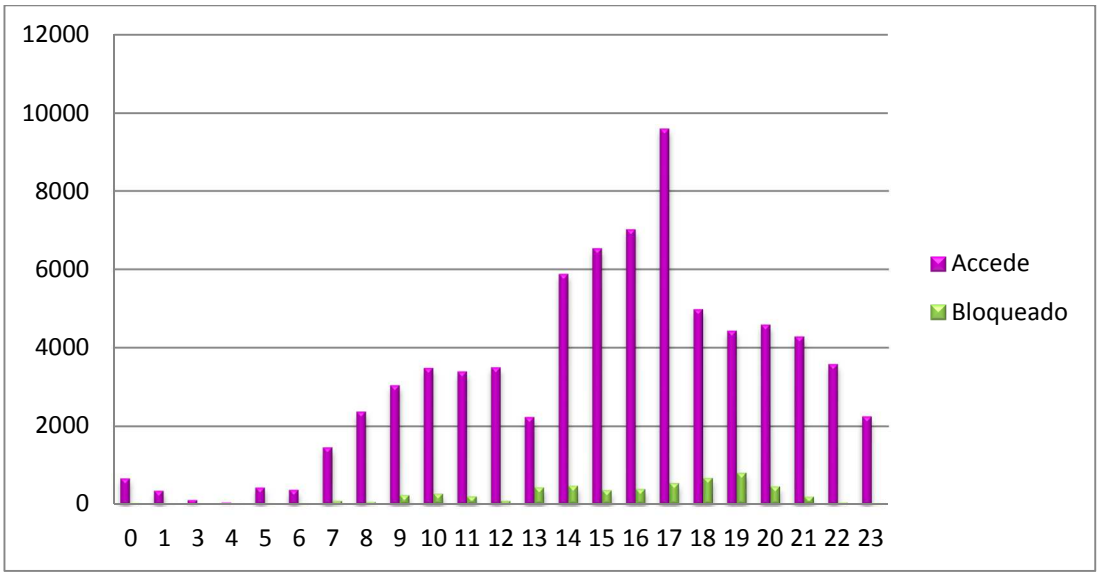


Figura 83. Número de accesos y bloqueos determinados por Hora

4.9 Contrastación de hipótesis

Después de instalar y capturar los registros que determinan el uso de Internet, y en base a la hipótesis planteada *"La aplicación de herramientas de filtrado de contenido Web disminuye significativamente el acceso a páginas con información no apropiada."*, se puede concluir que efectivamente la instalación de herramientas que controlan el filtrado de contenido en páginas Web reduce el acceso a contenido inapropiado en Internet.

Durante el periodo que se activó el bloqueo de páginas y palabras durante 15 días, desde el 9 al 24 de Octubre, se puede observar que el servicio Windows o demonio instalado en cada máquina, no se realizó los bloqueos que se visualizan en la tabla 18, evidenciando que los usuarios (niños y adolescentes) acceden a páginas con contenido inapropiado. Por otro lado se evidencia que esta herramienta ha permitido un mejor control por parte de los padres y/o representantes logrando vigilar e incluso bloquear paginas o palabras que consideren inadecuadas. La tabla 18 describe las palabras y sitios de mayor frecuencia que fueron bloqueados por el

sistema. Como se puede apreciar la palaba “Sexo” tiene una frecuencia no despreciable dentro del 30% de los usuarios evaluados, lo cual contrasta la hipótesis planteada.

Tabla 18.

Cuadro de sitios y palabras bloqueadas y número usuarios

Palabras / Sitios Bloqueados	# Bloqueos	# Usuarios
Drogas	17	7
Odio	29	10
Pornografía	5	3
Prohibido	14	7
Robar	11	3
Sexo	40	8
Terror	2	1
Violencia	10	5
www.chatiw.com	4	2
www.facebook.com	5136	29
www.puritanas.com	4	2
www.twitter.com	112	3
http://es.bongacams.com/	2	1

4.10 Conclusiones

En este capítulo se presentó la propuesta de una aplicación que permita mitigar el problema de acceso a Internet con contenido inapropiado por parte de los menores. Se presentaron los escenarios como; casos de uso, diagramas de secuencia, modelos conceptuales y de navegación que intervienen en esta propuesta. Adicionalmente se presenta los algoritmos utilizados los cuales se encuentran basados en el Procesamiento de Lenguaje Natural, y el modelo de recuperación de información. Una vez publicado el sitio Web e instalado el demonio, se obtuvieron resultados de las máquinas en la que fue instalado, estos fueron procesados y analizados para contrastar el acceso a páginas Web.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El libre acceso a Internet provoca que los niños y adolescentes se encuentren expuestos a contenido inapropiado. Para conocer cuál es el uso del Internet en los jóvenes entre 11 a 17 años se elaboraron encuestas que permitió identificar datos relevantes como: el acceso a Internet desde el hogar, tipo de páginas visitadas, el control o seguimiento por parte de los padres y/o representantes al momento de utilizar Internet, entre otros.
- Para el control de acceso a páginas Web con contenido inapropiado se investigó algunas herramientas que manejan Control Parental. Se determinó que existen varias organizaciones internacionales entre ellas la Comisión Europea que ha realizado un benchmarking basado en la funcionalidad, efectividad, usabilidad, seguridad y costo, determinando las mejores herramientas. A partir de este estudio se obtuvo la línea base de esta investigación y se realizó un análisis de las mismas de acuerdo a sus características.
- Se propuso realizar una aplicación que sea de fácil manejo y libre acceso con pertinencia y coherencia interna, manejando nuevos algoritmos que entregue un valor agregado a las herramientas que fueron analizadas. Se utilizó la técnica de Procesamiento de Lenguaje Natural basándose en el Modelo de Recuperación Booleano con algoritmos de búsqueda Boyer-Moore y búsqueda aproximada de filtrado
- Para el diseño e implementación se utilizó OOHDM, como lenguaje de programación Punto Net 2010, base de datos PostgresSQL, entregando al usuario final dos ambientes, el primero es el que se puede acceder desde la Web para registrar el usuario, las palabras y sitios Web que serán restringidos, y el otro ambiente es un servicio Windows (demonio) que se encuentra monitoreando el acceso y bloqueo de las páginas Web que se ingresan.
- Para obtener resultados de la aplicación realizada, se registraron e instalaron en algunas máquinas la aplicación durante 30 días, los primeros 15 días

fueron para registrar las páginas Web a las que ingreso el menor, en los días restantes se activó el bloqueo de sitios Web y palabras a las que no debería acceder el niño o adolescente.

- Con los datos obtenidos se logró obtener información importante como las páginas más visitas de acuerdo a diferentes categorías, el horario, la frecuencia de uso y principalmente los bloqueos a las páginas y palabras que fueron configuradas. Con esta información se pudo realizar la comprobación de la hipótesis formulada.

5.2 Recomendaciones

- Para controlar el acceso a páginas Web que contengan contenido inapropiado se recomienda utilizar cualquier herramienta que realice Control Parental. Dentro de esta investigación se encuentran listadas las herramientas que podrían utilizarlas.
- Los riesgos que se encuentran dentro de Internet, continuamente seguirán presentándose y los controles que se puedan implementar podrían resultar que en distintos casos no tenga éxito. Sin embargo es una manera de mitigar los peligros a los que se encuentran expuestos los niños y adolescentes
- Es conveniente educar a los niños y adolescentes desde una edad temprana de los posibles riesgos y consecuencias del acceso a contenido no apropiado. Los menores no pueden perder de vista la privacidad y la confidencialidad de cierta información. No deben tener contactos con desconocidos, es necesario concienciar a los menores de los peligros a los que podrían enfrentarse.
- Es necesario que como padres y/o representantes se realice una continua supervisión, acompañamiento y enseñanza de cuál es el correcto uso de Internet.

Referencias Bibliográficas

(INEC), I. N. (Diciembre de 2011). Obtenido de http://www.inec.gob.ec/sitio_tics/presentacion.pdf

Aguilera, P. (2010). *Seguridad Informatica.* Madrid: Editex.

Alonso Arévalo, J., & Martín Cerro, S. (2004). Benchmarking: una herramienta para gestionar la excelencia en las bibliotecas y los servicios de información. España.

Betfair. (11 de 01 de 2012). *betfair*. Obtenido de http://es.learning.betfair.com/app/answers/detail/a_id/2368/~/%C2%BFqu%C3%A9-es-el-filtro-de-control-parental%3F

Borja Fernández , C. (2010). *Las redes sociales. Lo que hacen sus hijos en Internet.* Alicante.

Broncano, R. G. (Abril de 2006). *Carlos III de Madrid*. Obtenido de http://modelosrecuperacion.tripod.com/vectorial.html

Broncano, R. G. (Abril de 2006). *Carlos III de Madrid*. Obtenido de http://modelosrecuperacion.tripod.com/booleano.html

Cáceres, S. (2005). *Fundación Orange*. Obtenido de http://fundacionorange.es/areas/28_observatorio/pdfs/censura.pdf

CyberAngels, T. W. (2007). *Cyber Angels*. Obtenido de http://www.cyberangels.org/docs/cybersafetyguide_spanish.pdf

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). *Access Denied The Practice and Policy of Global Internet Filtering.* London, England: William J. Drake and Ernest J. Wilson III.

Doctora Rocío Medina, P. (2011). *Liceo del Valle.* Obtenido de http://www.liceodelvalle.com.ec/web/guest/cyberbulling

Dr. Álvarez Marañón, G. (2009). *Internet segura para todos los usuarios.* Madrid: Catarata.

Educación, M. d. (09 de 2013). *http://geoportal.educacion.gob.ec/visor/index.html*. Obtenido de http://geoportal.educacion.gob.ec/visor/index.html

ESET. (13 de 09 de 2011). *ESET*. Obtenido de http://kb.eset-la.com/esetkb/index?page=content&id=SOLN2798&locale=es_ES

European Commission. (2011). Benchmarking of parental control tools for the online protection of children SIP-BenchII.

Fagan, P. (2012). *Family Research Council.* Obtenido de http://www.frc.org/pornography

Fernandez, J. F. (Diciembre de 2010). *Pantalla Amigas*. Obtenido de http://www.jorgefloresfernandez.com/2010/12/01/la-cultura-de-la-vida-%E2%80%9Cuso-seguro-de-internet-y-las-redes-sociales%E2%80%9D/

Franco, A. (2012). *La tecnología y los jóvenes.* Universidad Tecnológica Indoamérica.

Gómez Hidalgo, J., Puertas Sánz, E., Carrero, F., & de Buenaga Rodríguez, M. (Septiembre de 2004). Categorización de texto sensible al coste para el fltrado de contenidos inapropiados en Internet. Madrid, España.

Group, S. S. (Julio de 1991). RFC 1244.

Guins, R. (2009). *Technology and the culture of control.* Regents of the University of Minnesota.

Hanani, U., Shapira, B., & Shoval, P. (Agosto de 2001). *Springer Link.* Obtenido de http://link.springer.com/article/10.1023%2FA%3A1011196000674

Icard.net. (2012). *icard.net*. Obtenido de http://www.icard.net/web/icard/controlparental

K9 Web Protection. (2013). *K9 Web Protection*. Obtenido de http://www1.k9webprotection.com/

Keller, Í. (2012). *Ethic*. Obtenido de http://ethic.es/2011/10/china-refuerza-su-censura-frente-a-las-redes-sociales/

Lopez, J., & Romo, S. (2008). *Dirección y Gestión de los Sistemas de Información en la empresa.* Madrid: Esic.

Medina Ph.D, D. (2011). *Liceo del Valle.* Obtenido de http://www.liceodelvalle.com.ec/web/guest/cyberbulling

Melamud, D. A. (Febrero de 2009). *Scielo*. Obtenido de http://www.scielo.org.ar/scielo.php?pid=S0325-00752009000100007&script=sci_arttext

MsC. Martínez Rodriguez, A. (2006). *Indicadores cibermétricos ¿Nuevas propuestas para medir la información en el entorno digital?* . Obtenido de Acimed: http://bvs.sld.cu/revistas/aci/vol14_4_06/aci03406.htm

Mundo, B. (Diciembre de 2010). *BBC Mundo*. Obtenido de http://www.bbc.co.uk/mundo/noticias/2010/12/101220_internet_jovenes_proteccion_mr.shtml

Ortiz Henderson, G. (2012). L@s jóvenes y su relación con la red internet: de la adicción al consumo cultural. *RAZÓN Y PALABRA (ISSN 1605-4806)*, 16.

Pandasecurity. (2013). *pandasecurity*. Obtenido de http://www.pandasecurity.com/homeusers/downloads/docs/product/help/gp/2013/sp/84.htm

Parrini, L. (Junio de 2012). *La Palabra Abierta*. Obtenido de http://lapalabrabierta.blogspot.com/2012/06/que-hacen-sus-hijos-en-internet.html

Pfizer, F. (Septiembre de 2009). *www.fundacionpfizer.org*. Obtenido de http://www.fundacionpfizer.org/docs/pdf/Foro_Debate/INFORME_FINAL_Encuesta_Juventud_y_Redes_Sociales.pdf

PureSight. (2010-2011). *PureSight Online Child Safety*. Obtenido de http://www.puresight.com/About-Us/about-puresight.html

Segu-Kids. (2012). *Segu-Kids*. Obtenido de http://www.segu-kids.org/padres/control-parental.html

Serrano Mascaraque, E., Moratilla Ocaña, A., & Olmeda Martos, I. (2010). Métrica para la evaluación de la accesibilidad en Internet. *Revista española de documentación científica, ISSN 0210-0614, Vol. 33, Nº 3*, 19.

SIA, W. (2013). *WhileNet The Safe Internet*. Obtenido de http://www.whitenet.eu/en/detailed.html#up

Society, E. I. (08 de 12 de 2009). *Society, Europe's Information.* Obtenido de http://ec.europa.eu/information_society/activities/sip/projects/filter_label/sip_bench2/index_en.htm

Society, E. I. (15 de Noviembre de 2011). *Europe's Information Society*. Obtenido de http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7573

Symantec. (2013). *Norton Family*. Obtenido de https://onlinefamily.norton.com/familysafety/loginStart.fs

TI, D. (Enero de 2013). *Diario TI*. Obtenido de http://diarioti.com/mcafee-lanzara-en-chile-su-programa-global-de-seguridad-en-internet-para-escolares/60504?lang=es

Tsai, T.-H., Wei, C.-H., & Tsai, C.-Y. (Agosto de 2012). *Springer Link.* Obtenido de http://link.springer.com/article/10.1007%2Fs11135-012-9750-z

Velandia Mora, C. (2005). *Modelo Pedagógico con fundamentos en cibernetica social.* Medellin: Consejo Editorial Universitario.

Vista-tecnica. (06 de 03 de 2008). *vista-tecnica*. Obtenido de http://geeks.ms/blogs/vista-tecnica/archive/2008/03/06/control-parental-i-de-iv-por-alejandro-refojo.aspx

Glosario

Benchmarking.- Proceso de evaluación de productos, servicios o procedimientos de trabajo.

Bloqueo.- Interrupción, paralizar procesos que se encuentren ejecutándose.

Control.- Limitación, verificación o supervisión de actividades que se realizan.

Demonio.- Es un tipo especial de proceso no interactivo, se ejecuta en segundo plano es decir no es controlado directamente por el usuario.

Peligro.- Es una situación en la que podría ocurrir incidente probablemente dañino.

PLN.- Procesamiento de Lenguaje Natural.

Pornografía.- Son todos los textos imágenes o videos que con contenido sexual.

Riesgo.- Probabilidad de que ocurra algún suceso.

Internet.- Son las la red de computadoras, que se encuentran interconectadas entres si mediante un conjunto de protocolos TCP/IP.

Grooming.- Es una forma de acoso de persona adultas hacia menores de edad mediante el uso de la tecnología especialmente redes sociales.

Bulling.- Acoso, ya se de tipo físico o psicológico, con la finalidad de hacer daño, especialmente entre compañeros de colegio.

Web.- Es una red de alcance mundial (World Wide *Web).*

Dominio.- Es el nombre que puede contener caracteres alfanuméricos y hace referencia a una dirección física o IP.

URL.- Es una secuencia de caractéres que identifica de forma precisa a algún recurso de Internet el significado de sus siglas son: Uniform Resource Locator (Localizador Uniforme de Recursos)

OOHDM.- (Método de Diseño Hipermedia Objeto Orientado), metodología de desarrollo de aplicaciones Web.

Control Parental (Control Paterno).- Software mediante el cual los padres de familia pueden controlar el acceso al Internet.

Técnicos de los Colegios encuestados.- Son las personas encargadas de administrar el acceso al Internet.

Riesgo.- Es la probabilidad que ocurra un evento negativo.

Sistema Operativo.- Conjunto de programas que permite la administración de los recursos de un computador.

Línea Base.- Es la primera medición de los indicadores considerados en el desarrollo de un proyecto, viene a ser un punto de partida.

Base de datos.- Es un conjunto de datos organizados y relacionados de forma lógica, sobre un determinado tema.

Metadata.- Son los datos que describen a otros datos.

Anexos

UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE"
PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS
ENCUESTA DIRGIDA A NIÑOS Y ADOLESCENTES

OBJETIVO: Medir la frecuencia de uso, el tipo de información, amenazas y medios de vigilancia en el acceso a contenidos Web de os niños y adolescentes, con el fin de identificar mecanismos de control para mitigar el acceso a contenido inapropiado en el Internet.

INDICACIONES GENERALES:

- Señala con una X la respuesta de tu elección.
- Contesta con total sinceridad a cada uno de los ítems que presentamos.

DATOS INFORMATIVOS:

EDAD: _____ ENTIDAD EDUCATIVA: COLEGIO ☐ ESCUELA ☐
GENERO: FEMENINO☐ MASCULINO ☐ AÑO QUE CURSO: _____
LUGAR Y FECHA: _____

PREGUNTAS

1. ¿Has utilizado o utilizas Internet?
   ☐ Sí ☐No
   Si la respuesta es NO, termina la encuesta, caso contrario continua con la pregunta 2

2. ¿Qué dispositivo utilizas para acceder a Internet?
   ☐ Laptop / Portatil
   ☐ PC
   ☐ Celular
   ☐ Tablet
   ☐ Todas las anteriores

3. ¿Desde qué lugar accedes al Internet? – Puedes seleccionar más de una respuesta
   ☐ Casa / hogar
   ☐ Estudio / Colegio
   ☐ Casa de Amigos
   ☐ CafeNet
   ☐ Casa de Familiares
   ☐ Lugares Públicos con WIFI
   ☐ Lugar de trabajo Padre / Madre
   ☐ Otro ¿Cuál? _____

4. Tienes Internet en tu casa / hogar
   ☐ Sí ☐No
   Si la respuesta es NO continua en la pregunta 8.

5. ¿En qué lugar de tu hogar se encuentra ubicado el computador?
   ☐ Sala Social
   ☐ Sala de Estudio
   ☐ Tu Dormitorio
   ☐ Dormitorio de los padres o hermanos mayores
   ☐ Comedor
   ☐ Otro ¿Cuál? _____

6. ¿Conoces qué sistema operativo tiene tu computador?
   - ☐ Windows XP
   - ☐ Windows 7
   - ☐ Windows 8
   - ☐ Linux
   - ☐ Desconozco
   - ☐ Otro ¿Cuál? _____

7. ¿Tienes instalado algún programa de protección o antivirus en tu computador?
   - ☐ Si ¿Cuál?_____
   - ☐ No
   - ☐ Desconozco

8. ¿Con que frecuencia accedes a Internet?
   - ☐ Todos los días
   - ☐ Una vez a la semana
   - ☐ Al menos 2 o 3 veces a la semana
   - ☐ Una vez al mes
   - ☐ Otro ¿Cuál? _____

9. ¿A qué hora sueles conectarte a Internet?
   - ☐ En la mañana
   - ☐ En la tarde
   - ☐ Todo el día menos en la noche
   - ☐ Solo en la noche
   - ☐ A toda hora

10. ¿Cuánto tiempo en promedio utilizas el Internet en cada sesión? _____

11. ¿Para qué utilizas Internet?
    - ☐ Buscar Información relacionada a los estudios escolares
    - ☐ Redes sociales
    - ☐ Chatear
    - ☐ Escuchar música
    - ☐ Correo Electrónico
    - ☐ Descargar música / videos
    - ☐ Búsqueda de información de ocio y entretenimiento
    - ☐ Jugar
    - ☐ Otro ¿Cuál? _____

12. ¿Tienes creada una o varias cuentas/perfil en alguna red social?
    - ☐ Si Continua con la encuesta
    - ☐ No Pasa a la pregunta 16

13. ¿Cuál es la red social que más utilizas?
    - ☐ Facebook
    - ☐ Twiter
    - ☐ LinkedIn
    - ☐ Hi5
    - ☐ Otro ¿Cuál? _____

14. ¿Cuántos amigos tienes en la red social que más utilizas? _____

15. ¿De los amigos que tienes en la red social, aproximadamente a cuantos conoces personalmente? _____

16. ¿Te comunicas a menudo con personas que NO conoces personalmente?
    - ☐ Si
    - ☐ No

17. ¿Para qué usas estas redes o comunidades virtuales?
    - ☐ Estar en contacto con amigos frecuentes
    - ☐ Estar en contacto con amigos a los que pocas veces ve en persona
    - ☐ Hacer nuevos amigos
    - ☐ Otra ¿Cuál? _____

18. ¿Tus padres o algún adulto supervisa mientras estas conectado a Internet?
    - ☐ Siempre
    - ☐ Casi siempre
    - ☐ Algunas Veces
    - ☐ Rara vez
    - ☐ Nunca

19. Has sufrido alguna clase de peligro o agresión cuando utilizas Internet
    - ☐ Si ¿Cuál?_____ Continua con la encuesta
    - ☐ No Pasa a la pregunta 21

En caso que la respuesta sea Si.

20. ¿Les has comentado a tus padres sobre el problema que atravesaste?
    - ☐ Si
    - ☐ No ¿Porque?_____

21. ¿Qué acción tomaron tus padres frente a esta situación?
    _____

22. ¿Crees que estas utilizando el Internet correctamente?
    - ☐ Si
    - ☐ No
      ¿Porque?_____

UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE"
PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

ENCUESTA DIRIGIDA A LOS PADRES Y/O REPRESENTANTES DE NIÑOS Y ADOLESCENTES

OBJETIVO: Medir el grado de control y protección que los padres tienen frente al uso de Internet para los niños y adolescentes.

INDICACIONES GENERALES:

- Señala con una X la respuesta de tu elección.
- Contesta con total sinceridad a cada uno de los ítems que presentamos.

DATOS INFORMATIVOS:

EDAD: _____ GENERO: FEMENINO☐ MASCULINO ☐

LUGAR Y FECHA: _____

PREGUNTAS

1. ¿En su hogar existen niños y/o adolescentes entre las edades de 10 y 17 años?
   ☐ Si
   ☐ No
   Si la respuesta es No termina la encuesta, caso contrario continua con la siguiente pregunta

2. ¿Posee Internet dentro de su hogar?
   ☐ SI
   ☐ NO
   Si la respuesta es No termina la encuesta, caso contrario continua con la siguiente pregunta

3. ¿En qué lugar se encuentran los computadores con acceso a Internet dentro de su hogar?
   ☐ Sala Social
   ☐ Sala de Estudio
   ☐ Dormitorio de niños y/o adolescentes
   ☐ Su Dormitorio
   ☐ Comedor
   ☐ Otro ¿Cuál?_____

4. ¿Conoce qué sistema operativo tiene su computador?
   ☐ Windows XP
   ☐ Windows 7
   ☐ Windows 8
   ☐ Linux
   ☐ No conoce
   ☐ Otro ¿Cuál? _____

5. ¿Tiene instalado algún programa de protección, monitoreo o control de acceso al Internet?
   ☐ Si ¿Cuál?_____
   ☐ No

6. ¿Tiene instalado algún antivirus en su equipo con acceso a Internet?
   ☐ Si ¿Cuál?_____
   ☐ No

7. ¿Ha realizado alguna configuración de Control Parental en su computador?
   ☐ Si ¿Cuál?_____
   ☐ No

8. ¿Permite que sus hijos utilicen Internet a cualquier hora?
   ☐ Si, pueden acceder a cualquier momento
   ☐ Solo utilizan bajo su presencia
   ☐ Se utiliza a todas horas menos en la noche
   ☐ Solo 2 horas al día

9. ¿Supervisa que hacen su(s) hijo(s) en Internet?
   ☐ Si
   ☐ No

10. ¿Conoce cuáles son los peligros a los que está expuesto su hijo en Internet?
    ☐ Si
    ☐ No

11. ¿Cree que su hijo utiliza responsablemente el Internet?
    ☐ Si
    ☐ No

Gracias por su colaboración

UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE"
PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS
ENCUESTA DIRGIDA A TECNICOS INFORMÁTICOS

OBJETIVO: Medir las seguridades en el acceso al Internet, acceso a contenidos Web de los niños y adolescentes, con el fin de identificar mecanismos de control para mitigar el acceso a contenido inapropiado en el Internet.

INDICACIONES GENERALES:

- Señale con una X la respuesta de tu elección.
- Conteste con total sinceridad a cada uno de los ítems que presentamos.

DATOS INFORMATIVOS:

EDAD: _____ ENTIDAD EDUCATIVA: COLEGIO ☐ ESCUELA ☐
GENERO: FEMENINO☐ MASCULINO☐ AÑO CURSO: _____
LUGAR Y FECHA: _____

PREGUNTAS

1. ¿La Institución dispone de servicio de Internet?
   SI ☐
   NO ☐
   Si la respuesta es NO, termina la encuesta, caso contrario continua con la pregunta 2

2. Tipo de Institución:
   ☐ Pública
   ☐ Privada
   ☐ Otra ¿Cuál? _____

3. Número de estudiantes en el plantel: _____

4. ¿Con cuántos laboratorios de computación cuenta? _____

5. ¿Cuántos computadores de escritorio funcionales dispone? _____

6. ¿Cuántos computadores portátiles funcionales dispone? _____

7. Posee políticas de seguridad
   ☐ SI
   ☐ NO

8. Qué tipo de herramientas de seguridad tiene implementado
   ☐ Software
   ☐ Hardware
   ☐ Ninguna

   ¿Porque? _____

9. Bajo qué Sistema Operativo tiene configurado las seguridades informáticas
   - ☐ Linux
   - ☐ Unix
   - ☐ Solaris
   - ☐ Windows
   - ☐ Otro ¿Cuál? _____

10. Tiene creado perfiles de usuarios para la navegación
    - ☐ SI
    - ☐ NO

11. ¿Dispone de acceso a internet inalámbrico?
    - ☐ SI
    - ☐ NO

    Si la respuesta es NO, continúa con la pregunta 13, caso contrario continua con la pregunta 12

12. ¿El acceso inalámbrico tiene clave?
    - ☐ SI
    - ☐ NO

13. ¿Qué software, hardware o configuración para el control de seguridades tiene implementado?
    - ☐ Firewall
    - ☐ IDS
    - ☐ IPS
    - ☐ UTM
    - ☐ Antispam
    - ☐ Antiphishing
    - ☐ Antispyware
    - ☐ Antivirus
    - ☐ Servidor Proxy
    - ☐ IPTABLE
    - ☐ ACL's
    - ☐ VPN
    - ☐ Filtros Web
    - ☐ Otro ¿Cuál? _____

    Puede elegir varias opciones.

14. ¿Dispone de un Software para filtrar de contenido?
    - ☐ SI ¿Cuál? _____
    - ☐ NO

15. ¿Qué tipos de páginas se encuentra bloqueadas?
    - ☐ Pornografía
    - ☐ Redes sociales
    - ☐ Correo
    - ☐ Descarga de videos y música
    - ☐ Otras ¿Cuál? _____

    Puede elegir varias opciones.

Manual de Registro e Instalación de Control Parental

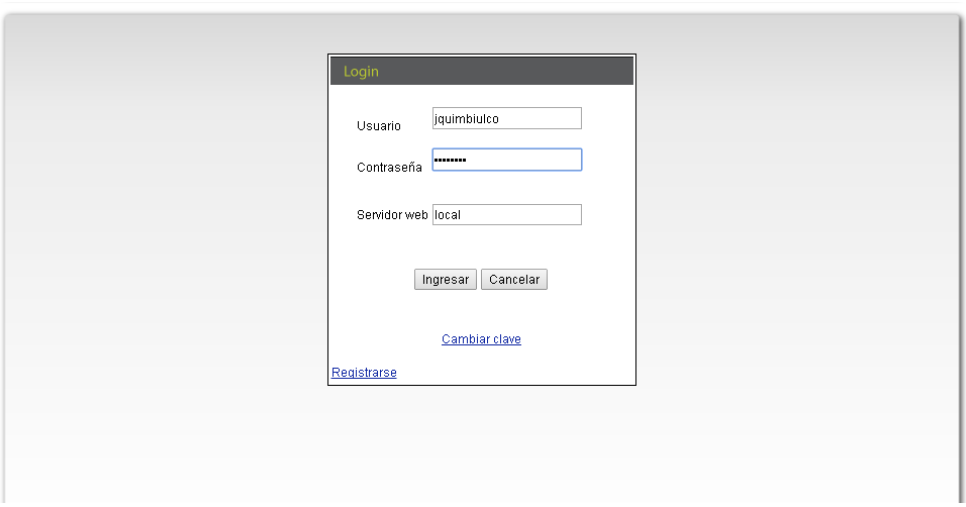
Para acceder a la aplicación se debe dirigir al link:

http://190.216.203.212/Control/Generico/WFrmRegistroUsuario.aspx

1. Se procede abrir la siguiente interfaz, en la que podrá registrarse ingresando los datos solicitados.

2. Una vez ingresados los datos se debe presionar el botón Enviar, una vez registrado presionar el link ingresar.

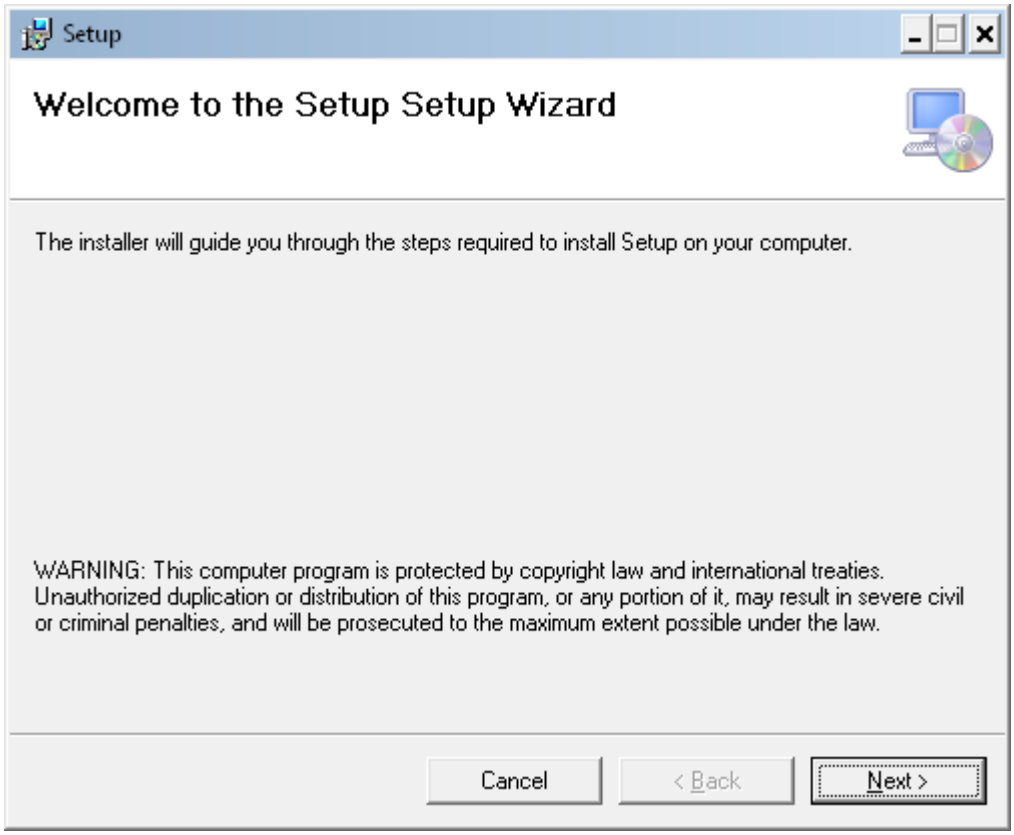
3. Se abre la siguiente interfaz en la que puede colocar el usuario y contraseña que creo anteriormente

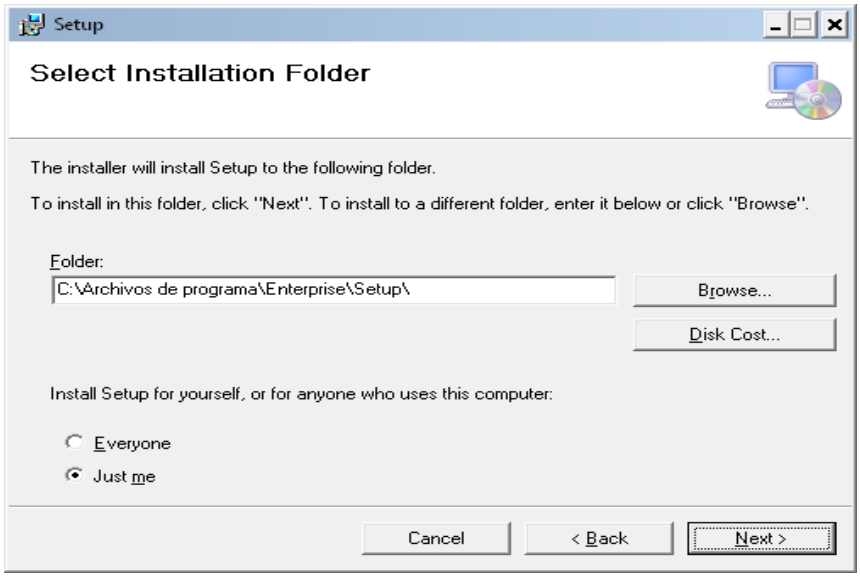


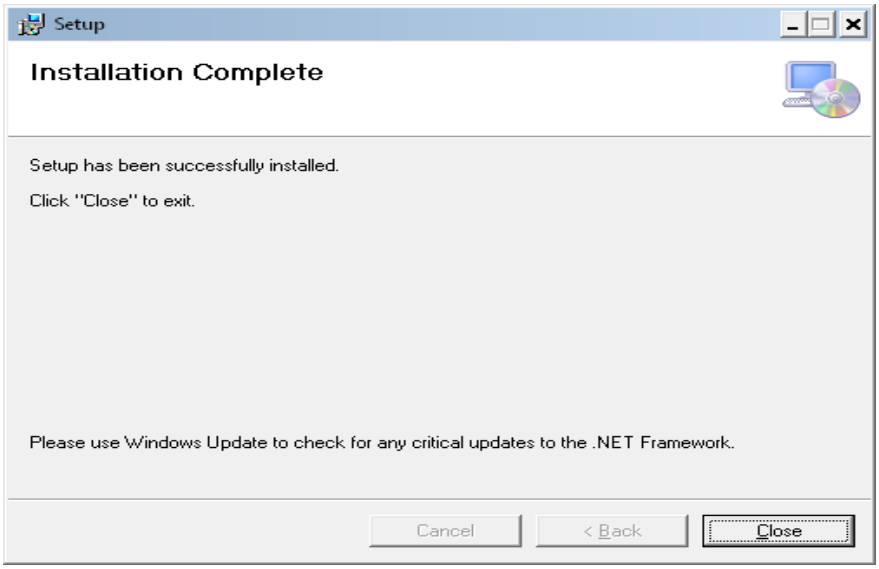
4. Una vez que se ingresa al sistema presionar la opción Descargar, ahí se descargará el instalador que contiene el servicio Windows que permitirá monitorear la navegación en Internet.

5. Ya con el instalador descargado se procede a instalar, seleccionando el instalador.

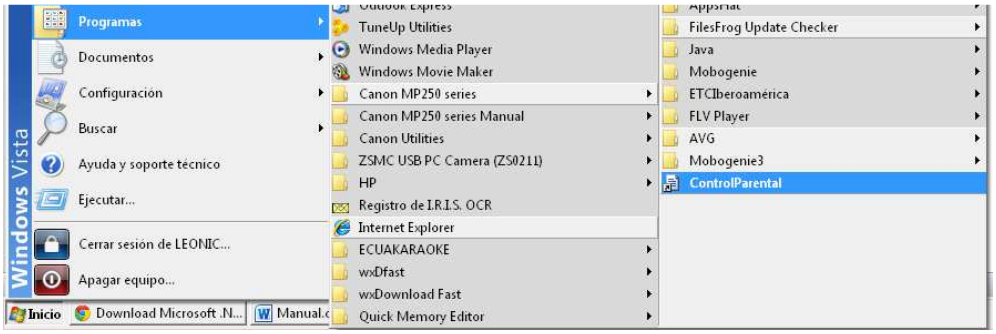
6. El instalador le indica que la instalación ha iniciado, presentando las siguientes interfaces para su instalación.



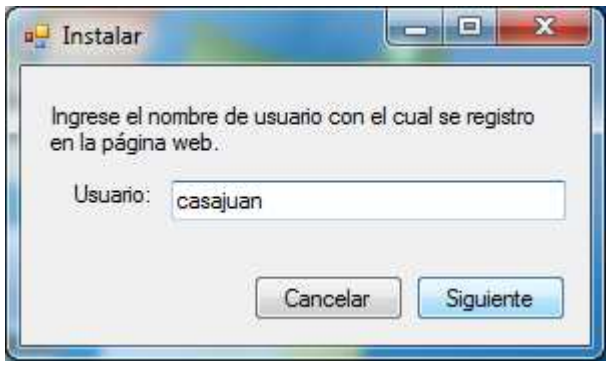




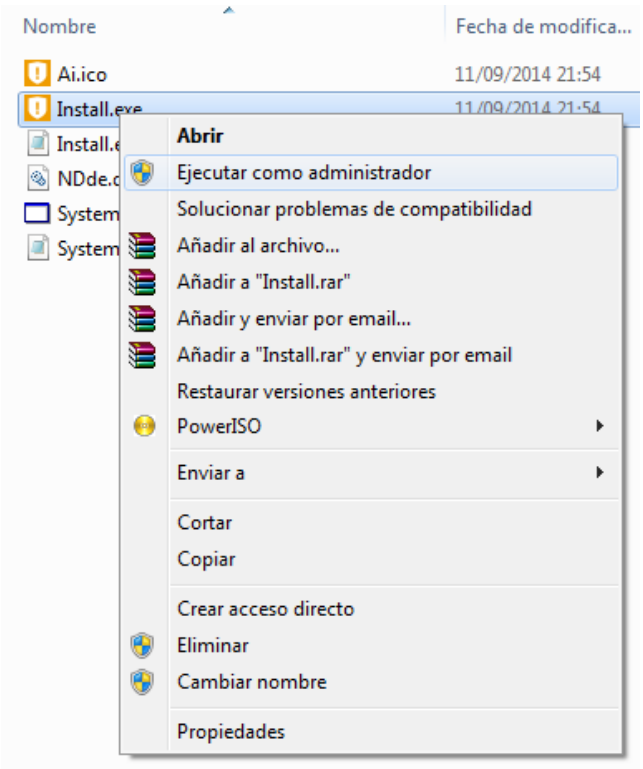
7. Una vez ya instalado dentro de la lista de programas se va encontrar el acceso directo a ControlParental, seleccionarlo para continuar con la configuración.



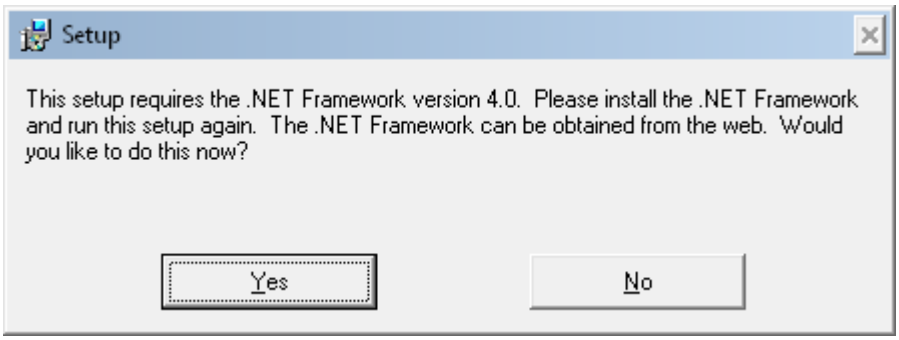
8. Se abre la siguiente Interfaz que debe ser configurada la primera y única vez colocando el usuario que corresponde, a continuación presionar el botón Siguiente.



En algunas máquinas se requiere que se ejecute como administrador dirigiéndose al siguiente directorio C:\Program Files (x86)\Enterprise\Setup, o al que se haya escogido en la instalación.

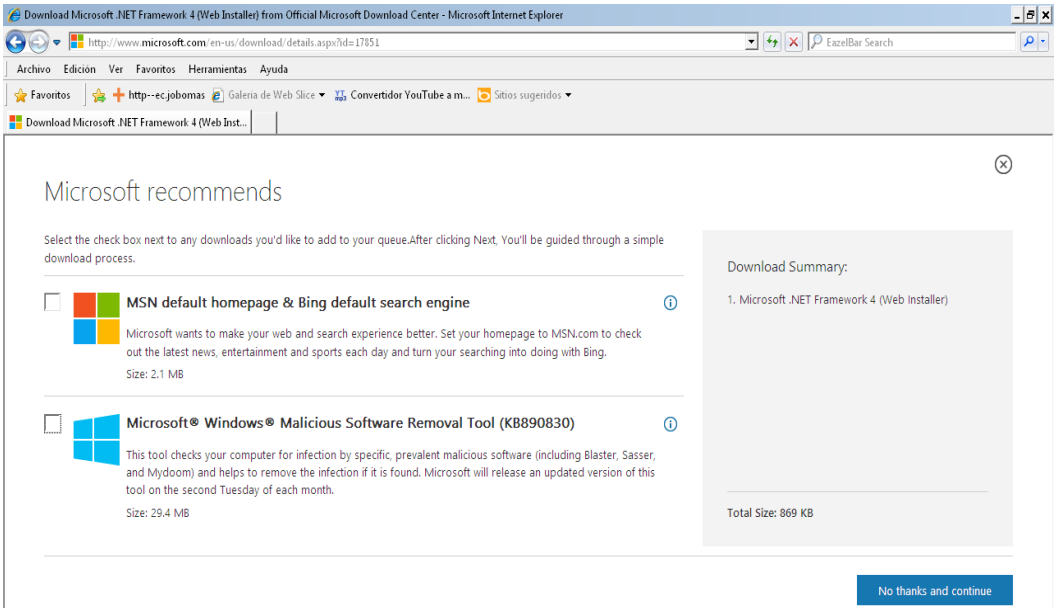


9. Dentro de algunos sistemas operativos que no vienen incluidos Framework, el sistema solicitara que debe tener instalado, este componente se puede obtener gratuitamente.



http://www.microsoft.com/en-us/download/confirmation.aspx?id=17851

10. Descargar y realizar la instalación solicitada.



11. Una vez instalado debe volver a ejecutar los pasos 5, 6, 7 y 8, para confirmar su correcta instalación se debe verificar si el icono Control Contenido está ejecutandose.

LISTADO DE PALABRAS Y SITIOS WEB INADECUADOS

Sitios Web
www.chatiw.com
www.hi5.com
www.facebook.com
www.redtube.com
www.xvideos.com
www.youporn.com
www.puritanas.com
www.tangasmix.com
www.juegos.com
www.instagram.com
www.twitter.com
http://es.bongacams.com/
http://es.gratisonlinesex.com/
http://es.bravotube.net/
Palabras
Sexo
Pornografía
Prostitución
Prostitutas
Matar
Suicidio
Robar
Asesinar
Licor
Drogas
Marihuana
Cocaína
Drogarme
Violación
Terror
Sangriento
Dieta
Pelear
Odio
Racismo
Motel

POR: ING. KARINA QUIMBIULCO, ING. ERNESTO SANGUANO, PHD WALTER FUERTES
MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS, UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE
E-MAIL: karina_tqs@hotmail.com, er_sanguano@hotmail.com, wmfuertes@espe.edu.ec

ACCESO A INFORMACIÓN NO AUTORIZADA,

UN PROBLEMA ÁLGIDO EN LA SOCIEDAD

El acceso a contenidos nocivos a través de la Internet expone a niños y adolescentes a información inapropiada de tipo pornográfico, pedófilo, xenófobo, terrorismo, drogas, armas, asociaciones ilícitas, escenas de violencia, que incrementan la agresividad de sus víctimas.

Ante esta problemática mundial y local se han estableciendo normas y procedimientos que regulen y controlen el mal uso de la Internet. Problemas delicados como el 'grooming' que implica la vulnerabilidad de la inocencia infantil; el 'bullying', que significa la intimidación como un acto de conducta agresiva; y la pornografía, entre otros, están siendo intervenidos por una solución técnica denominada Control Parental, que es una disciplina útil para impedir que niños o adolescentes puedan acceder a páginas web con contenido inapropiado.

En el Ecuador escasamente se ha tratado este tema. A escala gubernamental, por ejemplo, no se han establecido campañas sobre el uso correcto de las herramientas informáticas en los hogares y colegios. La legislación ecuatoriana publicó la Ley y Reglamento de Comercio Electrónico en el 2002, que hace referencia a infracciones informáticas, al uso ilegal de información o violación de sistemas de seguridad [1], sin embargo, no se han enfocado a establecer leyes con sanciones para los proveedores de la Internet y para los propietarios de páginas web con contenido inapropiado.

En este contexto, se realiza un análisis a los siguientes cuestionamientos: ¿Cuál es el porcentaje de uso de la Internet en Ecuador?, ¿cuál es el aporte y beneficios de control parental?, ¿qué técnicas son empleadas? y ¿cuáles son las mejores herramientas para controlar el uso de la Internet? Los resultados muestran que se debe concienciar en el uso de la Internet dentro los hogares, colegios y sitios públicos. Describe además, diversas técnicas y herramientas de control parental que señalan cómo proteger a los menores de edad de los peligros en el acceso a información no apropiada en Internet.

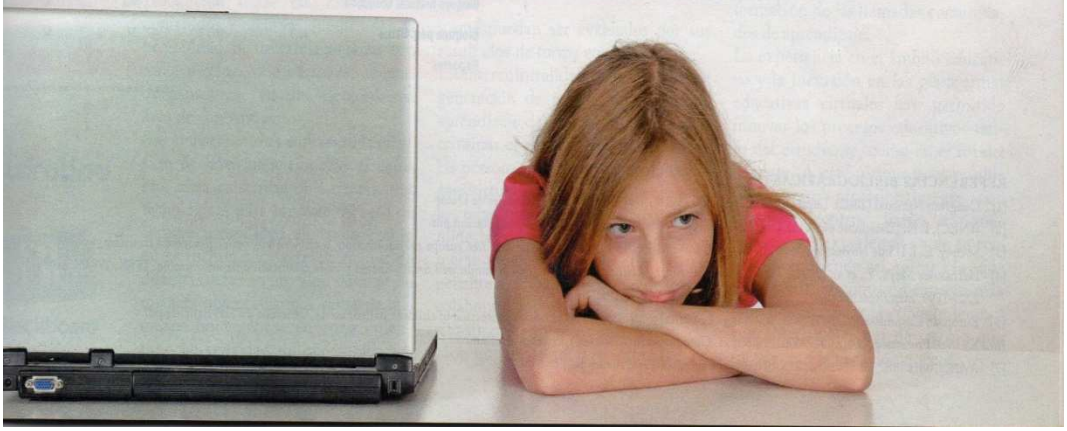
Uso de la Internet en Ecuador

Según la encuesta realizada por el INEC en diciembre del 2011, el 31,4% de la población de Ecuador ha utilizado Internet. De ese porcentaje, el mayor uso se localiza en los hogares con un 38,3%, seguido del 22,0% en las instituciones públicas [2]. Como se puede observar la mayor utilización se observa en los hogares en un escenario que no cuenta con controles básicos para el uso de la Internet.

Al encontrarse el equipo dentro de la casa, lo puede usar un niño con o sin nociones básicas de computación, siendo ellos y los adolescentes los más vulnerables a los peligros que se presentan en las redes sociales, páginas con información inapropiada y chats.

Aporte y beneficio de control parental

Según la Comisión Europea, el control parental ofrece todas las herramientas informáticas que permiten vigilar la navegación en la Internet, bloqueo de aplicaciones, configuración de bloqueo por tiempo, filtros de contenido y monitoreo [3]. No obstante, este sistema no solo se encuentra en las herramientas informáticas, la regulación parental también hace referencia a la conciencia que deben tomar los padres y representantes de niños y adolescentes. Es responsabilidad de los adultos enseñar el uso responsable de la Internet, en razón de que las vulnerabilidades y amenazas señaladas podrían traer graves consecuencias.



Técnicas de filtrado de control parental

Dentro de los métodos de control se pueden citar:

- **Control de navegación:** permite regular a qué sitios es posible acceder con diferentes técnicas de prevención: listas blancas/negras, bloqueo por palabras claves.
- **Bloqueo de aplicaciones:** herramientas que permiten bloquear ciertas páginas web, de mensajería o de correo electrónico.
- **Control de tiempo:** estas herramientas limitan el tiempo o las horas en las que un niño y/o adolescente puede utilizar o conectarse a Internet.
- **Navegadores infantiles:** herramientas que solo permiten el acceso a páginas adecuadas para niños.
- **Herramientas que bloquean la información que se presenta en la computadora:** son aplicaciones que impiden revelar información personal.
- **Monitoreo:** permite supervisar todas las páginas web visitadas.

Como una aplicación de estas técnicas, la Universidad de las Ciencias Informáticas (UCI), en Cuba, efectuó un estudio relacionado con el filtrado de contenido web [4], en la cual una de las características que tiene control parental es realizar un análisis inteligente de la información identificando las categorías que componen una página web como son: texto, imágenes y los enlaces aplicando algoritmos de inteligencia artificial en los controles que filtran contenido.

Conclusiones

El acceso inapropiado a la Internet sin ninguna restricción ha provocado que los niños y adolescentes estén expuestos a peligros como violencia, pornografía, acoso, entre otros. Las herramientas de control parental, su instalación y configuración contrarrestan el problema. Sin embargo, aunque ayuden a controlar el acceso a páginas no apropiadas, siempre existirá un margen de error, por tanto es recomendable culturizar y controlar el uso de la Internet dentro del hogar, particularmente a menores de edad.

Herramientas informáticas de control parental

La tabla 1 presenta la evaluación realizada como resultado de la ejecución de varias herramientas de control parental, en nuestro grupo de investigación luego de la definición de los criterios de comparación:

SOFTWARE / CRITERIO	AMIGO	WINDOWS LIVE PROTECCIÓN INFANTIL	AVIRA INTERNET SECURITY	K9 PROTECTION
Compatible Windows	SÍ	SÍ	SÍ	SÍ
Personaliza filtrado	SÍ	SÍ	SÍ	SÍ
Control parental	SÍ	SÍ	SÍ	SÍ
Fácil instalación	SÍ	SÍ	NO	SÍ
Fácil configurar	NO	SÍ	NO	NO
Gratuito	SÍ	SÍ	NO	NO
Bloqueo motores búsqueda	NO	NO	NO	SÍ
Bloquea pág. Https	NO	NO	SÍ	SÍ
Reportes	SÍ	SÍ	SÍ	SÍ

Tabla 1.- Evaluación de software según criterio

REFERENCIAS BIBLIOGRÁFICAS

[1] Congreso Nacional (2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

[2] (INEC), I. N. (Diciembre de 2011). Obtenido de http://www.inec.gob.ec/sitio_tics/presentacion.pdf

[3] Society, E. I. (15 de Noviembre de 2011). Europe's Information Society. Obtenido de http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7573

[4] Hernández Moya, Y., et al. (2011). Técnicas de Inteligencia Artificial en el filtro de contenido web Smart Keeper para la clasificación de información. ISSN: 1994-1536 | e-ISSN: 2227-1899 http://rcci.uci.cu.

[5] European Commission. (2011). Benchmarking of parental control tools for the online protection of children SIP-BenchII, Obtenido de SIP-BenchII.pdf

[6] K9 Web Protection. (2013). K9 Web Protection. Obtenido de http://www1.k9webprotection.com/

[7] Avira, Avira Internet Security 2013, http://www.avira.com/es/downloads

Mecanismo de Control Parental para Mitigar el Acceso a Información no Apropiada en el Internet

Walter Fuertes[1], Karina Quimbiulco[1], Ernesto Sanguano[1], José Luis García-Dorado[2], Fernando Galárraga[1]
[1]Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas "ESPE", Sangolquí, Ecuador

[2]Departamento de Tecnología Electrónica y de las Comunicaciones, Universidad Autónoma de Madrid, Madrid, España

wmfuertes@espe.edu.ec, karina_tqs@hotmail.com, er_sanguano@hotmail.com, jl.garcia@uam.es, jfgalarraga@espe.edu.ec

RESUMEN

Ante la falta de completitud de las herramientas actuales de Control Parental junto a las nuevas demandas que los padres requieren de estas herramientas, este trabajo presenta el diseño e implementación de mecanismos de Control Parental que exitosamente mitigan y registran el acceso a contenido no apropiado por parte de los niños y adolescentes a través del Internet. De este modo, primero se evaluaron varias herramientas de software valorando funcionalidad, eficacia, usabilidad, seguridad e índice de audiencia las cuales mostraron no ser completas. A continuación se realizó una investigación exploratoria mediante encuestas de una muestra representativa de niños, padres de familia y administradores de redes para determinar la línea base y los requisitos fundamentales de estas herramientas. Finalmente, se juntaron todas las piezas en una aplicación e interfaz computacional agregando criterios de pertinencia y congruencia interna. Cómo método de desarrollo se ha utilizado el Diseño de Hipermedia Orientada a Objetos, combinado con Procesamiento de Lenguaje Natural que utiliza el Modelo de Recuperación Booleano a través de los algoritmos de búsqueda de cadenas Boyer-Moore y búsqueda aproximada de filtrado. Los resultados preliminares muestran que no solo se ha bloqueado el acceso a contenido no apropiado a través del Internet, sino que la propuesta facilita mecanismos a los padres para controlar y medir el uso de Internet de sus hijos como un medio fundamental en el proceso de concienciación en los jóvenes.

Palabras clave: *Control Parental, OOHDM, Procesamiento de Lenguaje Natural, Ciberseguridad.*

ABSTRACT

Given the lack of completeness of the current implementations of parental control software along with the novel characteristics parents' demands on these pieces of software, this project presents the design decisions and implementation of Parental Control mechanisms that both register and avoid inappropriate content accesses by children and teenagers through the Internet. We first evaluated several state-of-the-art tools assessing their functionality, efficiency, usability, security, and accuracy. Then, we conducted an exploratory study spanning surveys of a representative sample of children, parents and network administrators to determine the baseline and the main requirements these sort of software must fulfil. With such foundations, we have implemented an application and front-end interface following criteria as relevance and internal consistency. As development method, we have applied Object Oriented Hypermedia Design combined with Natural Language Processing that uses the Boolean Retrieval Model by means of string searching algorithms as Boyer-Moore and fuzzy string search. The preliminary results show that not only the inappropriate content accesses through the Internet have been blocked, but also that the proposal provides parents with mechanisms to control and measure their children's Internet use as a fundamental mean in the process of prevention and awareness among the young population.

Keywords: Parental Control, OOHDM, Natural Language Processing, Cybersecurity.

1. INTRODUCCIÓN

En la actualidad, los jóvenes y adolescentes corren el riesgo de acceder a información con contenido inapropiado a través del Internet, como pornografía, acoso explícito, riesgo en línea, comunicación agresiva, violencia y terrorismo [1], lo que podría provocar efectos negativos como ser víctimas de un fraude, suplantación de identidad, acoso, adicción y agresividad [2]. De acuerdo con Livingstone et. al. [3] una fracción significativa de los niños y adolescentes entre 9 y 16 años de USA en un estudio del año 2013 accedía a contenido online inapropiado relacionado con la violencia, agresividad, terror, pornografía, violación, racismo, odio, drogas, alcohol, suicidio, anorexia, bulimia y pérdida de la autoestima. Ante este escenario, la comunidad científica ha propuesto una solución técnica denominada Control Parental [4][5] para impedir que niños o adolescentes puedan acceder a páginas Web con contenido inapropiado [6].

De este modo, en los últimos años ha existido gran interés en la industria para implementar herramientas de software de Control Parental que se ha convertido en una disciplina en constante desarrollo sobre todo desde un punto de vista comercial. Existen numerosos ejemplos de aplicaciones [7] como Norton Online Family, K9 Web Protection, Mcafee Family Protection, *Kaspersky Pure,* entre otras, que ciertamente mitigan el impacto de los problemas descritos pero no acaban con ellos. La razón es que aparecen constantemente nuevas amenazas o las tradicionales crecen a tasas muy significativas [6]. Ejemplos de nuevas amenazas son el cyber *grooming,* que implica la vulnerabilidad de la inocencia infantil; o el cyber*bulling*, que representa la intimidación como un acto de conducta agresiva. Y es por ello que la comunidad científica está buscando nuevas soluciones tecnológicas para atajar estos problemas. Ejemplos de investigaciones en este sentido son [9] donde los autores proponen un marco de trabajo que puede analizar contenidos de adulto remotamente en dispositivos inteligentes basados en Android; en [10] por su parte se desarrolló un sistema de reconocimiento de ataques de *cyber grooming* en tiempo real utilizando controladores de lógica difusa activando alarmas para padres. De manera complementaria la comunidad científica ha prestado atención a como estas herramientas pueden ser útiles en el los procesos de concienciación y prevención de la población juvenil. Esto es, no solo bloquear el acceso sino servir como mecanismos que permitan alertar a los padres quienes a su vez deben conciliar y hacer entender a los jóvenes las problemática de la cuestión [8]. En este sentido, en [5] los autores implementan un método de control de contenido basado en modelos colaborativos, donde los padres y los niños interactúan configurando las restricciones y filtros.

La presente investigación tiene como objetivo, establecer un procedimiento metodológico para diseñar, implementar y evaluar mecanismos de Control Parental que mitiguen el acceso a páginas Web con contenido inapropiado y facilite a los padres información útil en la tarea de educar a sus hijos. Para llevarlo a cabo se evaluaron herramientas de

Control Parental que permita valorarlas con criterios de funcionalidad, eficacia, usabilidad, seguridad e índice de audiencia (rating). Luego se procedió a elevar una encuesta a niños, padres y administradores de red, que permita conocer la línea base. Con este fundamento, se ha implementado una interfaz computacional agregando criterios de pertinencia y congruencia interna. Cómo método de desarrollo de aplicaciones Web se ha utilizado el Diseño de Hipermedia Orientada a Objetos, combinado con Procesamiento de Lenguaje Natural que utiliza el Modelo de Recuperación Booleano para la búsqueda por palabra clave y filtrado de contenido.

El resto del artículo ha sido organizado de la siguiente manera. En la Sección 2 se describe el marco teórico referencial que fundamenta esta investigación. En la Sección 3 se expone el diseño de la investigación compuesto por la evaluación herramientas de software de Control Parental, el análisis de los resultados del instrumento de medición y la descripción de la propuesta metodológica para el diseño, implementación y pruebas de la herramienta de Control Parental. La Sección 4 muestra los resultados obtenidos y su discusión. En la Sección 5, finalmente, se exponen las conclusiones y trabajo futuro.

2. MARCO TEORICO

2.1 Software de Control Parental

De acuerdo con Marcelo y Martín [11], el software de Control Parental está formado por una serie de herramientas que permiten a los padres estar informados sobre lo que hacen sus hijos con las nuevas tecnologías, y en caso necesario, controlar el acceso a determinadas páginas Web. En este mismo contexto, según la Comisión Europea, el Control Parental es el conjunto de herramientas informáticas que permiten controlar la navegación en Internet, bloqueo de aplicaciones, bloqueo por tiempo, filtros de contenido y monitoreo [12]. No obstante, el control no solo se encuentra en el software, el Control Parental también hace referencia a la conciencia que deben tomar los padres y representantes de niños y adolescentes, enseñando el uso responsable del Internet, en razón de las graves consecuencias que se derivan por falta de control.

Dentro de las principales técnicas de Control Parental, se pueden citar: (1) *Control de navegación* que permite controlar a qué sitios es posible acceder, con diferentes técnicas de prevención como listas blancas/negras, bloqueo por palabras clave; (2) *Bloqueo de aplicaciones* que permite bloquear ciertas páginas, mensajería, o correo electrónico; (3) *Control de tiempo* que limitan el tiempo o las horas en las que un niño y/o adolescente puede conectarse al Internet; (4) *Navegadores infantiles* que permiten el acceso a páginas adecuadas para niños; y (5) Monitoreo que permite supervisar todas las páginas web visitadas. Nuestra propuesta tiene una combinación de algunas de estas técnicas.

2.2 Cibernética Social & Cibermetría

Es una teoría interdisciplinaria que tiene como objetivo estudiar a la persona quien está directamente ligada a las redes sociales y los adolescentes que acceden de manera constante al Web [13].

La Cibermetría, por su parte*, e*s una disciplina dedicada a la descripción cuantitativa de los contenidos y procesos de comunicación que se producen en el ciberespacio [14]. Esta trabaja en torno a la información que circula en la Web, obteniendo datos importantes de acuerdo a la necesidad. Analiza, diversos factores, como la presencia de una institución o país en la red, las bases de datos y las herramientas de Internet, como sitios Web, servidores de correo electrónico, foros de debate, sitios de información bibliométrica, etcétera.

En nuestra propuesta han aprovisionado el uso de técnicas y métricas para analizar el comportamiento de los participantes y ciertos factores que lo inducen.

2.3 Procesamiento del leguaje natural (PLN)

El PLN es una “sub-disciplina de la Inteligencia Artificial y rama de la ingeniería lingüística computacional, que pretende lograr que una computadora aprenda a interpretar el lenguaje natural a través de dos caminos, uno epistemológico y otro heurístico: El epistemológico define el espacio de conceptos que el programa puede aprender. El heurístico define los algoritmos para el aprendizaje. Busca crear programas que puedan analizar, entender y generar lenguajes que los humanos utilizan, de manera que el usuario pueda llegar a comunicarse con el computador de la misma forma que lo haría con un humano” [15]. Existen algunas aplicaciones del PLN entre las cuales se encuentran la corrección de textos, traducción automática, recuperación de la información, extracción de información, resúmenes, búsqueda de documentos, sistemas inteligentes para la educación y el entrenamiento. En esta investigación se ha utilizado el algoritmo de búsqueda de cadenas secuenciales de Boyer-Moore, y el algoritmo de búsqueda aproximada de filtrado, como modelos de recuperación de la información.

2.4 Metodología de Diseño Hipermedia Orientada a Objetos (OOHDM)

OOHDM es una metodología de diseño de hipermedia, que utiliza el enfoque orientado a objetos, con técnicas de representación gráfica de relaciones entre objetos y de contextos navegacionales que proveen representación estructural y semántica [16]. Esta metodología se basa en cuatro etapas: diseño conceptual, diseño navegacional, diseño abstracto de interface e implementación. Ha sido escogida en esta investigación porque reúne las características necesarias para distinguir aspectos conceptuales (modelo del dominio) de su presentación (construcción de la interfaz de usuario). La metodología OOHDM es apropiada para desarrollo de sistemas Web simples y complejos. Las ventajas que ofrece son una clara identificación de los diferentes niveles de diseño en forma independiente de

la implementación y la forma gráfica que se usa para representar los modelos [17].

3. DISEÑO DE LA INVESTIGACIÓN

3.1 Evaluación de las herramientas de Control Parental

Con el fin de identificar algunos criterios de comparación y descubrir fortalezas y debilidades de las diferentes herramientas se realizó dos tipos de evaluaciones: (1) Mediante la definición propia de criterios de comparación; (2) Mediante el Benchmarking de herramientas de Control Parental que utiliza sus propios criterios.

Para el primer caso, la Tabla 1, muestra el resultado de evaluar varias herramientas de Control Parental, en función de criterios de compatibilidad, personalización, facilidad de instalación, precio y tipo de bloqueo. En el listado de herramientas se muestra a *K9 Web Protection* como uno de los mejores sistemas de protección, adicional a esta herramienta se analizó *Windows Live Protección Infantil, Amigo y Avira*. En la tabla también se muestran los criterios de comparación definidos y el cumplimiento o no de cada una de ellas.

Tabla. 1. Evaluación de Software según criterio de comparación.

HERRAMIENTA DE SOFTWARE/CRITERIO	H1	H2	H3	H4
Compatible Windows	SI	SI	SI	SI
Personaliza filtrado	SI	SI	SI	SI
Control Parental	SI	SI	SI	SI
Fácil Instalación	SI	SI	NO	SI
Fácil Configurar	NO	SI	NO	NO
Gratuito	SI	SI	NO	NO
Bloqueo motores búsqueda	NO	NO	NO	SI
Bloquea pág. HTTPS	NO	NO	SI	SI

H1: AMIGO; **H2**: LIVE PROTECTION, **H3**: AVIRA; **H4**: K9 PROTECTION

Para el segundo caso, y luego de este primer análisis se ha tomado como referencia la investigación efectuada en la Unión Europea sobre el software de Control Parental, de acuerdo a otros criterios como funcionalidad, efectividad, usabilidad, seguridad e índice de audiencia (rating). La Fig. 1 muestra el análisis realizado en base al benchmarking de herramientas de Control Parental para la protección Online de niños elaborado por SIP-BENCH III [7].

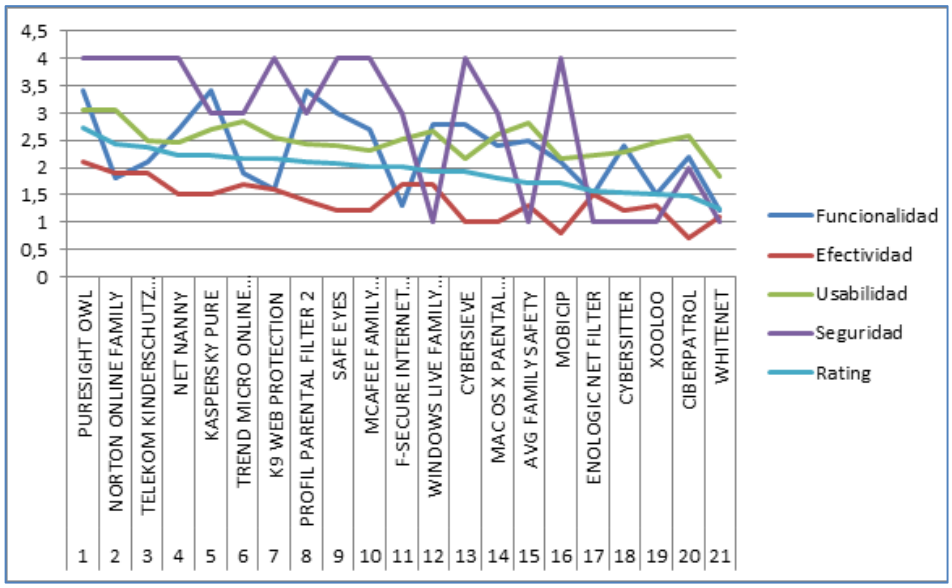


Figura Nº 1. Evaluación de Software según Benchmarking

Como se puede observar, el benchmarking provee un informe completo de los cinco criterios señalados de 21 herramientas evaluadas según SIP-BECH-III [7]. Este estudio además ayuda a los usuarios finales, en particular a padres y custodios de niños a elegir la herramienta de Control Parental más adecuada que mejor se adapte a sus necesidades.

Los datos de la Fig. 1 corresponden a una media de ocho meses de evaluaciones de expertos de estos productos, herramientas u otros sistemas y servicios que permiten a los usuarios controlar el acceso a contenidos inapropiados para niños en línea. Con un rango establecido de 1 a 4 para la calificación, se establece que ninguna de las 21 herramientas probadas alcanza la cobertura de la funcionalidad completa. La que más se acerca tiene 3,4; otras 7 están clasificadas bajo 2. Los 3 productos de más alta puntuación son: *Kaspersky Pure* (3,4), *Profil Parental Filter* 2 (3,4) y *PureSight Owl* (3,4). Por tanto el promedio de satisfacción está bajo 3,5. Extrapolando estos resultados conviene diseñar e implementar un mecanismo similar que resuelva algunas de estas limitaciones en una propuesta propia de Control Parental, añadiendo criterios de pertinencia y congruencia interna (i.e., que responda a nuestra realidad).

3.2 Diseño y aplicación de los instrumentos de investigación

Para continuar con el estudio de línea base, se realizó una investigación sobre el uso de Internet por parte de los menores de edad, estableciendo una muestra representativa en el Valle de los Chillos, ciudad de Sangolquí, provincia de Pichincha, Ecuador. Se tomó como referencia a colegios públicos y privados de esta zona. Así mismo se identificaron variables como el número de accesos a sitios Web de niños y adolescentes estudiantes de distintos colegios de esta localidad, además de las herramientas de filtrado de contenido Web de acuerdo a los datos establecidos en el apartado 3.1. Para conocer cuál es el uso que los niños y adolescentes dan al Internet, se realizaron encuestas tomando como referencia los datos entregados por el

Ministerio de Educación los cuales se encuentran publicados en la Web [18]. Para determinar el dominio, se investigó la cantidad de colegios que existen en el Valle de los Chillos y el número de alumnos matriculados en el periodo lectivo 2013-2014.

Para determinar el número de encuestados en base a los datos adquiridos del Ministerio de Educación [18], se procede a obtener el cálculo del tamaño de la muestra aplicando la ecuación (1):

$$n = \frac{(k^2) * N * p * q)}{(e^2 * (N-1)) + ((k^2) * p * q)} \quad (1)$$

Dónde:

- n: es el tamaño de la muestra (número de encuestas que se van a realizar);
- N: es el tamaño de la población o universo (número total de estudiantes);
- k: es una constante que depende del nivel de confianza que sea asignada; El nivel de confianza indica la probabilidad de que los resultados de la investigación sean ciertos;
- p: es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p = q = 0.5 que es la opción más conservadora;
- q: es la proporción de individuos que no poseen esa característica, es decir, es 1- p.

Con los datos calculados se diseñó y levantó tres tipos de encuestas: (1) encuesta dirigida a los estudiantes entre las edades 11 a 17 años pertenecientes a colegios públicos y privados de la muestra calculada, con el fin de identificar el tipo de información, amenazas y medios de vigilancia en el acceso a contenidos Web; (2) encuesta dirigida a los padres y representantes de los adolescentes, con el fin de medir el grado de control y protección que los padres tienen frente al uso de Internet para los niños y adolescentes; y (3) encuesta dirigida a los técnicos de colegios con el fin de verificar las técnicas de control y mitigación que son establecidas por el administrador de red para sus usuarios.

Luego del procesamiento estadístico descriptivo, los resultados de las encuestas (véanse Fig. 2, 3, y 4) ilustran que en la muestra establecida, no se están tomando las medidas preventivas de Control Parental, tanto de padres de familia o representantes, así como de los responsables de la administración de la seguridad de las redes. Los padres no conocen como bloquear el acceso a sitios Web, y no todos realizan procesos de supervisión, sin embargo de que los estudiantes pueden acceder desde cualquier sitio, en cualquier hora y utilizando cualquier dispositivo sea personal, familiar o institucional, lo cual en principio valida la hipótesis de investigación de nuestra propuesta.

Además, en base al cruce de las encuestas realizadas se determina una falta de control y protección por parte de los padres. Esto se debe a que no

existe la cultura de protección en el Internet para las personas más vulnerables como niños y adolescentes por parte de sus padres o custodios. Se debe además al desconocimiento de las herramientas de Control Parental existentes. De igual manera se debe la complejidad de configuración de estas herramientas, sobre todo en los usuarios que no manejan la tecnología.

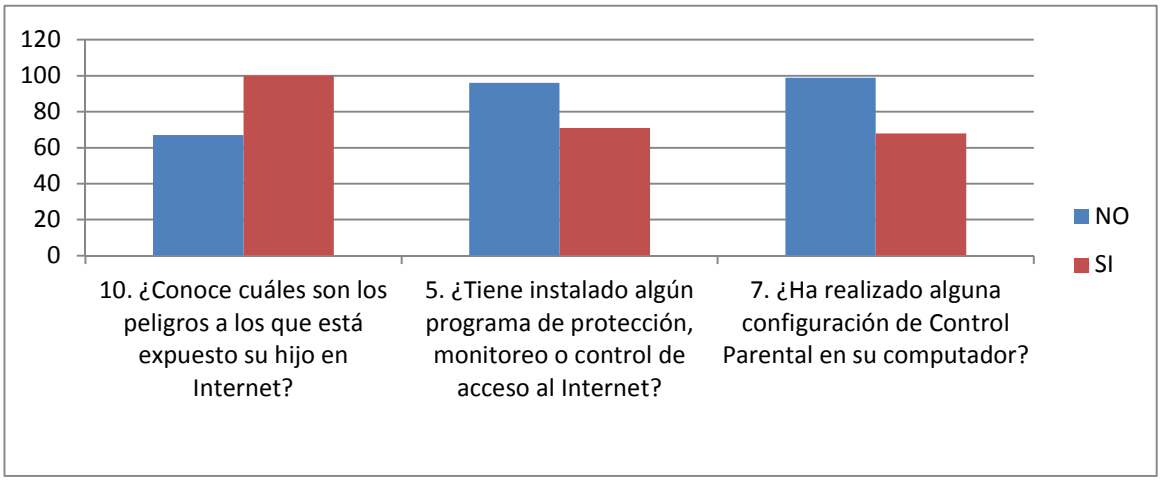


Figura Nº 2. Preguntas a los padres o representantes

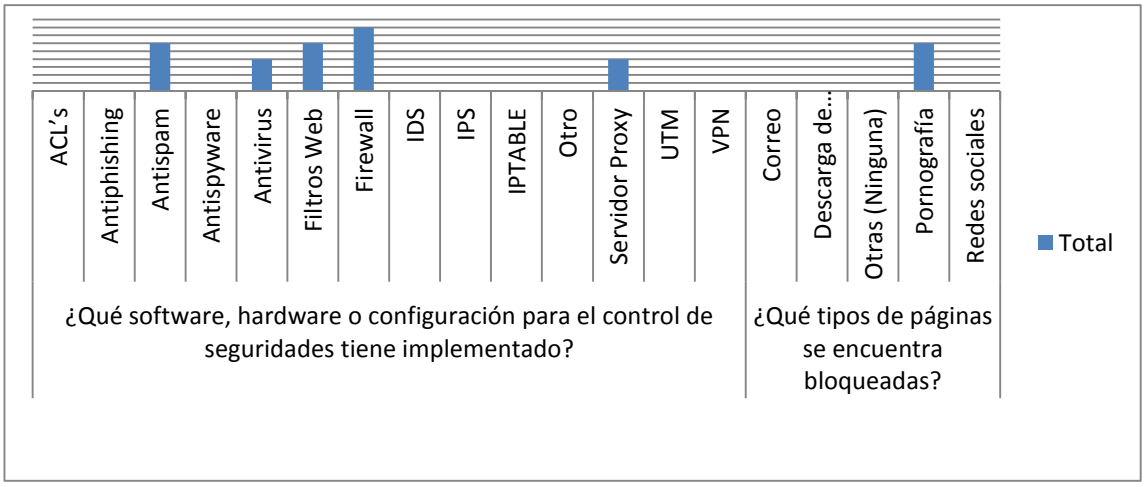


Figura Nº 3. Preguntas a administradores de seguridad y sitios Web en los colegios.

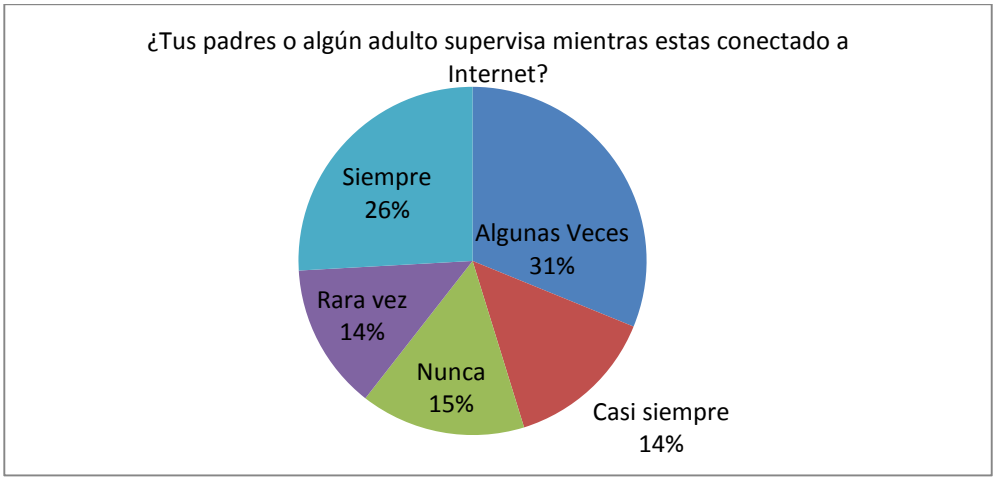


Figura Nº 4. Pregunta a los adolescentes

Sobre la base de estas consideraciones, y las deficiencias encontradas y explicadas en el apartado 3.1, se justifica la necesidad de desarrollar un mecanismo propio que ayude al control de la navegación y al bloqueo de sitios Web con contenido inapropiado.

3.3 Diseño del Mecanismo de Mitigación

Continuando con el procedimiento, luego de la investigación preliminar descrita en los apartados 3.1 y 3.2, y de comprender como funciona un mecanismo de Control Parental, se diseñó una propuesta distintiva. Elegimos OOHDM que es una metodología que permite el desarrollo hipermedial de aplicaciones Web mediante fases claramente establecidas, con un enfoque de proceso de Ingeniería de Software. El diseño inició con la definición de requerimientos funcionales identificado roles y tareas de administrador/usuario así como la especificación de escenarios. Además se definieron lo requisitos no funcionales y los respectivos diagramas de casos de uso.

Para la fase de Diseño, la Fig. 5 ilustra el Modelo Conceptual de la propuesta que representa la estructura del dominio de la aplicación. Cada una de las entidades (clases) y sus respectivas relaciones toman en cuenta el papel de los usuarios desde su perfil y las tareas que desarrollan. Además muestra cómo se registran datos importantes para la clasificación de la información y filtrado de contenidos, como palabras claves y páginas Web de búsqueda ingresada por los usuarios permitiendo registrar información significativa para los padres y o representantes de los menores. Las entidades que almacenan los datos de mayor importancia son: *TUSUARIO*, en donde se registran todos los usuarios (padres de familia e hijos) que podrán acceder a la aplicación y el servicio de control; la entidad *CONTENIDO* donde se encuentran las palabras y sitios Web parametrizados que se desean bloquear por el usuario; y la entidad *TLOGCONTENIDO* que contiene los registros de intentos de búsqueda o accesos a páginas no apropiadas.

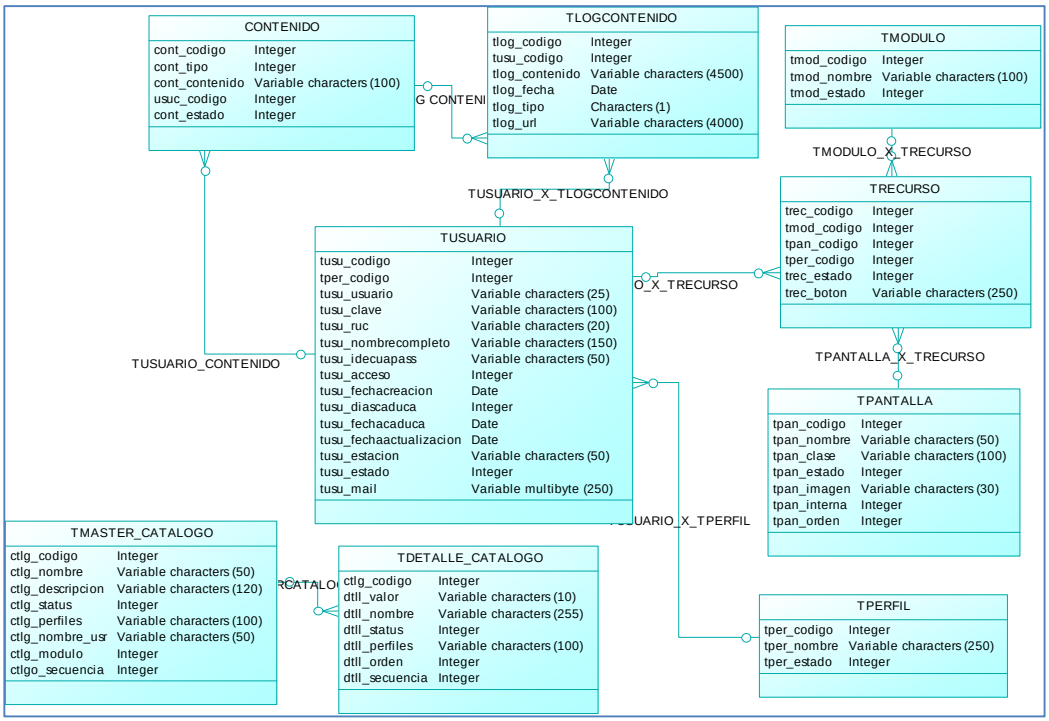


Figura Nº 5. Diseño conceptual

La Fig. 6 ilustra en cambio el Modelo Navegacional que representa el flujo que nuestra propuesta contiene (i.e., nodos y enlaces) de acuerdo con los diferentes perfiles de usuario. Este modelo provee una vista subjetiva del modelo conceptual tomando en cuenta que se presentan en dos ambientes: el que se encuentra publicado en la Web como administración y el servicio que está instalado en la computadora del cliente monitoreando las acciones dentro del Internet conectándose a una base de datos centralizada en un servidor Web para la alimentación de los datos.

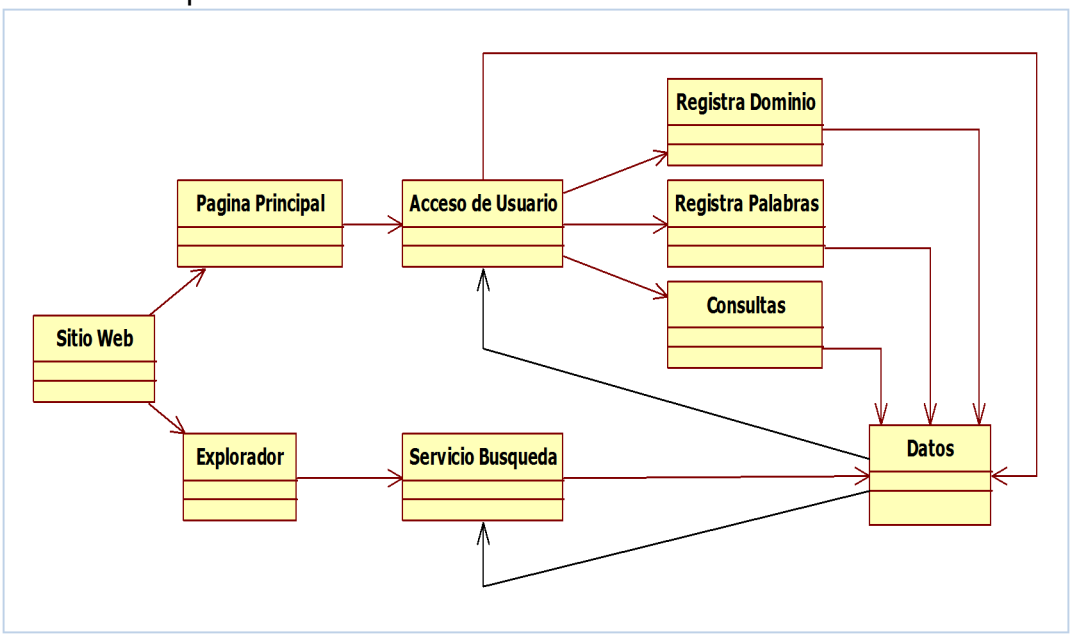


Figura Nº 6. Diseño Navegacional

3.4 Implementación del Mecanismo de Control

La Fig. 7 muestra la arquitectura del proyecto, cuyos elementos se ensamblan en forma ascendente partiendo de la capa de datos, la lógica del negocio, el gestor de comunicaciones, la interfaz computacional basada en Web y el usuario.

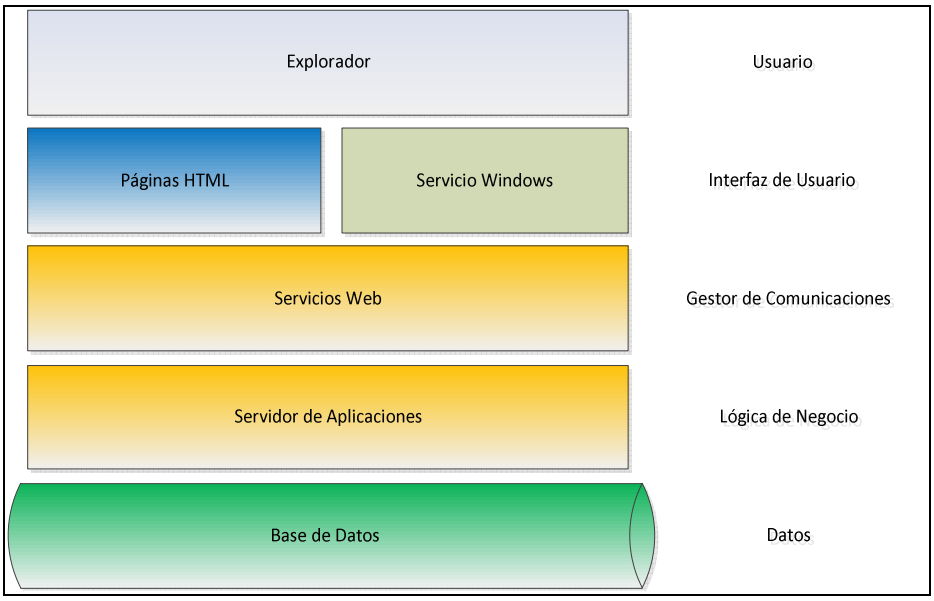


Figura Nº 7. Arquitectura del proyecto Control Parental

La herramienta de desarrollo que se utilizó fue Punto Net, y PosgreSQL Server 2008 como servidor de bases de datos para almacenar los accesos de los clientes que utilizarían esta propuesta. Para el control de acceso a sitios Web que tengan contenido inapropiado, esta propuesta se basó en el aprendizaje de palabras clave y sitios Web registrados. El mecanismo controla dentro de cada máquina el bloqueo de las páginas Web con palabras restringidas, el bloqueo de páginas Web que han sido registradas que no deben ser accedidas, y las listas negras. El sistema articula lo anterior con la base de datos centralizada, el registro de restricciones, el control de acceso a páginas Web y el registro de log de accesos, que son componentes que otorga seguridad en nuestra solución. La Fig. 8 muestra el diagrama de flujo del algoritmo programado en un primer nivel de explosión (abstracción) utilizando el modelo de recuperación booleano y la búsqueda aproximada de palabras restringidas.

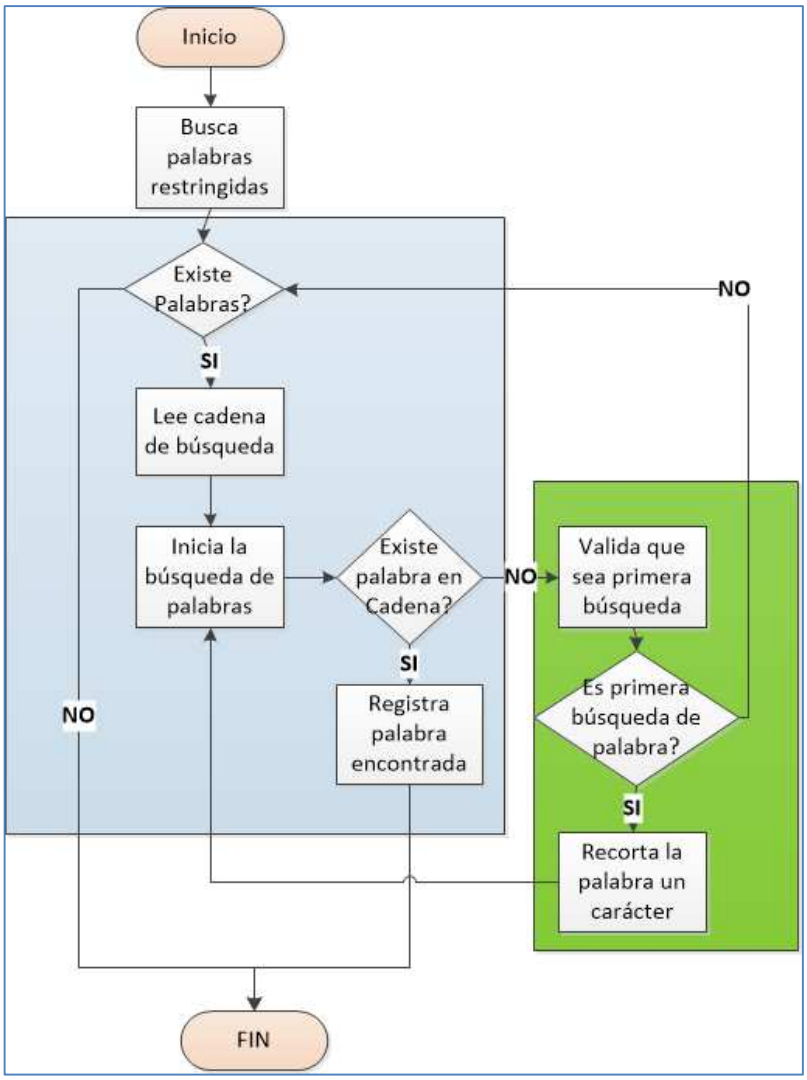


Figura Nº 8. Algoritmo de Bloqueo de páginas Web por palabras restringidas

Como se puede apreciar en la Fig. 8, el proceso de búsqueda de palabras se basa en dos algoritmos; de Boyer-Moore (color celeste) permitiendo la búsqueda de las palabras registradas dentro de todo el texto que contenga una página Web. En el caso de no ser encontrada una palabra se procede con la ejecución del algoritmo de búsqueda aproximada (color verde de la figura) obteniendo la palabra a buscar y disminuyendo al final un carácter verificando dentro de la página Web.

Cuando el usuario intenta abrir una página Web, el algoritmo inicia la búsqueda comparando la *meta data* de la página Web, que vendría a ser el texto o cadena, recorriendo el texto de izquierda a derecha, pero comparando el patrón con el texto de derecha a izquierda. Las palabras restringidas que constan en la matriz de palabras claves (patrón) o en la matriz de sitios Web restringidos, fueron previamente clasificadas por el sistema y modificadas o añadidas (de ser el caso) por el usuario. Para tener mayor eficiencia se minimiza el número de comparaciones entre palabras, es

decir si se encontró una palabra restringida ya no se realizan más búsquedas. En caso de no tener éxito con la búsqueda de palabras registradas se procede a recortar la palabra en un carácter al final y busca nuevamente en la cadena de búsqueda, permitiendo así tener palabras aproximadas a las que han sido restringidas. Si finalmente no tiene palabras restringidas se abre la página Web y el usuario continúa con la navegación. Caso contrario, bloquea el acceso a la página Web, almacena la palabra y sitio Web restringido y la presenta como acceso no permitido. En ambos casos se registra en la base de datos centralizada la información del acceso (fecha y hora de acceso, URL, cantidad de bytes), y los datos del usuario.

3.5 Ambiente de pruebas

Las pruebas de contenido, componentes, usabilidad, navegabilidad, y desempeño ayudaron a detectar y corregir los errores antes de la puesta en marcha del prototipo. La aplicación fue publicada en un servidor Web con Windows 2008 e Internet Information Server, Framework 4.0 y permaneció abierta durante un mes.

El sitio Web permitió acceder a los padres de familia que aceptaron probar el mecanismo de manera gratuita, a instalar el servicio que permite controlar el acceso a páginas con contenido inapropiado. El servicio se instaló en los computadores de varios hogares que formaban parte de la muestra representativa analizada. Los padres pudieron modificar las opciones de seguridad del prototipo. Así mismo pudieron acceder a reportes que presentan la búsqueda o intento de ingreso a páginas restringidas, con lo cual supervisaban el comportamiento de los accesos a Internet de sus familias, opcionalmente sin que sus hijos lo conozcan. Por su parte el administrador general de esta propuesta tenía acceso a toda la base de datos en dónde se registraban los diferentes usuarios y los accesos a través del Internet.

4. EVALUACIÓN DE RESULTADOS Y DISCUSIÓN

4.1 Evaluación de Resultados

Como resultado del registro de un mes en ambiente de pruebas, manteniendo principios de ética y confidencialidad, se realizó el procesamiento de la información, cuyos resultados han permitido conocer los patrones de acceso de los usuarios, por edad, fecha, sitio Web y su contenido. Así mismo se pudo determinar la frecuencia de búsqueda a sitios Web, categorizándolos por educación, salud, negocios, pornografía, malware y, spyware, etc.

Entre los principales resultados se registraron 55.307 accesos. Los sitios más visitados son: Web 2.0: foros, chat, redes sociales (16,417, 30%); almacenamiento en línea y servidores de contenido (13.016, 24%); sitios Web de entrenamiento: imágenes, juegos, videos compartidos (6.939, 13%). Se puede apreciar que si existieron accesos a sitios Web de pornografía (645, 1%). Menos del 0,001% equivalen a sitios Web sospechosos, spyware y malware. Esto demuestra que siempre existe interés por parte del público en general a contenido inapropiado.

Para poder analizar el comportamiento de los niños y adolescentes en edades comprendidas entre 9 y 16 años, se procesaron 10.126 registros del total de 55.307. La Fig. 9 muestra el porcentaje de acceso a sitios Web por contenido. Como se puede observar el 26% representa el acceso a videos compartidos (YouTube). El 25% representa a otros sitios Web, que el mecanismo no puede identificar concretamente. El 16% representa el acceso a redes sociales (Facebook, twitter). El 13% a buscadores (Google, Yahoo!). Sin embargo, se puede notar también que existieron 224 accesos a contenidos de pornografía, que representa el 2%, lo que demuestra una vez más el interés que tienen los niños o adolescentes de acceder información de contenido inadecuado.

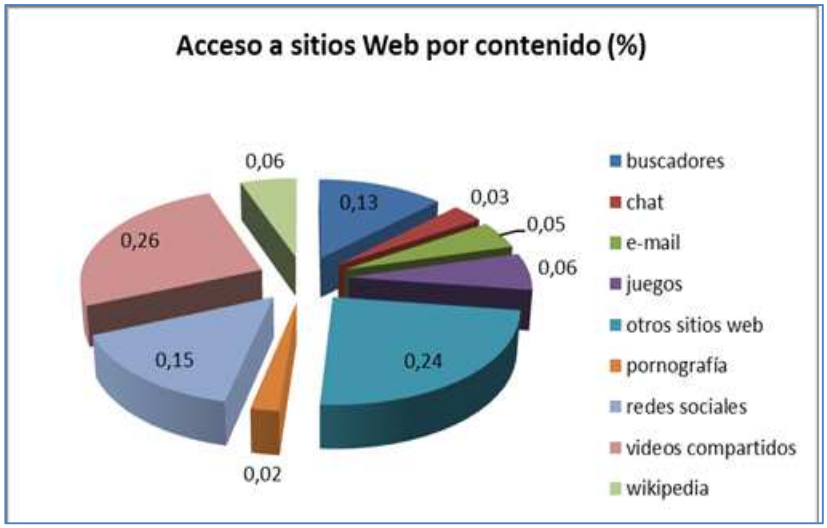


Figura Nº 9. Gráfico de barras del resumen de número de accesos por tipo de contenido.

4.2 Discusión

Nuestro mecanismo de Control Parental ha permitido detectar cuál es el uso que los niños y adolescentes dan al Internet. Lo más primordial, fueron bloqueados los sitios Web de contenido inapropiado para los niños y adolescentes lo cual modificará su comportamiento. Sin embargo, como se ha podido apreciar durante toda la investigación, el Control Parental no solo es software y reglas de filtrado. En este contexto, conviene educar a los niños y adolescentes desde una edad temprana de los posibles riesgos y consecuencias del acceso a contenido no apropiado. Los menores no pueden perder de vista la privacidad y la confidencialidad de cierta información. No deben tener contactos con desconocidos. No deben descargar programas maliciosos, pues podrían incluir virus, gusanos, spyware, troyanos, etc. Los padres deben acompañar a sus hijos y deben tener un control visual cuando el adolecente este utilizando el equipo. Cuando no estén cerca de ellos, debe estar instalada una herramienta de software de Control Parental para impedir y registrar el acceso a contenido no apropiado de niños y adolescentes.

5. CONCLUSIONES Y TRABAJO FUTURO

Esta investigación tuvo como propósito establecer el procedimiento metodológico para el diseño, implementación y pruebas de un mecanismo de Control Parental que permita analizar comportamientos y que además mitigue el acceso a contenido no apropiado en el Internet por parte de los niños y adolescentes. Este procedimiento se fundamentó en la evaluación de varias herramientas de software de Control Parental; en el análisis del instrumento exploratorio de medición; y en las diversas fases de OOHDM para implementar una interfaz computacional introduciendo un algoritmo de Procesamiento de Lenguaje Natural que utiliza el Modelo de Recuperación Booleano para la búsqueda por palabra clave y filtrado de contenido. Nuestra propuesta además de los criterios de funcionalidad, eficacia, usabilidad, seguridad e índice de audiencia, ha añadido criterios de pertinencia y congruencia interna. Los resultados preliminares muestran que las técnicas que se utilizan en nuestra propuesta han registrado por categorías el número de accesos, lo que permite un mayor control de la actividad de los menores en Internet y es por tanto una herramienta muy útil para los padres en la tarea de educar a sus hijos.

Como trabajo futuro se planea perfeccionar este proyecto mediante Inteligencia Computacional, modificarlo e instalarlo en dispositivos móviles. Después, estudiar en mayor detalle el impacto que en el tráfico y en el uso de Internet tiene la aplicación de controles como los aquí explicados en la población joven.

Referencias Bibliográficas

[1]. Smahel, D. & Wright, M. F., “Meaning of online problematic situations for children. Results of qualitative cross-cultural investigation in nine European countries London: EU Kids Online, London School of Economics and Political Science, 2014.

[2]. Chhachhar Abdul Razaque, Qureshi Barkatullah, Maher Zulfiqar Ahmed, Ahmed Shakil, “Influence of Internet Websites on Children Study. Journal of American Science; 10 (5):40-45]. (ISSN: 1545-1003), 2014.

[3]. Livingstone S., Kirwil L, Ponte, C., Staksrud E., “In their own words: What bothers children online? With the EU Kids Online Network, February 2013, Available at: http://eprints.lse.ac.uk/48357. Last acceded 22/08/2014

[4]. Livingstone S., Helsper E., “Parental mediation and children’s Internet use”. Journal of broadcasting & electronic media, 52 (4). pp. 581-599. ISSN 0883-8151. DOI:10.1080/0883815080243739

[5]. Hashish, Y., Bunt, A. and Young, J. E., “Involving children in content control: a collaborative and education-oriented content filtering approach”, Proceedings of the 32nd annual ACM conference on Human factors in computing systems, pp: 1797--1806, 2014.

[6]. Van der Zwaan, J. M., Dignum, V., Jonker, C. M. and van der Hof, S., “On Technology Against Cyberbullying”.Minding Minors Wandering the Web: Regulating Online Child Safety, pp: 211--228, Springer, 2014.

[7]. SIP-BENCH III, Benchmarking de Herramientas de Control Parental para la protección Online de niños, Disponible en: http://www.sipbench.eu/phase5.cfm/action.ranking.

[8]. Ivorra, E. “Estudio sobre la protección de los padres hacia sus hijos en Internet: Control Parental y otras estrategias”, en Huelva capital, España, Master-tesis, Universidad Internacional de Andalucía, 2014.

[9]. Jae-Deok, L., Byeong-Cheol, C., Seung-Wan, H. and Jeong-Nyeo, K. “Adult contests Analysis and Remote Management framework For Parental Control Based on Android Platform”, Advanced in Computer Science and its Applications, Vo. 279, pp: 161-66, Springer, 2014.

[10]. Dimitrios, M., Loannis, M., Marija, J. “GARS: Real-time system for identification, assessment and control of cyber grooming attacks”, Computers & Security volume 42, pp: 177—190 Elsevier, 2014

[11]. Marcelo, J. F. y Martín, E. “Protege a tus hijos de los riesgos de Internet y otras tecnologías”. Madrid: Grupo Amaya, S. A, 2010.

[12]. Society E.I., Europe's Information Society. Available at http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7573

[13]. Velandía Mora, C. “Modelo Pedagógico con fundamentos en Cibernética” Social. Medellín: Consejo Editorial Universitario, 2005

[14]. Martínez Rodriguez, A. “Indicadores cibermétricos ¿Nuevas propuestas para medir la información en el entorno digital?”. Disponible en: http://bvs.sld.cu/revistas/aci/vol14_4_06/aci03406.htm.

[15]. Benavides P., Rodríguez S., Procesamiento del Lenguaje Natural en la Recuperación de Información, Universidad de la Salle, Colombia. Dispon. en: http://eprints.rclis.org/9598/1/procesamiento_del_lenguaje_natural_en_la_recuperaci_n_de_informaci_n.pdf.

[16]. Silva, D. y Mercerat, B., “Construyendo Aplicaciones Web con una Metodología de Diseño Orientado a Objetos”. Disponible en http://www.unab.edu.co/editorialunab/revistas/r.../r22_art5_r.pdf.

[17]. Torres, M., Fuertes, W., Villacís, C., Zambrano, M., Prócel C., **“**Puzzlemote, Videojuego Controlado con el Mando de la Wii para Niños de 7 a 10 Años, Utilizando OOHDM e Inteligencia Artificial”**,** Revista Brasilera de la Universida de Federal do Paraná, A. to Z. Novas práticas em informação e conhecimento, ISSN: 2237-826X, 2013.

[18]. Ministerio de Educación del Ecuador, Información geo-referencial de educación. Disponible en: http://geoportal.educacion.gob.ec/visor/index.html.