



TESINA DE LICENCIATURA

Título: FoCoS: Una herramienta para concientización sobre seguridad en Internet

Autores: Geronimo Acevedo

Director: Lic. Paula Venosa – Lic. Claudia Banchoff

Codirector: N/A

Asesor profesional: N/A

Carrera: Licenciatura en Sistemas

Resumen

El presente trabajo detalla toda la labor de análisis e investigación realizada para alcanzar la implementación de una herramienta de concientización en seguridad y privacidad sobre Internet.

Para lograr dicha herramienta fue necesario realizar diversas tareas: análisis de distintos sitios web que brindan información sobre la Seguridad en Internet, análisis de Redes Sociales Open Source disponibles en la Web, investigación de alternativas para detectar la tecnología desde donde accede el usuario a un sitio web, entre otras.

Adicionalmente, esta herramienta producto de todo el trabajo realizado, se integró a un proyecto iniciado por la Facultad de Informática, "Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos", para permitir reunir/formar una comunidad que comparta experiencias, inquietudes, conocimientos, opiniones, etc.

Palabras Claves

- Seguridad en Internet
- Concientización
- Redes Sociales
- Open Source
- Mahara
- FoCoS

Trabajos Realizados

- Análisis sobre sitios web en español orientados a la Seguridad y Privacidad en Internet.
- Análisis sobre herramientas para la detección del tipo de acceso a Internet.
- Investigación, análisis y prueba de herramientas Open Source disponibles para implementar redes sociales.
- Implementación de un entorno de difusión de contenidos sobre privacidad y seguridad de la Información, con orientación a los distintos tipos de usuarios.
- Integración al desarrollo de un módulo que identifique desde dónde accede el usuario.

Conclusiones

Los objetivos planteados al comienzo del trabajo se alcanzaron al lograr la implementación de un entorno de difusión de contenidos sobre Privacidad y Seguridad de la Información, con orientación a los distintos tipos de usuarios. Integrando al mismo, una red social de manera tal de generar una comunidad alrededor de la temática, incorporando el manejo de roles, enfocado al proyecto "Caperucita fue víctima de la Ingeniería Social". Asimismo, durante la fase de investigación nos encontramos con una herramienta que no sólo nos permitió armar una red social sino que estaba orientada a la educación, lo que facilitó la adecuación de nuestros objetivos.

Trabajos Futuros

Completar la integración de la herramienta desarrollada con el proyecto de "Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos", para dar soporte tanto en lo referido a la documentación como a la plataforma de comunicación.



UNIVERSIDAD NACIONAL DE LA PLATA

Facultad de Informática

FoCoS: Una herramienta para concientización sobre
seguridad en Internet.

Tesis presentada para obtener el título de Licenciado en Sistemas

Acevedo Geronimo

Director de tesis: Lic. Paula Venosa – Lic. Claudia Banchoff

Índice

Objetivos.....	3
Motivación.....	3
Desarrollos propuestos.....	3
Pasos a seguir.....	4
Introducción.....	4
Estructura Organizativa del trabajo.....	5
Concientización en aspectos de seguridad en Internet con fines educativos.....	6
Segu-kids.....	10
Chicos en Internet.....	16
Internet Segura Para Todos.....	19
Programa Internet Segura.....	23
Navega Protegido.....	26
Internet Segura – IQUA.....	30
Navegando Seguros.....	34
Resumen.....	38
Tabla Resumen.....	39
Conclusión	40
Redes Sociales Open Source.....	42
Elgg.....	43
Clonesumating.....	45
Dolphin.....	46
Applessed.....	48
Mahara.....	49
OpenPNE.....	51
Ospo.....	52
AstroSPACE.....	53
FlightFeather.....	54
Conclusión	55

Herramientas o métodos para la detección del tipo de acceso.....	56
Get Browser.....	57
Browser detect.....	61
Detect Mobile Browser.....	62
jQuery.browser.....	63
Tabla comparativa	65
Conclusión.....	66
FoCoS: Una herramienta para concientización sobre seguridad en Internet.....	67
FoCoS: el Sitio Web.....	68
FoCoS: el modulo de identificación de dispositivos.....	72
FoCoS: la Red Social.....	76
FoCoS en el Proyecto Caperucita y el Lobo en el Ciberespacio.....	87
Conclusiones.....	89
Conclusión.....	89
Próximos Pasos.....	89
Referencias.....	90
Bibliografía.....	91

Capítulo 1

Objetivos

El objetivo del presente trabajo es implementar una red social como apoyo a la concientización en seguridad y privacidad sobre Internet. Para ello, se analizarán herramientas que permiten implementar redes sociales, focalizando en herramientas Open Source. Se generará un espacio de comunicación y difusión sobre aspectos de privacidad y seguridad de la información, incorporando distintos dispositivos desde los que se puede acceder, adecuando los consejos y recomendaciones, así como los distintos roles de los actores intervinientes en el funcionamiento de la red. Se definirán perfiles de usuarios con roles diferenciados (por ejemplo: docentes, alumnos, padres facilitadores, etc.) quienes tienen distintos grados de responsabilidades y conocimientos sobre la temática de la red social.

Este desarrollo se integrará con el proyecto de “*Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos*”, el cual fue acreditado como proyecto de extensión de la Facultad de Informática en la convocatoria 2010 de la Universidad Nacional de La Plata. Este proyecto trata sobre la implementación de talleres de seguridad informática dirigida a jóvenes, padres, docentes y personas de la tercera edad. En este contexto, el desarrollo producto de esta tesina, se utilizará como soporte tanto en lo referido a la documentación como a la plataforma de comunicación.

Motivación

Cada día son más los niños y adolescentes que utilizan Internet para sus tareas escolares, por diversión, entretenimiento o para contactarse con amigos. Esto se ve reflejado en el uso masivo de las redes sociales (mapa mundial de redes sociales [Ref1]). De la misma forma cada vez son más los peligros en Internet debido al uso indebido de personas mal intencionadas que no respetan la confidencialidad y privacidad de la información de personas honestas.

Internet no es solamente navegar en la web, también involucra otros servicios como el correo electrónico, la mensajería instantánea, el chat, etc. Este último suele ser el elemento preferido empleado por personas deshonestas para contactarse con menores y establecer una comunicación con ellos. Numerosos estudios y reportes indican los riesgos y peligros en el uso de Internet, especialmente pensando en los niños y jóvenes (*Un estudio advierte de los riesgos del "Cyberbullying" entre escolares* [Ref2], *Grooming: Un peligro oculto al otro lado del computador* [Ref3], *Titulares sobre el Grooming* [Ref4], *Cyberbullying' es el rival de moda* [Ref5]).

Desarrollos propuestos

En este contexto, se implementará un entorno de comunicación en el cual se difundirán conceptos, consejos, sugerencias y recomendaciones sobre la Privacidad y Seguridad en Internet. Se generará una Red Social como soporte, especialmente diseñada para que la comunidad pueda comunicarse, conocer sus problemas comunes, comentar sus propias experiencias, manifestar sus inquietudes, etc. Contará también con una sección en la cual

se reconocerá desde donde accede el usuario, ya sea una PC o un dispositivo móvil, y también se detectarán algunas características útiles, como por ejemplo que sistema operativo está utilizando, para brindar consejos y/o sugerencias de forma clara y precisa para que el usuario pueda aplicar sin inconvenientes.

Y por último, se llevará a cabo la integración con el proyecto de extensión *“Caperucita fue víctima de la ingeniería social”*.

Pasos a seguir

- Análisis sobre sitios web en español orientados a la Seguridad y Privacidad en Internet focalizados en la comunidad en general: niños, jóvenes y adultos. Evaluación de calidad de los contenidos, la población a la cual están dirigidos y los servicios brindados por dichos sitios.
- Análisis sobre herramientas para la detección del tipo de acceso y los distintos mecanismos para adaptar y adecuar las recomendaciones, sugerencias o consejos a los mismos.
- Investigación, análisis y prueba de herramientas Open Source disponibles para implementar redes sociales. Se realizarán análisis teniendo en cuenta la estructura, el mantenimiento (si es que lo tiene), las funcionalidades y contenidos posibles, la seguridad, la facilidad de adecuación, etc.
- Implementación de un entorno de difusión de contenidos sobre Privacidad y Seguridad de la Información, con orientación a los distintos tipos de usuarios. Integrando al mismo, una red social de manera tal de generar una comunidad alrededor de la temática, incorporando el manejo de roles, enfocado al proyecto *“Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos”*.
- Integración al desarrollo de un módulo que identifique desde dónde accede el usuario y qué características tiene el equipo del cual accede para poder impartir algunos de los conceptos analizados en la etapa anterior. Este módulo podrá ser accedido tanto desde PCs como desde dispositivos móviles (las interfaces serán adaptadas a ellos).

Introducción

Las Redes Sociales tienen un papel más que importante en la actualidad, tanto niños y jóvenes como adultos acceden a ellas para compartir, para comunicarse, para expresar lo que sienten o piensan, para divertirse, etc. Una red social no es sólo una herramienta para pasar el tiempo y divertirse con un grupo de amigos, una red social es un excelente instrumento para impartir conocimientos, sugerencias, consejos, experiencias y todo tipo de información útil. Para ello, es posible utilizar las redes sociales más populares de hoy en día como Facebook, Twitter, etc o implementar una propia, con herramientas Open Source disponibles (40 Redes Sociales Open Source [Ref6]).

Otro aspecto a tener en cuenta, es que el acceso a Internet desde distintos dispositivos móviles (celular, iPad, notebook, palms, etc) crece más y más determinando distintas condiciones de uso y seguridad.

La mejor herramienta de seguridad con que contamos es la educación, y no sólo para niños y jóvenes sino también para todos aquellos que hacemos uso de estas tecnologías. Estar informados nos proporciona instrumentos para prevenir la gran cantidad de riesgos existentes en Internet y nos permite concientizarnos sobre las formas de protección y prevención, haciendo uso responsable de las tecnologías existentes.

A lo largo del presente trabajo se profundizará sobre estos planteos iniciales para poder comprender la tematica que nos ocupa, concluyendo el trabajo con el desarrollo de una herramienta para dar soporte al proyecto mencionado.

Estructura Organizativa del trabajo

El presente informe está conformado por 5 capítulos, que contienen tanto la parte de investigación y como la parte de implementación de la herramienta propuesta (FoCoS).

El capítulo 2 contiene el análisis realizado sobre distintos sitios web que brindan información sobre la Seguridad en Internet, contienen educativos dirigidos a niños, adolescentes, padres y docentes.

En el capítulo 3 se analizan las Redes Sociales Open Source disponibles en la Web con el objetivo de hallar la ideal para el desarrollo de FoCoS, una herramienta para concientización sobre seguridad en Internet, que se utilizará de soporte en el proyecto de "Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos".

El capítulo 4 presenta algunas de las alternativas que existen en la Web para detectar la tecnología desde donde accede el usuario a un sitio web. Las herramientas analizadas en este capítulo fueron elegidas teniendo en cuenta su posible integración con FoCoS y su disponibilidad como software libre.

El capítulo 5 presenta FoCoS. Se muestran los módulos que contiene, las funciones que brinda y las actividades que se pueden realizar en él. Adicionalmente, se entra en detalle en las tareas que fueron realizadas para alcanzar lo que hoy es esta herramienta de difusión de contenidos sobre Privacidad y Seguridad de la Información.

Capítulo 2

Concientización en aspectos de seguridad en Internet con fines educativos.

Hoy en día son muchos los sitios web que brindan información sobre aspectos de seguridad y privacidad en Internet. Gran parte de ellos sólo presentan temas de soporte, como por ejemplo el sitio oficial de Microsoft [Ref23] que tiene una sección de seguridad donde exhibe algunos temas, mientras que otros sitios se enfocan exclusivamente en la seguridad en Internet desarrollando una gran variedad de temas, dando consejos y sugerencias, presentando herramientas para la protección y control, etc.

En este capítulo se analizarán algunos de los sitios web más destacados que brindan información sobre la Seguridad en Internet. Como el foco de esta tesina es dar soporte al proyecto caperucita, se han seleccionado aquellos sitios dirigidos a niños, adolescentes, padres y docentes.

Para cada sitio se detallará lo siguiente:

- *Introducción.* Una breve descripción en la que se expone lo que brinda el sitio, cuáles son sus objetivos, cuál es su misión, por quiénes está conformado, a quién está dirigido, etc. Esta información es sumamente importante para dejar en claro quiénes respaldan la información publicada y a quiénes está dirigida.
- *Estructura y contenido.* En este punto se describirá cómo está organizado estructuralmente el sitio, es decir, cómo organiza la información que brinda y se analizará el contenido, detallando los temas que presenta y especificando si los aborda superficialmente o de forma detallada.
- *Análisis.* En este espacio se analizarán varios aspectos referidos a los mecanismos/formas en que transmiten la información y los canales de comunicación existentes.

Casi llegando al final de esta sección se presentará una Tabla Resumen donde se podrá revisar de un pantallazo toda la información abordada. Y por último, una conclusión que resumirá todo el trabajo de investigación y análisis sobre los sitios.

A continuación se exhibe una encuesta realizada por Segu-Info [Ref7] para conocer la opinión de lo que debería contener un sitio de seguridad para niños y adolescentes. Dicha encuesta, al igual que la tabla que se detalla luego, fue tomada como base para realizar el análisis de cada sitio.

La Figura 1 muestra la encuesta realizada por Segu-Info.

Pais		Animaciones		Contenido	
Argentina	59,50	Si	55,50	Con poco texto y gráficos explicativos	59,18
España	8,00	Pocas	37,50	Con poco texto, definiciones breves y con enlaces de referencias	39,18
Colombia	6,00	No	7,00	Con mucho texto y con definiciones extensas	1,63
Mexico	4,00		100,00		100,00
Chile	3,50				
Bolivia	2,50	Areas		Lenguaje	
Costa Rica	2,50	Padres	40,80	Con lenguaje informal	73,02
Venezuela	2,50	Docentes	33,60	Con lenguaje formal	26,98
Ecuador	2,00	Otros profesionales	20,27		100,00
Peru	2,00	Ninguna otra	5,33		
Uruguay	2,00		100,00	Tipo de Información	
EE.UU.	1,50	Informar sobre Delitos		Uso de Internet en general	15,99
Brasil	0,50	Si	91,50	Uso del chat y mensajería instantánea	15,88
El Salvador	0,50	No	8,50	Uso responsable del ordenador	15,03
Honduras	0,50		100,00	La importancia del derecho a la privacidad	13,11
India	0,50	Preguntas y Respuestas		Copyright, contenido legal, uso de redes P2P, descarga de libros y música	11,30
Nicaragua	0,50	Si	95,00	Consejos para padres y docentes	10,77
Panamá	0,50	No	5,00	Información sobre organizaciones relacionadas con la protección de menores	9,91
Paraguay	0,50		100,00	Instrumentos de control (por ej. control parental, bloqueo de contenido, etc.)	8,00
Puerto Rico	0,50				100,00
	100,00	Trivia		Zona de descarga	
		Si	92,00	Si, con consejos	37,14
		No	8,00	Si, artículos breves para discusión	25,71
			100,00	Si, con afiches	16,83
				Si, con videos	11,75
				No	8,57
					100,00

Figura 1: Encuesta de Segu-Info.

La siguiente tabla presenta todos los temas que debería contener, como mínimo, un sitio enfocado en la seguridad en Internet. Para cada tema se da una breve explicación. En cada sitio se analizará cuales de estos temas se desarrollan, y si se desarrolla superficialmente o de forma detallada cada uno de ellos.

Tabla de Contenidos Mínimos

Temas	Explicación
Redes Sociales	Las redes sociales son páginas o sitios que permiten a las personas conectarse con sus amigos e incluso realizar nuevas amistades con el fin de compartir contenidos, interactuar y crear grupos sobre intereses similares: trabajo, lecturas, juegos, amistad, relaciones amorosas, etc.
Contraseñas	Las contraseñas son las claves que utilizamos para obtener acceso a información personal que almacenamos en algún equipo y a nuestras cuentas en línea.
Virus	Los Virus Informáticos son sencillamente programas creados para infectar sistemas y a otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente y así interferir en el funcionamiento general del equipo, registrar, dañar o eliminar datos, o bien propagarse por otros equipos y a través de Internet. Serían similares a los virus que afectan a los humanos ya que hay que implementar antibióticos, en este caso serían los Antivirus.
Cyberbulling o Ciberacoso	El Cyberbulling no se refiere específicamente a un acoso de índole sexual, sino a aquellas acciones más relacionadas con la

humillación, ridiculización pública, distribución de rumores, y otras formas de acoso emocional entre niños y adolescentes que han sido llevadas a Internet y el resto de los nuevos medios de comunicación.

Cybersexo

El cybersexo es una forma de sexo virtual (sin contacto físico) en el cual dos o más personas conectadas a una red (como Internet) se envían mensajes sexualmente explícitos que describen una experiencia sexual real o imaginada. Es un tipo de juego de roles en el cual los participantes fingen que están manteniendo relaciones, describen sus acciones y responden a los mensajes de los demás participantes con el fin de estimular sus deseos y fantasías.

Grooming

Junto al ciberbullying surge otra situación que puede implicar un riesgo para la seguridad e integridad de los menores. Se trata del grooming, esto es, un acoso ejercido por un adulto y se refiere a las acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor. Se podría decir que son situaciones de acoso con un contenido sexual explícito o implícito.

El rasgo característico del ciberbullying es la existencia de un acoso entre iguales, mientras que en el grooming el acosador es un adulto y existe una intención sexual.

Pedofilia

La Pornografía Infantil es la reproducción sexualmente explícita de la imagen de un menor. La distribución de este tipo de pornografía, se relaciona estrechamente con la pedofilia; la atracción sexual, por parte de un adulto, hacia niños y/o adolescentes.

Estimular, engañar o forzar a los niños a posar en fotografías o participar en videos pornográficos implica una forma de explotación de los menores, y atenta contra la dignidad de los niños.

Es muy común que el adulto, intente ganarse la confianza y cariño del menor, para luego llevar a cabo sus objetivos.

Phishing

El phishing es la actividad de atraer al usuario hacia un delito de fraude informático, a través de la colocación de un "anzuelo" para atraer su atención y/o información. El objetivo del delito es robar información personal y/o financiera del usuario.

La amenaza consiste en utilizar técnicas de Ingeniería Social para lograr que el usuario otorgue su información. El atacante, simula la identidad de alguna entidad conocida y de confianza por el usuario. Las vías de este ataque pueden ser un correo electrónico, un mensaje de texto o un llamado telefónico, entre

otros.

El atacante intenta duplicar la identidad simulada de la forma más realista posible, y cercana a la realidad para hacer más creíble el engaño y lograr que mayor cantidad de usuarios caigan en la trampa.

Robo de Identidad

El Robo de Identidad es un delito que tiene lugar cuando alguien se hace pasar por otra persona y utiliza información personal de índole financiera para solicitar préstamos, tarjetas de crédito, o tramitar distintos servicios. El ladrón se aprovecha de sus sólidos registros crediticios, y deja un registro negativo a su nombre.

Spam

Se define como spam a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico pero puede presentarse por programas de mensajería instantánea o por teléfono celular.

El spam es el correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva.

Segu-kids

Introducción

Segu-Kids [Ref8] es un espacio creado para brindar información a Jóvenes, Padres y Docentes sobre Seguridad en Internet.

Este emprendimiento de Segu-Info [Ref24] brinda información en forma libre y gratuita y es el primer sitio pensado con el objetivo de apoyar y acompañar a la familia y a los educadores.

El nacimiento de Segu-Kids se debe a la gran cantidad de riesgos existentes en Internet y a la necesidad de crear concientización y educación sobre las formas de prevención y protección, haciendo uso responsable de las tecnologías existentes.

Su Creador y Director

Cristian F. Borghello, es Licenciado en Sistemas, actualmente es Director de Segu-Info, se desempeña como consultor independiente en Seguridad de la Información y es Director Técnico y de Educación en una importante empresa antivirus.

Escribe para diversos medios especializados e investiga en forma independiente sobre Seguridad Informática y de la Información. El interés por la Seguridad de la Información y su investigación lo ha llevado a mantener Segu-Info y Segu-Kids.

Todos los contenidos de este sitio expresan la opinión personal de su creador.

Estructura y contenido

Segu-Kids está dividida en 3 grandes secciones: “Jóvenes”, “Padres” y “Docentes”. En estas tres secciones vuelca todo su contenido. La información que brinda en cada una de ellas está dirigida a la comunidad correspondiente, es decir, en la sección Jóvenes se presenta información útil para la comunidad joven (niños y adolescentes), en la sección Padres la información está dirigida a los padres y en la Docente a los docentes y educadores. La Figura 2 muestra la página de inicio del sitio.



Figura 2: Página de inicio de Segu-Kids.

A continuación se presentan los temas de cada sección y se los clasifica en: Incompleto, Completo y Muy Completo dependiendo del *contenido*.

Cuando hablamos de contenido, hacemos referencia a todos los puntos tratados en cada tema, es decir, si se profundizó lo suficiente, teniendo en cuenta la importancia del tema, o sólo se realizó un desarrollo superficial.

Sección Jóvenes

La sección Jóvenes desarrolla los siguientes temas:

Temas abordados	Contenido
En el blog o fotolog	Completo
En el chat	Completo
En el correo	Muy Completo
En el cyber	Completo
En los foros y grupos	Completo
En los juegos online	Muy Completo
En las redes sociales	Completo
En las redes P2P	Incompleto
Cadenas de correo	Incompleto
Edades	Muy Completo
Navegando en la web	Incompleto
Netiquette	Incompleto
Uso de contraseñas	Incompleto
Consejos	Muy Completo

La Figura 3 muestra la página inicial de esta sección.



Figura 3: Sección de Jóvenes en Segú-Kids.

Sección Padres

La sección Padres desarrolla los siguientes temas:

Temas	Contenido
Cyberbullying	Completo
Cybersexo	Incompleto
Grooming	Completo
Herramientas	Muy Completo
Pedofilia	Completo
Phishing	Incompleto
Robo de identidad	Muy Completo
Spam	Completo
Contratos familiares	Completo
Control parental	Muy Completo
Consejos	Completo

La Figura 4 muestra la página inicial de esta sección.



Figura 4: Sección de Padres en Segú-Kids.

Sección Docentes

La sección Docentes desarrolla los siguientes temas:

Temas	Contenido
Edad de los menores (actividades llevadas a cabo en Internet por los menores según su edad)	Incompleto
Intimidad y privacidad	Completo
Organizaciones	Muy Completo
Preguntas frecuentes	Completo
Material de apoyo	Muy Completo
Estadísticas	Muy Completo
Consejos	Incompleto

La Figura 5 muestra la página inicial de esta sección.

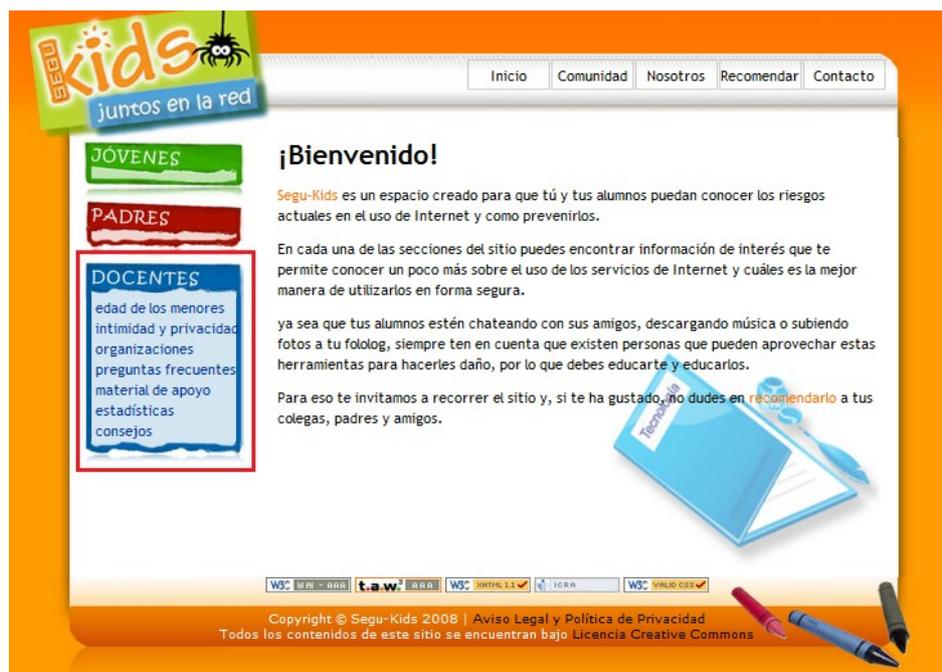


Figura 5: Sección de Padres en Segú-Kids.

Como podemos observar, son muchos los temas que se desarrollan y cumplen casi en su totalidad con los propuestos en la encuesta realizada por Segú-Info. Esto es así, ya que como mencioné anteriormente el director de Segú-Info es el creador de Segú-Kids y este sitio sería el producto de tal encuesta. Pero más allá de eso, no significa que el sitio sea totalmente completo y adecuado. Si bien está basado en dicha encuesta, la cual es muy completa, y contiene los temas presentados en la Tabla de Contenidos Mínimos no tiene en cuenta ciertos aspectos importantes que mencionaremos en breve.

Análisis

Dos puntos importantísimos que estuvieron presentes en la encuesta para desarrollar un sitio web para jóvenes son el “lenguaje” y “el contenido”.

En el caso de Segú-Kids, el lenguaje utilizado es independiente de la sección en la que nos encontremos, es decir, utiliza la misma forma de expresión para dirigirse a los jóvenes, padres y docentes; la división en secciones es sólo para dar una orientación de cuáles son los temas que les podrían interesar o ser útil a uno o a otro (dependiendo de la edad) y no para mostrar contenido de forma tal que si un niño o adolescente lea pueda comprender sin ningún problema y no tenga que buscar palabras que desconoce o no tenga que releer varias veces porque no puede entender lo que se le está explicando. Segú-kids no hace esta diferencia entre las diferentes secciones, si bien utiliza un lenguaje informal (esto es bueno ya que dirigirse, por ejemplo, a los jóvenes de manera formal aburre y lleva al joven a abandonar el sitio), no está haciendo una diferencia entre los jóvenes y adultos. La forma de dirigirse a un niño o adolescente para captar su atención debe ser especial. No sólo alcanza a veces con mantener una informalidad.

En cuanto al contenido, Segú-kids no trata a todos los temas con el mismo nivel de profundidad. Si bien, en la encuesta realizada por Segú-Info se

afirma que los jóvenes prefieren poco texto y definiciones breves, en muchos casos es necesario explicar con más detalle para que se pueda comprender el grado de importancia que tienen algunos temas. Siempre existe la forma de explicar algo de forma entretenida o divertida para poder captar la atención del lector (por ejemplo en el sitio Internet Segura Para Todos [Ref10] se tiene en cuenta esto)

Otro punto importante es la falta de una sección de preguntas y respuestas para que la comunidad pueda expresar sus inquietudes, dudas, experiencias, opiniones, ideas, etc. Una sección de este tipo sería muy útil ya que las personas deberían poder, de alguna forma, resolver sus dudas o inquietudes.

Por último, cabe mencionar que Segu-kids ya tiene unos años en la Web y muchas actualizaciones no se le hicieron, por lo que algunos temas actuales muy interesantes no se encuentran presentes o hay poca información de ellos.

Si bien, en Segu-Kids el lenguaje utilizado no diferencia el tipo de público y el nivel de profundidad con el cual se trata determinados temas no es suficiente, se trata de un muy buen sitio para la comunidad. Contiene excelentes gráficos explicativos que facilitan la comprensión, en su página de inicio presenta una lista breve de consejos útiles de seguridad, contiene noticias con la fecha de publicación y un link al sitio que la trata, y algo muy importante que no mencionamos hasta aquí es que Segu-Kids brinda buenos consejos/sugerencias en todos los temas que expone.

Chicos en Internet

Introducción

Chicos en Internet [Ref9] es un sitio web que promueve el uso de Internet de manera segura para toda la familia.

Internet es un lugar maravilloso pero también inseguro. La mejor manera de proteger a los niños de los aspectos negativos de Internet es a través de la Educación. Es necesario que conozcamos y tomemos conciencia de los riesgos y que aprendamos formas de mantenerlos alejados de los peligros.

Según sus creadores, su misión es:

- Promover el uso de Internet en forma productiva, divertida, libre y segura para toda la familia.
- Educar y concientizar en los beneficios y los peligros de Internet, de manera que las personas y las organizaciones puedan establecer sus propios mecanismos de control y seguridad en el uso de la tecnología.

Los creadores del sitio son:

Un grupo de padres con hijos pequeños y adolescentes que buscamos reunir esfuerzos para que nuestros niños puedan aprovechar al máximo de las nuevas tecnologías. Hoy como recursos inagotables de contenidos educativos, de entretenimiento y de comunicación y mañana como instrumento laboral. A estos efectos hemos buscado aunar esfuerzos propios y ajenos en función de los objetivos expresados.

Estructura y contenido

El sitio cuenta con un menú en el cual se despliegan varios ítems. Entre ellos, los que son de interés para esta tesina son los siguientes:

- Guía para niños y adolescentes.
- Guía para padres_y docentes.
- Reglas para el Colegio.
- Noticias.
- Artículos.

La Figura 6 muestra la página inicial de Chicos en Internet



Figura 6: Página de inicio de Chicos en Internet.

En el primer ítem, Guía para niños y adolescentes, se dan 6 consejos sobre seguridad en Internet en general. Este ítem contiene poca información útil, generaliza demasiado y no hace hincapié en ningún tema específico.

En Guía para padres y docentes se dan también consejos de seguridad en Internet en general. Consejos muy simples y generales, no profundizan temas importantes como lo son el cyberbullying, cybersexo, grooming, el robo de identidad, etc.

En Reglas para el Colegio se presenta un conjunto de reglas para los niños y adolescentes para el uso responsable de Internet y de las Computadoras en el Colegio. Esta sección es muy buena, hay varios consejos de lo que se debe y no debe hacer en las computadoras del colegio. De la gran cantidad de sitios visitados pocos son los que ofrecen estos consejos. Lo ideal sería que éste ítem esté integrado en Guía para niños y adolescentes ya que esos consejos o sugerencias están dirigidos a ellos.

Noticias y Artículos presentan varios temas importantes sobre la seguridad en Internet, temas de suma importancia hoy en día. Algunos de ellos son:

- Uso Seguro de Internet.
- Internet: falta conciencia sobre el riesgo de contactarse con extraños.
- El 83% de los chicos usa Internet sin el control de sus padres.
- Temor por el robo de datos en Internet.
- Ciberacoso.
- Seguridad infantil.

- Programa protege a chicos.
- Otros.

A modo de resumen, se presentan a continuación cada uno de los temas que brinda el sitio y se los clasifica en: Incompleto, Completo y Muy Completo dependiendo del *contenido*.

Cuando hablamos de contenido, hacemos referencia a todos los puntos tratados en cada tema, es decir, si se profundizó lo suficiente, teniendo en cuenta la importancia del tema, o sólo se realizó un desarrollo superficial.

Temas	Contenido
Guía para niños y adolescentes	<i>Incompleto</i>
Guía para padres y docentes	<i>Incompleto</i>
Reglas para el colegio	<i>Muy Completo</i>
Noticias	<i>Completo</i>
Artículos	<i>Completo</i>

Análisis

Chicos en Internet es un sitio con muy poca información sobre la seguridad en Internet, con escasos consejos y con una inadecuada organización del contenido.

Si bien presenta algunos temas interesantes en la sección de Noticias y Artículos, la inseguridad en Internet implica otros temas que no pueden dejarse de lado, y alguno de estos temas importantes no son tratados en este sitio. De los temas definidos en la Tabla de Contenidos Mínimos sólo desarrolla Cyberacoso o Cyberbullying, Robo de identidad y Grooming.

No contiene una sección de preguntas y respuestas para que tanto los niños como los adultos puedan sacarse dudas o inquietudes. Tampoco presenta gráficos ni animaciones para ayudar a comprender, sólo texto explicativo el cual no es muy claro y preciso.

Así concluimos que, Chicos en Internet es un sitio muy simple, con escasos recursos, con poca información y con una inadecuada organización del contenido.

Internet Segura Para Todos

Introducción

En este sitio encontrarán recomendaciones para el uso de Internet, descripciones de las herramientas más utilizadas, ayudas técnicas para proteger su computador y sugerencias de sitios para visitar.

Estructura y contenido

Internet Segura Para Todos [Ref10] está dividida en dos grandes secciones: Niños y Padres. En estas dos secciones vuelca todo su contenido. La información que brinda en cada una de ellas está dirigida a la comunidad correspondiente, es decir, en la sección Niños se presenta información útil para la comunidad joven (niños y adolescentes). En la sección Padres la información está enfocada a los padres.

La Figura 7 muestra la página inicial de Internet Segura Para Todos



Figura 7: Página de inicio de Internet Segura Para Todos.

La sección de niños tiene la siguiente estructura:

- **APRENDER**
 - Aprendiendo a Navegar.
 - Cómo busco información.
 - Investigando en Internet.
- **COMUNICAR**
 - El Chat.
 - El Correo Electrónico.
 - Recomendaciones.
- **Internet SEGURA**
 - Tips de seguridad.
 - El Código CyberÉtico.
 - Qué es el Grooming y Ciberbullying.
- **AGENDA**
- **MATERIALES**

De estos temas los que interesan son los que se detallan en Internet Segura y Comunicar (en esta se dan consejos sobre el uso adecuado/seguro del chat y el correo electrónico). En el resto de los puntos se explica a los niños sobre el uso de Internet dejando de lado la seguridad.

En el módulo Internet Segura se desarrollan los siguientes ítems:

- Tips de seguridad.
- El Código Cyberético.
- Qué es el Grooming y Ciberbullying.

La Figura 8 muestra la página inicial de esta sección.



Figura 8: Sección de Niños en Internet Segura Para Todos.

En “Tips de seguridad” se expone una lista de precauciones que los niños deberían considerar a la hora de usar Internet. En este ítem se informa, a rasgos generales, a los jóvenes que es lo que deben y no deben hacer en Internet.

El Código Cyberético es una forma de concientización que contiene un conjunto de normas o principios para concientizar a los niños sobre el uso correcto de Internet.

Y en “Que es el Grooming y el Ciberbullying” sólo se da la definición de lo que es el Grooming y el Ciberbullying sin entran en detalle.

El módulo de padres posee la siguiente estructura:

PADRES

- Recomendaciones.

- Prevención.
- Ayudas Técnicas.

La Figura 9 muestra la página inicial de esta sección.



Figura 9: Sección de Padres en Internet Segura Para Todos.

En “Recomendaciones” se exponen varios consejos que pueden aplicar con sus hijos. Una lista de 9 consejos simples pero muy útiles. Luego presentan consejos y sugerencia que les pueden ser útiles a ellos para navegar seguros. Estos consejos son sobre el correo electrónico, los programas gratuitos y utilitarios, sobre la privacidad de la información y actualizaciones de Windows.

En “Prevención” se brinda una lista de instrucciones para que los padres apliquen junto con sus hijos, y así puedan prevenir cualquier tipo de problema en Internet.

En “Ayuda Técnica” se describen las herramientas de Internet más utilizadas en la actualidad. También presentan ayudas técnicas para proteger su computador del ataque de virus o de desconocidos al conectarse a la red. Esta sección está bastante completa.

Se presentan a continuación cada uno de los temas que brinda el sitio y se los clasifica en: Incompleto, Completo y Muy Completo dependiendo del contenido.

Cuando hablamos de contenido, hacemos referencia a todos los puntos tratados en cada tema, es decir, si se profundizó lo suficiente, teniendo en cuenta la importancia del tema, o sólo se realizó un desarrollo superficial.

Niños

Temas abordados	Contenido
Tips de seguridad	<i>Incompleto</i>
El código CyberÉtico	<i>Completo</i>
Qué es el Grooming y Ciberbullying	<i>Incompleto</i>

Padres

Temas abordados	Contenido
Recomendaciones	<i>Completo</i>
Prevención	<i>Completo</i>
Ayudas técnicas	<i>Muy Completo</i>

Análisis

Analizando el Sitio pudimos observar que no se abordan temas de suma importancia. En la sección de niños sólo se da una serie de tips de seguridad dirigidos prácticamente al chat y al correo electrónico, no se hace hincapié en temas que hoy en día son claves como por ejemplo los foros y grupos, los Cyber, y ni que hablar de las Redes Sociales. Por lo tanto, se desarrollan muy pocos temas de la Tabla de Contenidos Mínimos.

Otro punto a resaltar es la ausencia de una sección destinada a un docente, maestro o profesor. Uno de los principales acceso a los niños para que estos tomen conciencia de la gravedad del asunto es el colegio. La educación debe ser impartida desde ambos lados, tanto del lado de los padres como en el colegio. Y una sección destinada a los Docentes, por ejemplo, sería de mucha utilidad para que estos conozcan cuales son los riesgos que corren sus alumnos y que medidas pueden tomar ante ello.

Tampoco cuenta con una sección de preguntas y respuestas para que la comunidad pueda opinar y sacarse dudas o inquietudes. Como ya se ha dicho, una sección de este tipo ayuda mucho.

No se brinda información sobre delitos o noticias actuales de lo que sucede en Internet. Brindar este tipo de información suele ser muy útil no sólo para mantener informadas a las personas sobre lo que ocurre en el día a día sino también para captar su atención y que logren comprender los peligros que hay en Internet y que se concienticen de ello.

Un punto a favor a destacar de este sitio es el lenguaje utilizado para dirigirse a los niños y los gráficos y animaciones que contiene. El sitio presenta los temas de tal forma que un niño pueda entender sin problemas. El diseño pedagógico ambientado a niños es muy bueno, al igual que sus gráficos y animaciones que ayudan a la comprensión.

Resumiendo, el sitio es escaso en información y en recursos, está muy Incompleto, pero la forma en que representa los temas es adecuada según el publico al que está dirigido.

Programa Internet Segura

Introducción

Programa Internet Segura [Ref11] es un espacio del sitio “www.chicos.net.ar” el cual fue creado para la educación e inclusión social de niños, niñas y jóvenes. Este sitio presenta muchos espacios entre los cuales se destaca el programa de Internet Segura en el cual se trata todo lo referido a seguridad en Internet.

Estructura y contenido

En la página de inicio del programa Internet Segura se presentan las siguientes secciones:

- Niños y Niñas
- Adolescentes
- Docentes

La Figura 10 muestra la página inicial del Programa Internet Segura



Figura 10: Página de inicio del Programa Internet Segura.

Tanto la sección de Niños y Niñas, como la de Adolescentes brindan consejos y sugerencias sobre la seguridad en Internet en forma general. En ninguna de las dos se hace hincapié en algún tema específico, sólo se dan recomendaciones en general. Ninguno de los temas definidos en la Tabla de Contenidos Mínimos son desarrollados.

La Sección de Docentes es más completa. Contiene videos para compartir con los alumnos y para cada video plantea cual es el punto de reflexión. Cuenta con un menú en el cual se presentan los siguientes ítems:

- Tips de seguridad para niños
- A qué peligros están expuestos los niños en Internet
- Rol del docentes

- Pautas para docentes y padres
- Recomendaciones
- Publicaciones
- Materiales para el Docente

La Figura 11 muestra la página inicial de esta sección.

PROGRAMA Internet Segura

INICIO

- ⚠️ [Tips de seguridad para niños](#)
- ⚠️ [¿A qué peligros están expuestos los niños en Internet?](#)
- ⚠️ [Rol del docente](#)
- ⚠️ [Pautas para docentes y padres](#)
- ⚠️ [Recomendaciones](#)
- ⚠️ [Sitios para visitar](#)
- ⚠️ [Publicaciones](#)
- ⚠️ [Materiales para el docente](#)
- ⚠️ [Prensa](#)
- ⚠️ [Archivo](#)
- ⚠️ [Apoyan Internet Segura](#)
- ⚠️ [Contacto](#)

Pensar el uso responsable de Internet

Los niños, las niñas y adolescentes cuentan con dispositivos tecnológicos desde los cuales acceden a información, intercambian opiniones e intervienen activamente en las redes sociales virtuales. Los cambios en los modos de comunicarse y buscar datos son radicales, los beneficios múltiples, pero con ellos aparecen riesgos que debemos minimizar.

En coincidencia con la entrega de computadoras a todos los alumnos de escuelas media del país por parte del Ministerio de Educación de la Nación; Educ.ar y Chicos.net le acerca materiales para el posicionamiento del tema en el marco de las instituciones educativas.

ACTIVIDAD 1

TEMA: ADICCIÓN
VIDEO: NO TE DEJES ATRAPAR

[Te invitamos a ver este video con tus alumnos](#)

NO TE DEJES ATRAPAR

YouTube

0:00 / 1:27

Realizado por alumnos del Colegio Labarden. Primer Puesto Concurso Tecnología Sí 2009

Para reflexionar
¿Que nos pasa con las tecnologías que nos rodean? ¿Cómo las usamos? ¿Para qué nos sirven estas herramientas? ¿En qué punto nuestra actitud en relación a las tecnologías puede perjudicarnos?

Figura 11: Sección Docentes del Programa Internet Segura.

En cada ítem se realiza un breve desarrollo y se dan recomendaciones y consejos útiles para docentes, maestros o profesores. Esta sección es completa y de mucha utilidad para los docentes.

Se presentan a continuación cada uno de los temas que brinda esta sección para docentes y se los clasifica en: Incompleto, Completo y Muy Completo dependiendo del *contenido*.

Cuando hablamos de contenido, hacemos referencia a todos los puntos tratados en cada tema, es decir, si se profundizó lo suficiente, teniendo en cuenta la importancia del tema, o sólo se realizó un desarrollo superficial.

Temas	Cantidad
Tips de seguridad para niños	<i>Muy Completo</i>
A qué peligros están expuestos los niños en Internet	<i>Completo</i>
Rol del docentes	<i>Completo</i>
Pautas para docentes y padres	<i>Muy Completo</i>
Recomendaciones	<i>Completo</i>
Publicaciones	<i>Completo</i>
Publicaciones	<i>Completo</i>

Análisis

Las secciones de “Niños y Niñas” y “Adolescentes” no contienen suficiente contenidos. Al igual que el sitio Chicos en Internet, carece de contenido, se dan recomendaciones y consejos en general y no se abordan temas particulares como los descritos en la Tabla de Contenidos Mínimos que son muy importantes hoy en día.

Un punto importante a destacar es que el sitio no cuenta con una sección para Padres. La educación debe empezar por la casa, si los padres no están al tanto de lo que sucede en Internet no podrán prevenir a sus hijos. El cyberbulling, el cybersexo y la pedofilia son cuestiones sumamente importantes que los padres deben conocer y estar informados. También existen temas que son de mucha utilidad para uso propio de los mayores, tal es el caso del robo de identidad y el phishing.

En el área de Niños y Niñas, si bien no es mucho lo que se explica, se debería utilizar un lenguaje más sencillo que se adapte a ellos. Captar la atención de un niño no es fácil y más cuando se trata de temas tan complejos y delicados como estos.

Este Programa de Internet Segura tampoco cuenta con un módulo de preguntas y respuestas para que los usuarios puedan sacarse sus dudas o inquietudes.

No hay informes sobre delitos o noticias actuales relacionadas con la seguridad en Internet.

En resumen, este programa es muy Incompleto, carece de contenido importante y de recursos útiles.

Navega Protegido

Introducción

Navega Protegido [Ref12] es una alianza entre Ricky Martin Foundation y Microsoft para proteger a los niños de peligros en el ciberespacio. Comprometidos con el bienestar de este segmento de la población, los objetivos que sus creadores se proponen son:

- Brindar consejos y recomendaciones para que puedas proteger a tu familia, tu patrimonio y la identidad de quienes utilizan Internet en tu hogar o en sitios públicos.
- Educar a los niños, maestros, tutores y padres de familia de Latinoamérica en el uso seguro y responsable de Internet.
- Disminuir los riesgos asociados al uso de Internet para que los jóvenes y los niños de Latinoamérica no sean sujeto de ataques de software malicioso, Virus, Phishing, acosadores sexuales, contenido violento o pornográfico, o robo de identidad.
- Lograr que los niños puedan sacar el máximo provecho de Internet de manera segura.

Estructura y contenido

Navega Protegido contiene un menú en el cual presenta las siguientes tres secciones:

- Protege a tu familia.
- Protégete a ti mismo.
- Protege a tu equipo.

La Figura 12 muestra la página inicial de Navega Protegido



Figura 12: Página de inicio de Navega Protegido.

En estas tres secciones despliega su contenido. Se desarrollan varios temas que pueden ser de mucha utilidad para quienes desean usar Internet de forma segura.

A continuación se realiza un análisis como el que se hizo en Segu-Kids para cada una de las tres secciones. Se presentan los temas de cada sección y se los clasifica en: Incompleto, Completo y Muy Completo dependiendo del contenido.

Cuando hablamos de contenido, hacemos referencia a todos los puntos tratados en cada tema, es decir, si se profundizó lo suficiente, teniendo en cuenta la importancia del tema, o sólo se realizó un desarrollo superficial.

Protege a tu familia

Esta sección presenta los siguientes temas:

Temas	Contenido
Seguridad web de tu familia	Incompleto
Seguridad de los niños	Completo

La Figura 13 muestra la página inicial de esta sección.



Figura 13: Sección Protege a tu familia en Navega Protegido.

Protégete a ti mismo

Esta sección presenta los siguientes temas:

Temas	Contenido
Protégete del spam	<i>Incompleto</i>
Protégete de los virus	<i>Incompleto</i>
Cuidado con el phishing	<i>Incompleto</i>
Protégete del spyware	<i>Completo</i>
Comercio electrónico	<i>Completo</i>
Banca en línea	<i>Completo</i>
Equipos en lugares públicos	<i>Incompleto</i>
Consejos si vas a viajar	<i>Completo</i>

La Figura 14 muestra la página inicial de esta sección.

The screenshot shows the 'Navega Protegido' website interface. At the top, there is a navigation bar with 'España', 'Español', and 'Sign in' options. The main header reads 'NAVEGA PROTEGIDO EN INTERNET'. Below this, there are three main sections: 'Protege a tu familia', 'Protégete a ti mismo' (highlighted with a red circle), and 'Protege tu equipo'. The 'Protégete a ti mismo' section is expanded, showing a list of sub-topics: 'Protégete del spam', 'Protégete de los virus', 'Cuidado con el phishing', 'Protégete del spyware', 'Comercio electrónico', 'Banca en línea', 'Equipos en lugares públicos', and 'Consejos si vas a viajar'. Below the list, there is a 'Participa' section with options like 'Navega Responde', 'Alerta para Padres', 'Denunciar', and 'Invita a un amigo'. The main content area features a video player and several paragraphs of text discussing online safety and digital privacy.

Figura 14: Sección *Protégete a ti mismo* en *Navega Protegido*.

Protege a tu equipo

Esta sección presenta los siguientes temas:

Temas	Contenido
Actualizaciones	<i>Incompleto</i>
Configuración	<i>Incompleto</i>
Respaldo de tu información	<i>Completo</i>
Cuidados con tu PC de oficina	<i>Completo</i>
Recursos útiles	<i>Incompleto</i>

La Figura 15 muestra la página inicial de esta sección.



Figura 15: Secci3n Protege a tu equipo en Navega Protegido.

Análisis

Como podemos observar el sitio cuenta con bastante informaci3n, abarca varios temas pero no llega a cubrir en su totalidad los definidos en la Tabla de Contenidos M3nimos

El contenido no se encuentra organizado de forma ideal. Si bien est3 dividido en tres secciones, lo correcto ser3a organizar la informaci3n de acuerdo a las edades como lo realizan los sitios que ya hemos visitado. Por ejemplo en la secci3n "Protégete a ti mismo" existen ítems que pueden ser de interesar para los jóvenes y no para los adultos, y viceversa. Mantener la informaci3n organizada en un sitio es un punto importante a tener en cuenta.

No se presentan gr3ficos ni animaciones para ayudar al lector a comprender, ni tampoco cuenta con alg3n medio en el cual la comunidad puede expresar sus inquietudes u opiniones y as3 poder resolver sus dudas.

Como aspecto positivo a destacar de Navega Seguro son las noticias/novedades que expone en su p3gina de inicio, las cuales son actuales y muy 3tiles.

Resumiendo, la organizaci3n de la informaci3n no es adecuada; no hay suficiente informaci3n para ni3os y jóvenes, estos deber3an ser los que m3s informados deben estar y no posee un medio para poder consultar inquietudes y resolver dudas.

Internet Segura – IQUA

Introducción

Internet segura [Ref13] es un programa de sensibilización que tiene como misión promover el uso seguro de Internet contribuyendo a generar una cultura de responsabilidad, que permita a los niños y adolescentes beneficiarse cada vez más de este nuevo medio.

Esta dirigida a:

- Familias que quieran proteger y enseñar a los menores a utilizar Internet de una manera más segura.
- Profesionales de la educación que deseen educar al alumnado en la utilización de Internet con seguridad y de manera responsable.
- Niños y jóvenes menores de edad que quieran aprender a estar seguros mientras navegan por Internet.
- Todos los usuarios de Internet que deseen contribuir a hacer de Internet un entorno seguro para todos, actuando de manera responsable.

La red Internet Segura cuenta con la participación de organizaciones, instituciones y empresas que trabajan conjuntamente para promover un uso responsable y seguro de Internet.

Estructura y contenido

El sitio presenta la información en dos secciones: “Beneficios y Riesgos” y “Recomendaciones”.

En Beneficios y Riesgos se desarrollan los siguientes puntos:

- Los contenidos.
- Situaciones de contacto.
- El comercio electrónico.
- Cuestiones legales.
- Riesgos en función de los servicios de Internet.

Y en Recomendaciones los siguientes:

- Consejos para padres y educadores.
- Consejos para niños y adolescentes.
- Herramientas de control.

La Figura 16 muestra la página inicial de Internet Segura



Figura 16: Sección de Beneficios y Riesgos en Internet Segura.

En la sección de Beneficios y Riesgos se realiza una mera descripción de los riesgos que existen hoy en día, se los define y en algunos casos se dan algunas recomendaciones. Por ejemplo en el ítem “Los contenidos” sólo se define que son los contenidos ilegales, los contenidos nocivos y los contenidos falsos, y no se da ningún tipo de consejo o recomendación. Pero en el ítem “Situaciones de contacto” se dan las definiciones y descripciones de algunas situaciones en las que las personas pueden contactarse y comunicarse, y para esos casos si se dan algunas recomendaciones y consejos.

La Figura 17 muestra la página inicial de esta sección



Figura 17: Sección de Recomendaciones en Internet Segura.

En la sección de Recomendaciones se presentan varios puntos a tener en cuenta por los padres, educadores, niños y adolescentes. Para los niños y adolescentes se hace una división por edades, se dan consejos para niños de 8 a 10 años, para niños de 11 a 13 años y para jóvenes de 14 a 15 años. También en esta sección se presentan herramientas/instrumentos para controlar de alguna forma el acceso seguro a Internet.

A modo de resumen, se presentan a continuación cada uno de los temas que brinda el sitio y se los clasifica en: Incompleto, Completo y Muy Completo dependiendo del *contenido*.

Cuando hablamos de contenido, hacemos referencia a todos los puntos tratados en cada tema, es decir, si se profundizó lo suficiente, teniendo en cuenta la importancia del tema, o sólo se realizó un desarrollo superficial.

Beneficios y Riesgos

Temas	Cantidad
Los contenidos	Incompleto
Situaciones de contacto	Completo
El comercio electrónico	Incompleto
Cuestiones legales	Completo
Riesgos en función de los servicios de Internet	Incompleto

Recomendaciones

Temas	Cantidad
Consejos para padres y educadores	Completo
Consejos para niños y adolescentes	Muy Completo
Herramientas de control	Completo

Análisis

Este sitio desarrolla de forma muy completa todos los temas que presenta, el problema está en que no presenta muchos, se dejan de lado temas importantísimos como los vistos en los demás sitios y los definidos en la Tabla de Contenidos Mínimos (cyberbullying, grooming, robo de identidad, etc). Los consejos que se dan para niños y adolescentes son los mismos que se dan en Segu-Kids, y esto así es porque Segu-Kids los copia de este sitio (está aclarado en su página).

No hay gráficos ni animaciones para facilitar la comprensión, sobre todo de la población de niños y jóvenes, sólo texto explicativo. El sitio tampoco cuenta con un área de preguntas y respuestas para que los usuarios puedan expresar sus inquietudes y opiniones.

Tampoco se dan informes de delitos, noticias actuales y todo ese tipo de información que capta mucho la atención de los usuarios y ayuda a que tomen conciencia de los riesgos que hay hoy en día.

En conclusión, Internet Segura–IQUA es un sitio que sólo da información a grandes rasgos sin centrarse en temas específicos, escasa en contenidos.

Navegando Seguros

Introducción

Navegando Seguros [Ref14] es un portal diseñado y producido por la red Peruana contra la pornografía infantil, con el apoyo de la Embajada del Reino de los Países Bajos.

Este portal está dirigido tanto a padres de familia, maestros de escuelas, niños, niñas, adolescentes en edad escolar, como al público en general, quienes en y para su vida diaria utilizan las tecnologías de información y comunicación, entre ella la Internet con sus componentes y los teléfonos celulares de tercera generación para comunicarse, acceder a información y divertirse.

Según el creador, su misión es:

Evitar que usuarios de las tecnologías de información y comunicación, principalmente menores de edad, sean víctimas de abusos o explotación sexual, estafa, engaño, acoso, extorción u otra forma de engaño, logrando hacer de la Internet un ambiente más sano y seguro para todos los cibernautas.

Contenido y estructura

“Navegando seguros” contiene tres grandes secciones: Menores de edad, Padres y Educadores. En estas vuelca toda su información dando consejos, sugerencias, recomendaciones, etc.

La Figura 18 muestra la página inicial de Navegando Seguros



Figura 18: Página de inicio de Navegando Seguros.

Al igual que se hizo con Segu-Kids y con Navega Protegido, se presentan los temas de cada sección y se los clasifica en: Incompleto, Completo y Muy Completo dependiendo del *contenido*.

Cuando hablamos de contenido, hacemos referencia a todos los puntos tratados en cada tema, es decir, si se profundizó lo suficiente, teniendo en cuenta la importancia del tema, o sólo se realizó un desarrollo superficial.

Menores de edad

En este módulo se desarrollan los siguientes temas:

Temas	Cantidad
Internet y sus posibilidades	Completo
9 consejos para navegar	Muy Completo
Seguridad en tu correo	Incompleto
Uso de los recursos	Completo
Uso del teléfono celular	Completo
Consejo final	Incompleto

La Figura 19 muestra la página inicial de esta sección



Figura 19: Sección de Menores de Edad en Navegando Seguros.

Padres

En la sección Padres se desarrollan los siguientes temas:

Temas	Cantidad
Menores de edad y tecnología	<i>Completo</i>
Lo que debemos saber	<i>Muy Completo</i>
La Internet en el hogar	<i>Muy Completo</i>
El celular con cámara	<i>Completo</i>
El abuso sexual infantil	<i>Completo</i>
Síntomas de abuso	<i>Completo</i>
Cómo actuar	<i>Completo</i>

La Figura 20 muestra la página inicial de esta sección



Figura 20: Sección de Padres en Navegando Seguros.

Educadores

En esta sección se desarrollan los siguientes temas:

Temas	Cantidad
Uso de Internet en el aula	<i>Muy Completo</i>
Uso de celulares en el colegio	<i>Completo</i>
El abuso sexual infantil	<i>Completo</i>
Síntomas de abuso	<i>Completo</i>
Como actuar	<i>Completo</i>
Lo que hay en Internet	<i>Muy Completo</i>

La Figura 21 muestra la página inicial de esta sección



Figura 21: Sección de Educadores en Navegando Seguros.

Análisis

Como podemos observar, en todos los temas que se desarrolla (salvo en Seguridad en tu correo y Consejo final) el contenido es suficiente, es decir que se presenta bastante información para que los jóvenes, padres y educadores puedan comprender y estar al tanto de lo que sucede en Internet hoy en día.

Otro aspecto importante a resaltar es el lenguaje utilizado. Se realiza una clara diferencia entre las tres áreas a la hora de expresar los conceptos y sugerencias.

Navegando Seguros no presenta ciertos temas de suma importancia, no profundiza sobre temas esenciales como los definidos en la Tabla de Contenidos Mínimos.

El sitio tampoco cuenta con una sección de preguntas y respuesta para expresar inquietudes, dudas o problemas.

No contiene gráficos ni animaciones para facilitar la comprensión de ciertos temas y tampoco presenta informes o noticias de la actualidad, las cuales suelen captar la atención del usuario y lo puede motivar a que se informe y tome conciencia.

Resumiendo, el sitio no cuenta con la suficiente información que se necesita hoy en día para estar informado de todos los riesgos que existen en Internet.

Resumen

Para darle un cierre a los análisis realizados expondremos una tabla resumen en donde se detallan todos los puntos que se tuvieron en cuenta a la hora de analizar los sitios. La tabla estará conformada por los siguientes ítems y sus posibles respuestas:

- *Animaciones* - **Si o No.**
- *Informar sobre delitos* - **Si o No.**
- *Sección de preguntas y respuestas* - **Si o No.**
- *Acceso desde distintos dispositivos* - **Si o No.**
- *Áreas* - Todas las áreas que desarrolle.
- *Contenido* - **Incompleto, Completo o Muy Completo.** En este ítem se tendrá en cuenta el contenido presentado por cada sitio teniendo en cuenta la Tabla de Contenidos Mínimos definida al inicio de este capítulo.

Tabla Resumen

	Animaciones y Gráficos	Informar sobre delitos	Preguntas y respuestas	Acceso desde distintos dispositivos	Áreas	Contenido
<i>Segu-Kids</i>	No	Si	No	No	Jóvenes, Padres, Docentes	Completo
<i>Chicos en Internet</i>	No	SI	No	No	Niños y Jóvenes, Padres y Docentes	Incompleto
<i>Internet Segura Para Todos</i>	Si	No	No	No	Niños, Padres	Incompleto
<i>Internet Segura</i>	Si	No	No	No	Niños y Niñas, Adolescentes, Docentes	Incompleto
<i>Navega seguro</i>	No	Si	No	No	familia	Incompleto
<i>Internet Segura – IQUA</i>	No	No	No	No	Riesgos, Recomendaciones	Incompleto
<i>Navegando Seguros</i>	No	No	No	No	Menores de edad, Padres, Educadores	Completo

Conclusión

Como se puede observar en la Tabla Resumen, de todos los sitios analizados, Segu-Kids es el sitio más completo. La información que el resto de los sitios no están brindando es de mucha utilidad para aquellos usuarios que tienen el deseo de conocer cuáles son los riesgos que se presentan en Internet hoy en día y de qué forma pueden afrontarlos. **La mejor herramienta de seguridad con que contamos es la educación**, estar informados nos proporciona instrumentos para prevenir la gran cantidad de riesgos existentes en Internet y nos permite concientizarnos sobre las formas de protección y prevención, haciendo uso responsable de las tecnologías existentes. Por eso mismo, es indispensable que sitios como estos cuenten con la información necesaria para lograr que la comunidad tome conciencia y se prevenga de los riesgos realizando un uso adecuado de Internet.

Otro punto importante a destacar es la forma en que los sitios se dirigen a la comunidad, o sea el lenguaje que utilizan para expresar los conceptos, ideas, consejos, sugerencias, etc. Cuando nos dirigimos a niños y jóvenes el lenguaje a utilizar debe ser muy cuidado, ya que no es fácil captar su atención y lograr que comprendan sin inconvenientes, y más cuando se trata de temas como estos. Varios de los sitios analizados no tienen en cuenta este punto, como por ejemplo Segu-Kids, y se dirigen tanto a niños como a adultos de la misma forma. Para poder llegar a la comunidad entera y lograr que estos tomen conciencia el lenguaje utilizado debe ser el adecuado.

También debemos tener en cuenta que una sección de preguntas y respuestas sería lo ideal para que la comunidad pueda expresar sus inquietudes, sus problemas o sus dudas, y para que también puedan brindar sus opiniones, sus experiencias, o sus ideas. De los sitios visitados ninguno cuenta con una sección como ésta, no tienen foros, grupos, no se asocian a ninguna red social y ni tampoco permiten dejar comentarios. Lo ideal sería contar con un sitio que brindara a la comunidad la posibilidad de comunicarse y compartir.

No nos olvidemos que las Redes Sociales tienen un papel más que importante en la actualidad, los jóvenes y también los adultos acceden a ellas para compartir, para comunicarse, para expresar lo que sienten o piensan, para divertirse, etc. Una Red Social es un excelente instrumento para impartir conocimientos, sugerencias, consejos, experiencias y todo tipo de información útil. En la actualidad disponemos de una gran variedad de Redes Sociales de código abierto que podemos adaptar a nuestras necesidades (los costos serían cero). Entonces, una red social podría ser la herramienta adecuada para que sitios como estos puedan “atrapar” a la comunidad entera y lograr concientizarlos sobre los peligros que hay en Internet y brindarles consejos y sugerencias para que puedan de alguna forma estar prevenidos.

Hoy en día el acceso a Internet desde distintos dispositivos móviles (celular, iPad, notebooks, palms, etc) crece más y más y cada vez se hace más difícil controlar. Como se dijo antes la mejor herramienta de seguridad con las que contamos es la educación. De los sitios analizados, muy pocos brindan información, consejos o sugerencias para el uso adecuado de Internet desde dispositivos móviles. Tampoco se puede acceder a ellos desde dispositivos móviles como los celulares por ejemplo. Sería de mucha utilidad que un sitio

que debe informar e impartir conceptos tan importantes, como lo son los temas relacionados con la seguridad en Internet, pueda ser accedido desde distintos dispositivos móviles, y que brinde consejos, recomendaciones y sugerencias para estos dispositivos también.

Por último, observando la Tabla Resumen podemos notar que la mayoría de los sitios carecen de informes sobre delitos o noticia actuales. Un sitio con este tipo de información permite que la comunidad tome conciencia sobre lo que ocurre hoy en día en Internet que no siempre suele ser bueno. Existen noticias que pueden ser impactantes y un poco fuertes, pero lamentablemente eso es lo que muchas veces despierta en las personas la curiosidad y las lleva a informarse y a estar al tanto de lo que está pasando. Por eso mismo, estos informes suelen ser de mucha utilidad y aportan un granito más de arena para que la comunidad tome conciencia de los peligros que hay en Internet, se mantenga informada y pueda prevenirse.

Capítulo 3

Redes Sociales Open Source

Las Redes Sociales ocupan un lugar más que importante en la actualidad, tanto niños y jóvenes como adultos acceden a ellas para comunicarse, para expresar sus conocimientos o experiencias, para compartir, para divertirse, etc. Una red social no es sólo una herramienta para pasar el tiempo y divertirse con un grupo de amigos, una red social es un excelente instrumento para impartir ideas, sugerencias, consejos, recomendaciones y todo tipo de información útil. Para ello, es posible utilizar las Redes Sociales más populares de hoy en día como Facebook, Twitter, etc o implementar una propia, con herramientas Open Source disponibles (40 Redes Sociales Open Source [Ref6]).

En este capítulo se analizarán Redes Sociales Open Source disponibles en la Web con el objetivo de hallar la más adecuada para el desarrollo de FoCoS, una herramienta para concientización sobre seguridad en Internet, que se utilizará de soporte en el proyecto de “Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos”. Para cada Red Social se analizó e investigó sobre los siguientes puntos:

- Documentación:** Documentación existente que se brinde en el sitio oficial.
- Facilidad de adecuación:** Posibilidad de realizar mejoras de forma rápida y sencilla sin la necesidad de ser un experto en el tema.
- Mantenimiento:** Saber si se realizan actualizaciones frecuentes.
- Funcionalidades:** Que funciones útiles presenta.
- Acceso desde móviles:** Comprobar si es posible el acceso desde dispositivos móviles.
- Plugins:** Existencia de plugins útiles que puedan aplicarse.
- Perfiles de Usuarios:** Posibilidad de manejar diferentes perfiles de usuario con diferentes privilegios.
- Lenguajes:** Posibilidad de presentar el sitio en diferentes idiomas.
- Licencia:** Bajo que licencia se distribuye.
- Sitio oficial:** Link al sitio oficial.

Elgg

Elgg es una plataforma de Servicios de redes sociales de código abierto que ofrece comunicación (nos ayuda a poner conocimientos en común), comunidad (nos ayudan a encontrar e integrar comunidades) y cooperación (nos ayudan a hacer cosas juntos). Todo puede ser compartido entre los usuarios utilizando los controles de acceso y puede ser catalogado mediante tags (etiquetas). Elgg proporciona la funcionalidad necesaria para que podamos ejecutar nuestra propia Red Social.

Para ejecutar Elgg, es necesario contar con un servidor web y una cierta cantidad de conocimientos técnicos. Provee un framework para construir servicios web y exponer funcionalidades a otros sitios web y aplicaciones de escritorio haciendo integraciones con aplicaciones de terceros.

Elgg es un producto de código abierto liberado bajo la GNU Public License v2, lo que significa que el código fuente está licenciado para nuestro uso.

Es posible agregar más funcionalidades de las que Elgg ofrece en su forma más simple por medio de plugins.

En la siguiente tabla se presentan los puntos que consideramos para el análisis e investigación de cada Red Social.

Elgg	
Documentación	El sitio oficial brinda mucha información útil en español tanto para administradores, para desarrolladores como así también para el resto de las personas que estén interesadas y quieran conocer de qué se trata Elgg.
Facilidad de adecuación	El motor de Elgg está desarrollado en PHP y toda su estructura se encuentra programada en módulos. Posee un conjunto de vistas o interfaces muy bien organizadas, lo cual también ayuda y facilita la tarea de adecuación de la misma.
Mantenimiento	Elgg está en constante mantenimiento, las versiones cambian aproximadamente cada 3 meses y la comunidad de Elgg aporta continuamente una gran variedad de Plugins útiles.
Funcionalidades	<p>La mayor parte de las funcionalidades del usuario final en Elgg viene de los plugins. El paquete completo Elgg viene con una selección de plugins preinstalados.</p> <p>Elgg posee varias funcionalidades útiles, entre ellas podemos mencionar las siguientes:</p> <ul style="list-style-type: none">• Crear grupos que comparten intereses comunes o afiliaciones.• Subir videos y compartir fotos.• Celebrar debates en los foros.• Posibilidad de interactuar con otras personas. <p>En Elgg se realizan controles de seguridad para evitar la</p>

		inyección de código malicioso. Tanto el campo de login como la registraci3n de usuarios son seguros. Se realizan los filtros adecuados en todas las entradas de usuario para no permitir c3digo malicioso.
Acceso desde m3viles		En Elgg es posible el acceso desde diferentes dispositivos m3viles (tel3fonos celulares, iPhone), soporta m3ltiple vistas.
Complementos (Plugins)		La mayor parte de las funcionalidades del usuario final en Elgg viene de plugins. La comunidad Elgg aporta continuamente plugins de todo tipo, nuevas funcionalidades, nuevos estilos, etc.
Perfiles de usuario		S3lo se pueden manejar dos perfiles: Usuario Final y Administrador. No es posible crear diferentes perfiles con diferentes permisos.
Lenguaje		Diversidad de lenguajes. Los paquetes de lenguajes est3n disponibles para descargarlos en el sitio de la comunidad de Elgg. Hay paquetes de lenguajes para el n3cleo de Elgg y tambi3n hay paquetes de lenguajes para plugins espec3ficos.
Licencia		El paquete de Elgg completo est3 disponible bajo la licencia GNU (General Public License) versi3n 2.
Sitio Oficial		http://www.elgg.org/

Clonesumating

Clonesumating es un software de Redes Sociales basado en perfiles, etiquetas, blogs, propiedad digital y una variedad de funciones avanzadas.

Clonesumating cuenta con muchas de las funciones de Redes Sociales, incluyendo el manejo de perfiles de usuario, el etiquetado de usuario, actividades en grupo, calendario de eventos, etc.

A continuación se presenta una tabla con los puntos que consideramos para el análisis e investigación de cada Red Social.

Clonesumating	
Documentación	El sitio oficial no brinda ningún tipo de documentación
Facilidad de adecuación	El motor de Clonesumating se encuentra desarrollado en Perl y su estructura fue diseñada de forma compleja. Por tal motivo no es sencilla su adecuación salvo para programadores expertos.
Mantenimiento	No se realiza mantenimiento con frecuencia, sólo se publicaron 2 versiones: una en Abril del 2007 y la otra en Mayo del 2010.
Funcionalidades	Al no proporcionar plugins, todas las funcionalidades que se quieran agregar se deben programar y adherirlas al motor de Clonesumating. Entre sus funcionalidades brinda: <ul style="list-style-type: none">• manejo de perfiles de usuario• etiquetado de usuario• actividades en grupo• calendario de eventos
Acceso desde móviles	No es posible el acceso desde diferentes dispositivos móviles.
Complementos (Plugins)	No existen complementos para Clonesumating.
Perfiles de usuario	Clonesumating permite la creación de perfiles de usuarios con diferentes privilegios.
Lenguaje	Se encuentra disponible sólo en Inglés.
Licencia	Iniciativa Open Source OSI – Licencia MIT
Sitio Oficial	http://code.google.com/p/clonesumating/

Dolphin

Dolphin es una Red Social de código abierto, descargable, escalable y personalizable. Dolphin está compuesta por un conjunto de scripts PHP, plugins y aplicaciones móviles que proporcionan un control total.

Dolphin es escalable, rápida y probada en diversas comunidades online. Está respaldada por una selección de cientos de extensiones.

En la siguiente tabla se presentan los puntos que consideramos para el análisis e investigación de cada Red Social.

Dolphin	
Documentación	Dolphin no pone a disposición del usuario ningún tipo de documentación en su sitio oficial.
Facilidad de adecuación	Está desarrollado en PHP y todo el sitio se encuentra programado en módulos de forma organizada. Para desarrolladores con conocimientos en PHP no debería resultar compleja su modificación para agregar nuevas funcionalidades o adecuarlo a necesidades.
Mantenimiento	Dolphin está en constante mantenimiento y la comunidad aporta continuamente una gran diversidad de Plugins útiles. Las versiones son lanzadas con una periodicidad de dos meses.
Funcionalidades	Cuenta con una gran variedad de funcionalidades más las que se le pueden agregar a través de los plugins. Entre sus funciones podemos mencionar las siguientes: <ul style="list-style-type: none">• Detallar nuestro perfil.• Crear comunidades y redes de amigos.• Mantener nuestro blog.• Incluir fotos y vídeos.• Etiquetar todas nuestras entradas.• Importar contenido.
Acceso desde móviles	A través de Dolphin es posible el acceso desde diferentes dispositivos móviles.
Complementos (Plugins)	En esta red social es posible añadir o integrar diseños personalizados y características por medio de Plugins.
Perfiles de usuario	Permite crear múltiples niveles de membresía con permisos configurables. También es posible establecer diferentes niveles de acceso a todas las partes del sitio de la comunidad, incluyendo las páginas específicas e incluso bloques separados de página.
Lenguaje	Se encuentra disponible sólo en Ingles.

Licencia

BoonEx Dolphin Comercial de licencia permanente.

Dolphin es gratuito para descargar y usar. La copia gratuita debe mantener vínculos con BoonEx (empresa privada centrada en la comunidad del software) en todas las páginas, para eliminarlos, debemos pedir una licencia permanente o Prime (ambas son licencias pagas).

Sitio Oficial

<http://www.boonex.com/dolphin>

Applesed

Appleseed es una Red Social de código abierto, totalmente distribuida y descentralizada.

Con Appleseed es posible conectarse con amigos, enviar mensajes, compartir fotos y vídeos y participar en discusiones. El sitio se puede personalizar para satisfacer intereses y comunidades.

Cualquier persona puede descargar el software, instalarlo en cualquier servidor web, y conectar su sitio a la red de Appleseed.

Applesed	
Documentación	En el sitio oficial se presentan muy pocos documentos y sólo para desarrolladores.
Facilidad de adecuación	Está desarrollada en PHP y toda su estructura se encuentra programada en módulos. Para programadores con conocimientos en PHP no debería resultarles difícil adecuarla a sus necesidades.
Mantenimiento	Applesed se actualiza con periodicidad, se lanzan versiones cada 3 meses aproximadamente y la comunidad realiza buenos aportes al proyecto.
Funcionalidades	Cuenta con gran variedad de funcionalidades mas las que se le pueden agregar a través de los plugins. Podemos destacar: <ul style="list-style-type: none">• conectarse con amigos.• enviar mensajes.• compartir fotos y vídeos.• participar en discusiones.
Acceso desde móviles	No es posible en Applesed el acceso desde dispositivos móviles.
Complementos (Plugins)	Muchas de las funcionalidades del usuario final en Applesed vienen de plugins. Applesed en su forma más simple viene con una selección de plugins preinstalados.
Perfiles usuario de	En Applesed sólo es posible manejar dos tipos de perfiles: Usuario Final y Administrador. No es posible crear diferentes perfiles con diferentes permisos.
Lenguaje	Se encuentra disponible sólo en Inglés.
Licencia	Todo el código de Appleseed es 100% software libre bajo licencia GPL (General Public License).
Sitio Oficial	http://opensource.appleseedproject.org/

Mahara

Mahara consiste en: un sistema combinado de un portafolio y una red social. Un portafolio es un sistema donde los estudiantes podrán hacer una relación de "evidencias de aprendizaje permanente" tales como ensayos, obras de arte, o cualquier otra cosa que realicen y pueda ser almacenada en formato digital. Y los sistemas de Redes Sociales básicamente son sistemas diseñados para que la gente pueda interactuar con sus amigos y pueda crear sus propias comunidades en línea. Con Mahara, se puede controlar qué elementos y qué información pueden ver los otros usuarios.

Mahara proporciona una instalación de red social donde los usuarios pueden crear y mantener una lista de amigos dentro del sistema, elegir si otros usuarios pueden agregar a su lista de amigos de forma automática o por solicitud y su aprobación.

Mahara	
Documentación	Brinda información útil para administradores, para desarrolladores y para los usuarios. Se encuentra disponible en la Web una wiki en español de Mahara, el objetivo de esta wiki es proporcionar entre los usuarios que utilizan el español como primer idioma, una mejor comprensión de esta plataforma y de las muchas posibilidades que ofrece.
Facilidad de adecuación	Mahara ha sido diseñado desde el principio como un sistema abierto, un sistema conectable. Crear nuevas funcionalidades, autenticarse de forma personalizada y muchas más cosas pueden ser implementadas simplemente escribiendo un plugin que utilice de forma apropiada la API principal. Esto significa que es libre y fácil para personalizar casi todo en Mahara para que se adapte a nuestras necesidades.
Mantenimiento	Mahara es mejorado constantemente, cambia de versión con mucha frecuencia. En el último mes se lanzaron 5 versiones distintas y la comunidad Mahara se encuentra continuamente realizando aportes y ayudando a que este proyecto crezca más y más.
Funcionalidades	<p>Mahara ha sido diseñado como una aplicación web con una arquitectura plug-in. Esto significa que es posible la separación entre el hardware de los servidores de búsqueda, las bases de datos, el almacenamiento de archivos y la web.</p> <p>Además Mahara está diseñado para:</p> <ul style="list-style-type: none">• Equilibrar la carga entre varios servidores web.• Tener un sistema compartido de archivos desde un servidor centralizado. <p>Entre la gran cantidad de funcionalidades que ofrece podemos mencionar las siguientes:</p> <ul style="list-style-type: none">• Blogs.

		<ul style="list-style-type: none"> • Buzón de mensajes. • Lista de amigos. • Foros de grupos. • Perfiles. • Gestión de ficheros. <p>Mahara detecta automáticamente la configuración del sistema que representa una amenaza de seguridad.</p> <p>Proporciona una abstracción de base de datos y validación de entrada que impide los ataques de inyección de código malicioso.</p> <p>La autenticación del usuario puede estar vinculada a sistemas externos, como los sistemas de gestión de los estudiantes o bases de datos tales como su número de identificación de estudiante.</p>
Acceso móviles	desde	Es posible acceder a Mahara desde diferentes dispositivos móviles.
Complementos (Plugins)		El paquete completo Mahara viene con una selección de plugins preinstalados. Uno puede bajarse del sitio oficial una gran cantidad de plugins disponibles para extender la funcionalidad de Mahara.
Perfiles usuario	de	En Mahara se pueden manejar distintos perfiles con diferentes privilegios. El sitio permite realizar la gestión de instituciones, esto es, dar de alta una institución y permitir que los usuarios (alumnos o estudiantes) formen parte de ella. En estas instituciones se pueden crear grupos de trabajo (no son los grupos creados por cada usuario) para controlar al resto de los usuarios, con estos grupos trabajo se podría monitorizar las vistas para controlar que lo que se publica es adecuado, censurar determinados feedback, etc.
Lenguaje		Diversidad de lenguajes. Los paquetes de lenguajes pueden descargarse del sitio oficial e instalarse.
Licencia		Mahara se distribuye gratuitamente como software de código abierto (bajo la GNU General Public License versión 3). Debido a que es software de código abierto, otras organizaciones están invitadas a contribuir a la evolución del software.
Sitio Oficial		http://mahara.org/

OpenPNE

OpenPNE es un motor de servicio de red social, escrito en PHP. Tiene muchas características: control de amigos, invitación de un amigo, un diario, blog, buzón de mensajes, etc. Es un software de código abierto y libremente disponible para cualquier persona de forma gratuita.

OpenPNE está comprometido con el software de comunicación y se puede utilizar cómodamente en cualquier organización, y alinear a las distintas funciones.

OpenPNE	
Documentación	El sitio oficial brinda información útil para desarrolladores y para usuarios.
Facilidad de adecuación	El motor de OpenPNE se encuentra desarrollado en PHP y su diseño modular maximiza la flexibilidad y extensibilidad.
Mantenimiento	Actualizaciones periódicas. Se actualiza la versión aproximadamente cada un mes.
Funcionalidades	OpenPNE presenta las funcionalidades básicas de una red social: <ul style="list-style-type: none">• Amigos.• Un diario.• Blog.• Buzón de mensajes.• Entre otras.
Acceso desde móviles	No es posible el acceso desde dispositivos móviles a OpenPNE.
Complementos (Plugins)	Es posible añadir o integrar diseños personalizados y características a través de los Plugins.
Perfiles de usuario	No es posible definir diferentes perfiles con privilegios propios.
Lenguaje	Disponible en Japonés e Inglés.
Licencia	GNU General Public License (GPL).
Sitio Oficial	http://www.openpne.jp/

Ospo

OSPO es un proyecto Open Source de red social. Brinda las funciones estándar (añadir y quitar amigos, top10, etc), la integración de foros, el módulo de música (directorio de artistas con los álbumes, canciones), la integración de shoutcast, blog (añadir, borrar, modificar, ver, etc) y entre otras cosas.

Ospo	
Documentación	No hay documentación disponible en el sitio oficial de Ospo
Facilidad de adecuación	El motor de Ospo se encuentra desarrollado en PHP y su diseño modular facilita su adecuación para desarrolladores con conocimientos en php.
Mantenimiento	OSPO no es actualiza hace tiempo. Sólo se lanzo una única versión en el 2007.
Funcionalidades	Ospo presenta las funcionalidades básicas de una red social: <ul style="list-style-type: none">• Detallar nuestro perfil.• Crear comunidades y redes de amigos.• Incluir fotos y vídeos.• Buzón de mensajes.• Entre otros.
Acceso desde móviles	No es posible el acceso desde dispositivos móviles.
Complementos (Plugins)	No existen complementos disponibles.
Perfiles de usuario	No es posible definir diferentes perfiles con privilegios propios.
Lenguaje	Disponible sólo en Inglés.
Licencia	GNU General Public License (GPL).
Sitio Oficial	http://ospo.sourceforge.net/

AstroSPACE

AstroSPACES es una de las primeras soluciones de código abierto de Redes Sociales, es muy eficiente y muy fácil de usar.

Esta red social se puede alojar en un servidor propio, donde se puede tener control completo sobre los miembros de su comunidad y contenido del sitio.

AstroSPACE	
Documentación	El sitio oficial no brinda ningún tipo de documentación.
Facilidad de adecuación	El motor de AstroSPACE se encuentra desarrollado en PHP. Su estructura no se encuentra diseñada completamente de forma modular lo que dificulta la labor de un programador que desea realizar adecuaciones para satisfacer sus necesidades.
Mantenimiento	AstroSPACE no ha sufrido muchas actualizaciones. La última versión fue lanzada en 2009.
Funcionalidades	Presenta las funcionalidades básicas de una red social. <ul style="list-style-type: none">• Buzón de mensajes.• Subir fotos y videos para compartir.• Grupos de amigos.• Un diario.• Entre otras.
Acceso desde móviles	Es posible acceder a AstroSPACE desde dispositivos móviles.
Complementos (Plugins)	No se desarrollaron complementos para integrar a AstroSPACE.
Perfiles de usuario	No es posible definir diferentes perfiles con privilegios propios.
Lenguaje	Disponible sólo en Inglés.
Licencia	GNU General Public License (GPL).
Sitio Oficial	http://ospo.sourceforge.net/

FlightFeather

FlightFeather es una red social creada con la intención de que cualquier persona pueda tener la oportunidad de ejecutar un sitio de Redes Sociales en el hardware mínimo y sin desperdiciar ancho de banda.

Capacidad de respuesta y conservación de los recursos fue el objetivo de diseño más importante de FlightFeather.

FlightFeather	
Documentación	En el sitio oficial no existe documentación disponible para los usuarios y desarrolladores.
Facilidad de adecuación	El motor de FlightFeather se encuentra desarrollado en Python y su estructura se encuentra diseñada de forma compleja. Por tal motivo no es sencilla su adecuación salvo para programadores expertos.
Mantenimiento	No se actualiza hace tiempo. Sólo se lanzaron unas pocas versiones en el 2007.
Funcionalidades	Presenta las mismas funcionalidades básicas que la red social analizada anteriormente.
Acceso desde móviles	No es posible con FlightFeather el acceso desde dispositivos móviles.
Complementos (Plugins)	No se desarrollaron complementos para este motor.
Perfiles de usuario	No es posible definir diferentes perfiles con privilegios propios.
Lenguaje	Se encuentra disponible sólo en Inglés.
Licencia	GNU General Public License (GPL).
Sitio Oficial	http://flightfeather.sourceforge.net/

Conclusión

Como podemos observar existen disponibles en la Web una gran variedad de Redes Sociales Open Source que están a nuestra disposición para descargarlas y adaptarlas a nuestras necesidades. La mayoría de estas Redes Sociales siguen un paradigma de programación llamado “programación modular” lo cual genera un código más legible y manejable. Si bien, estas Redes Sociales siguen un buen paradigma de programación que facilita su adecuación sólo dos de ellas (Elgg y Mahara) presentan la documentación suficiente como para comprender completamente su estructura y poder abordar un nuevo desarrollo o una nueva funcionalidad sin inconvenientes.

Todas estas Redes Sociales vienen por defecto en inglés, Elgg y Mahara son las únicas que brindan los paquetes para traducirlas al español. La traducción al español que se puede hacer en Elgg no es 100% completa, algunas palabras y oraciones no son traducidas. En Mahara la traducción es más completa, prácticamente no quedan oraciones ni palabras sin traducir.

Un punto importante a tener en cuenta es que el acceso a Internet desde distintos dispositivos móviles (celular, iPad, notebook, palms, etc) crece más y más determinando distintas condiciones de uso y seguridad. Por fortuna, la mayoría de las Redes Sociales analizadas cuentan con la posibilidad de ser accedidas desde distintos dispositivos móviles ya que soportan múltiples vistas.

En cuanto al mantenimiento que se les realiza, por lo general, son actualizadas frecuentemente y su comunidad aporta soluciones inmediatas a los problemas que surgen.

Un aspecto importantísimo que se evaluó en cada red social fue la posibilidad de poder generar diferentes perfiles con distintos privilegios, ya que resulta imprescindible contar con una herramienta que posea esta funcionalidad para poder dar soporte al proyecto de “Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos”.

Resumiendo, podemos llegar a la conclusión de que existen varias y muy buenas Redes Sociales open Source disponible para descargar y adaptar a nuestras necesidades. A pesar de que algunas de ellas pueden ser utilizadas sin inconvenientes, si tuviéramos que elegir hoy en día una, sin dudas sería Mahara ya que es la que cumple en su totalidad con todos los requisitos que debe tener una herramienta para convertirse en FoCos y poder dar soporte al proyecto de Caperucita.

Capítulo 4

Herramientas o métodos para la detección del tipo de acceso

Construir una red social como apoyo a la concientización en seguridad y privacidad sobre Internet resulta de mucha utilidad para la comunidad.

La incorporación de un módulo que permita reconocer desde donde accede el usuario y así poder adecuar los consejos y recomendaciones al tipo de acceso, permitiría personalizar el servicio y, dada la gran variedad de dispositivos de acceso a web existentes en la actualidad y a su uso masivo, resultaría casi indispensable.

Existen en la Web diferentes alternativas para detectar la tecnología desde donde accede el usuario. El objetivo de este capítulo es presentar algunas de ellas para tenerlas en cuenta a la hora de desarrollar el prototipo planteado en esta tesina.

Las herramientas analizadas aquí fueron elegidas teniendo en cuenta su posible integración con FoCoS. Para esto, debe ser open source, respetar estándares e integrarse adecuadamente con las posibles redes sociales a utilizar.

Get Browser

`Get_browser()` [Ref15] es una función de PHP que permite obtener información sobre el navegador.

Esta misma información, podemos averiguarla con PHP accediendo a las variables del sistema. En particular, podemos averiguar el navegador y el sistema operativo que está utilizando el usuario con la variable de sistema del servidor `$_SERVER['HTTP_USER_AGENT']`. Pero esta variable nos ofrece una información que no es fácil de interpretar. Por ejemplo, en Internet Explorer 7, esta variable tendrá el siguiente valor:

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1).

Si utilizamos Firefox en la misma computadora, al ver el contenido de esta variable obtendremos el siguiente valor:

Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.8.0.10) Gecko/20070216 Firefox/1.5.0.10.

En realidad, a partir de esa información y realizando algunos cálculos y comparaciones, podríamos deducir las funcionalidades que soporta el navegador y qué sistema operativo se está utilizando. Pero para resolver esto de forma más simple podemos utilizar una función que nos va a devolver directamente la información bien trabajada y lista para utilizar. Directamente podremos saber si el navegador soporta distintas funcionalidades o tecnologías y qué sistema operativo corre en la máquina del usuario, sin necesidad de deducir nada y sin necesidad de conocer todos los navegadores existentes.

`get_browser()` indica de lo que es capaz el navegador del usuario y nos permite obtener información adicional como el sistema operativo que el usuario está utilizando y la tecnología desde la cual está accediendo. Intenta determinar las capacidades del navegador consultando el archivo de información del navegador *browscap.ini*. Este archivo contiene una lista de todos los navegadores existentes desde su primera versión hasta la última.

`get_browser` ([string *\$user_agent* [bool *\$return_array* = false]])

user_agent: Por omisión, se utiliza el valor de la cabecera HTTP User-Agent; sin embargo, se puede alterar este comportamiento (es decir, consultar la información de otro navegador) pasando el parámetro opcional *user_agent* a *get_browser()*. Es posible ignorar el parámetro *user_agent* con el valor NULL.

return_array: Si está establecido a TRUE, esta función devolverá un array en vez de un object.

La información se devuelve en un objeto, el cual contendrá varios elementos de datos que representan, por ejemplo, los números de versión mayor y menor del navegador; valores TRUE/FALSE para características como los frames, JavaScript, y cookies; y así sucesivamente.

A continuación presentamos un ejemplo escrito en el lenguaje PHP para listar toda la información sobre el navegador del usuario.

```

<?php
$navigator = get_browser(null, true);
while (list($key, $val) = each($navigator)) {
    echo "<br>$key => $val \n";
}
?>

```

El resultado del ejemplo sería el siguiente:

```

browser_name_regex → $^mozilla/5\0 \(. *windows nt 5\1.*\)
applewebkit/* \.(html, like gecko).*chrome/14\..*safari/*$$
browser_name_pattern → Mozilla/5.0 (*Windows NT 5.1*) AppleWebKit/*
(KHTML, like Gecko)*Chrome/14.*Safari/*
parent → Chrome14
platform → WinXP
browser → Chrome
version → 14.0
majorver → 14
win32 → 1
frames → 1
iframes → 1
tables → 1
cookies → 1
vbscript → 1
javaapplets → 1
cssversion → 3
minorver → 0
alpha= → 0
beta → 0
win16 → 0
win64 → 0
backgroundsounds → 0
javascript → 0
activexcontrols → 0
isbanned → 0
ismobiledevice → 0
issyndicationreader → 0
crawler → 0
aolversion → 0

```

Como podemos observar, esta función nos brinda mucha información sobre el navegador.

La tabla que se presenta a continuación expone de forma sencilla los parámetros más significativos, de los cuales podemos sacar provecho a la hora de analizar desde donde está accediendo el usuario, para poder brindar buenos consejos o sugerencias sobre seguridad.

Parámetro	Descripción
Parent	Este parámetro contiene el nombre del navegador y su versión.
Platform	Define el sistema operativo que está usando el usuario. Por ejemplo: Windows XP, Vista o 7, Linux, Unix, etc.
Browser	Contiene sólo el nombre del navegador.
Versión	Contiene sólo la versión del navegador.
MajorVer	En este parámetro se almacena la parte mayor de la versión del navegador. Por ejemplo, si la versión es 5.1, en esta variable se almacenará el 5.
MinorVer	En este parámetro se almacena la parte menor de la versión del navegador. Por ejemplo, si la versión es 5.1, en esta variable se almacenará el 1.
Cookies	Este parámetro determina si el navegador acepta cookies o no.
VBScript	Este parámetro determina si es posible la ejecución en el navegador de un script desarrollado en Visual Basic.
JavaApplets	Este parámetro determina si es posible la ejecución en el navegador de aplicaciones Java.
javascript	Determina si el navegador soporta javascript.
isMobileDevice	Define si el usuario está accediendo desde un dispositivo móvil (celular, iPad, palms, iphone, etc).

Como podemos ver, sería muy sencillo obtener cualquier dato sobre el navegador y las tecnologías que soporta. Por ejemplo, para saber si soporta Javascript accederíamos a la propiedad `$navegador->javascript`. Si vale 1 es que lo soporta y si el valor es 0 es que no lo soporta.

Vale aclarar que el valor `cookies` simplemente quiere decir que el navegador mismo tiene la capacidad de aceptar cookies y no quiere decir que el usuario haya habilitado el navegador para que acepte cookies o no.

Para que esto funcione, se debe configurar el archivo de configuración de PHP *php.ini* para que el parámetro “browscap” apunte correctamente a la ubicación del archivo *browscap.ini* en nuestro sistema. Browscap.ini no forma parte de la distribución de PHP, pero se puede encontrar un archivo *browscap.ini* actualizado en la Web (Browser Capabilities Project [Ref16]).

Aunque *browscap.ini* contiene información sobre varios navegadores, depende de las actualizaciones del usuario para mantener la base de datos al día.

Browser detect

Browser detect [Ref17] es un script escrito en el lenguaje de programación Javascript utilizado para detectar propiedades del navegador del usuario.

Este script funciona como cualquier otro script, tan sólo debe ser copiado en el directorio donde se encuentran los archivos de Javascript y funciona de inmediato.

Browser detect retorna como resultado un objeto con ciertas propiedades que nos permiten obtener información sobre el navegador o el sistema operativo que está utilizando el usuario.

Se pueden consultar tres propiedades del objeto BrowserDetect devuelto por este script.

- **Nombre del navegador:** BrowserDetect.browser.
- **Versión del navegador:** BrowserDetect.version.
- **Nombre del sistema operativo:** BrowserDetect.OS.

Este script sólo seguirá siendo útil siempre y cuando comprobemos que los nuevos navegadores todavía siguen las reglas establecidas en el mismo.

La clave de la detección del navegador del usuario es saber dónde buscar la información necesaria. Este script utiliza navigator.userAgent, ésta es una variable que devuelve información completa sobre el agente de usuario.

Detect Mobile Browser

Detect Mobile Browser [Ref18] es un proyecto Open Source que nos ofrece scripts en diferentes lenguajes (.htaccess de Apache, JSP, PHP, Rails, ASP, Perl, Python, Javascript y ColdFusion). Con estos scripts podemos saber si un usuario está accediendo desde un dispositivo móvil (celular, iPad, palms, iphone, etc) o desde su máquina de escritorio.

Este proyecto se encuentra en constante mantenimiento, con lo cual los scripts se encuentran actualizados.

A continuación se presenta una imagen del sitio oficial que brinda esta herramienta y como podremos observar, en la página de inicio utiliza *Detect Mobile Browser* para comprobar si estamos accediendo desde un dispositivo móvil.

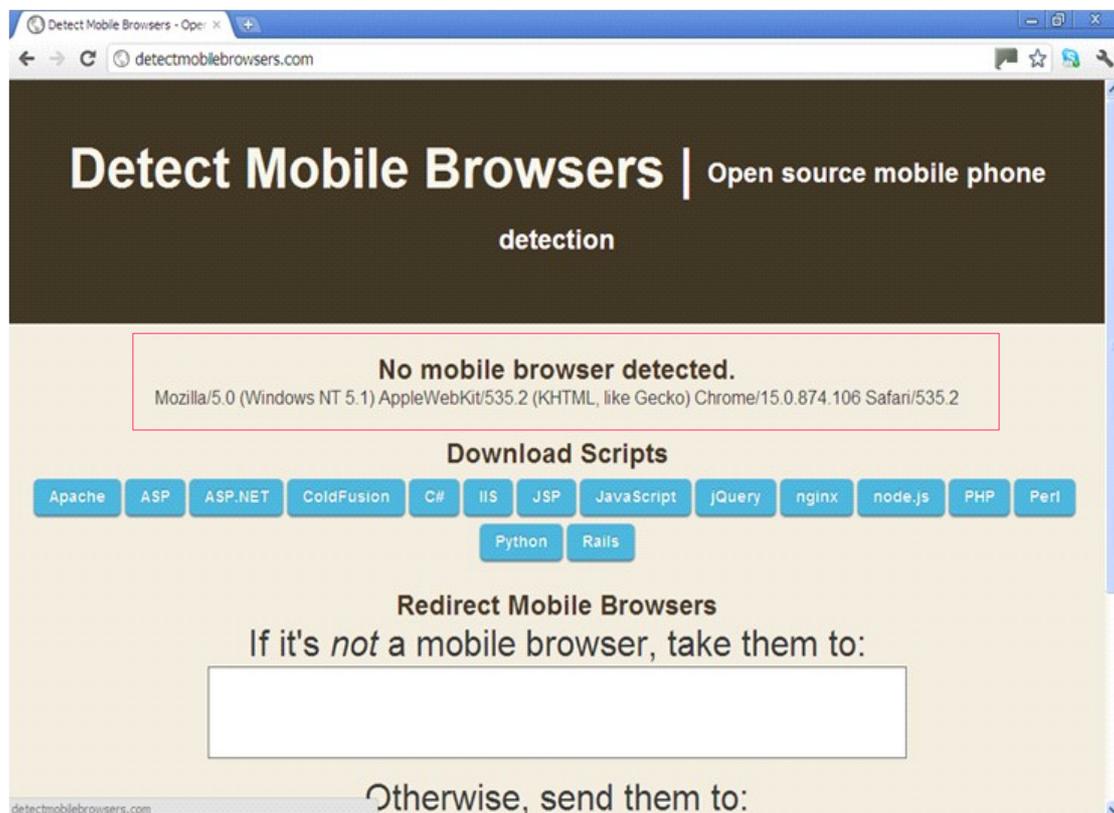


Figura 22: Detect Mobile Browser

Como podemos ver, el sitio nos informa que no detectó ningún dispositivo móvil (No mobile browser detect) y nos brinda información de nuestro navegador, es decir que detectó desde donde estamos accediendo y que características posee el navegador que estamos utilizando. De la misma forma, nosotros podríamos descargarnos el script (seleccionando cualquiera de los lenguajes definidos en el sitio oficial nos descarga automáticamente el script en el lenguaje seleccionado) y embeberlo en el código de nuestra página de inicio para identificar si el usuario accede desde un dispositivo móvil.

jQuery.browser

jQuery es una biblioteca de Javascript que permite simplificar la manera de interactuar con los documentos HTML, manipular el árbol DOM, manejar eventos, desarrollar animaciones y agregar interacción con la técnica AJAX a páginas web.

jQuery provee numerosas funcionalidades que ahorran tiempo a la hora de desarrollar aplicaciones web. Entre estas funcionalidades provee la función *jQuery.browser* [Ref19].

jQuery.browser es una función que permite identificar de forma única los navegadores de los usuarios.

Esta función devuelve un objeto en Javascript que contiene toda la información sobre el navegador del usuario. También agrega los selectores CSS del navegador, lo que significa que se puede modificar elementos de estilo o escribir funciones para navegadores específicos.

jQuery.browser nos permite acceder a la información del navegador del usuario de forma sencilla e intuitiva. Por ejemplo, puede ser así de simple:

```
<!DOCTYPE html>
<html>
<head>
  <style>
    p { color:blue; margin:20px; }
    span { color:red; }
  </style>
  <script src="http://code.jquery.com/jquery-latest.js"></script>
</head>
<body>

<p></p>
<script>
$("p").html( "El número de versión del navegador es el siguiente: <span>" +
  $.browser.version + "</span>" );
</script>
</body>
</html>
```

El resultado que arrojaría sería el siguiente

```
El número de versión del navegador es el siguiente: 535.2
```

Así podemos obtener la versión del navegador que está utilizando el usuario. De la misma manera podríamos identificar mucha más información utilizando alguna de las siguientes funciones:

- browser.name:** El nombre del navegador utilizado.
`alert ($ browser.name.) // "chrome".`
- browser.versionNumber:** La versión del navegador (como un entero).

```
alert ($ browser.versionNumber.) // "14".  
alert ($ browser.versionNumber + 1.) // "15".
```

•**browser.versionX**: El lanzamiento del navegador (2x, 3x, etc.).

```
alert ($ browser.versionX.) // "1".
```

•**layout.name**: El nombre del motor de diseño que se utiliza.

```
alert ($ layout.name.) // "webkit".
```

•**os.name**: El sistema operativo utilizado.

```
alert ($ os.name.) // "win".
```

jQuery.browser se encuentra bajo la licencia GPL. Esto quiere decir que este programa es software libre: podemos redistribuirlo y/o modificarlo bajo los términos de la Licencia Pública General (GPL) publicada por la Free Software Foundation.

Tabla comparativa

A continuación se expone una tabla comparativa que muestra cómo operan las herramientas mencionadas en este capítulo. Se toma como ejemplo el acceso desde el navegador Chrome versión 14 corriendo desde la plataforma Windows XP.

	get_browser()	Browser detect	Detect Mobile Browser	jQuery.browser
Nombre del Navegador	Chrome	Chrome	-	chrome
Versión del navegador	14.0	14	-	14.0
Sistema Operativo	Win XP	Win32	-	win
Dispositivo Móvil ?	0	-	0	-
Navegador acepta Cookies ?	0	-	-	-

Como podemos observar los resultados arrojados por cada herramienta son similares. En cuanto a los parámetros de *Dispositivo Móvil* y *Navegador acepta Cookies*, los posibles valores son 0 (NO) o 1(SI).

Conclusión

Como pudimos observar existen formas simples de conocer desde donde accede el usuario y que características posee el agente de usuario o navegador por el cual está accediendo.

Todas estas técnicas utilizan la variable de sistema del servidor `$_SERVER['HTTP_USER_AGENT']`. En esta variable se encuentra toda la información necesaria para poder deducir:

- Qué navegador está utilizando el usuario y cuáles son sus principales características.
- Si está accediendo desde un dispositivo móvil o no.
- Qué sistema operativo está utilizando.

Entonces, para lograr un correcto reconocimiento del tipo de acceso del usuario sólo basta con poner en marcha alguno de los script mencionados anteriormente o también se podría realizar una combinación de ellos para obtener resultados más específicos.

Si bien cualquiera de las herramientas planteadas aquí podrían ser de utilidad para el desarrollo de FoCoS, elegimos la función estándar “Get Browser” que nos brinda PHP, ya que la misma es muy completa y se alimenta de una enorme base de datos con las últimas versiones de los navegadores disponibles en la actualidad y no requiere de la utilización de ninguna librería adicional.

Capítulo 5

FoCoS: Una herramienta para concientización sobre seguridad en Internet.

Como ya hemos mencionado anteriormente, implementar un entorno de difusión de contenidos sobre Privacidad y Seguridad de la Información, con orientación a los distintos tipos de usuarios resultaría de mucha utilidad. Pero integrar al mismo, una Red Social de manera tal de generar una comunidad alrededor de la temática, incorporando el manejo de roles y enfocado al proyecto “Caperucita fue víctima de la Ingeniería Social”, sería aún más útil y brindaría aún más beneficios/oportunidades. No nos olvidemos que las Redes Sociales ocupan un lugar más que importante en la actualidad, tanto niños y jóvenes como adultos acceden a ellas para comunicarse, para expresar sus conocimientos o experiencias, para compartir, para divertirse, etc.

También, la incorporación de un módulo que permita reconocer desde donde accede el usuario y así poder adecuar los consejos y recomendaciones al tipo de acceso, permitiría personalizar el servicio y, dada la gran variedad de dispositivos de acceso a web existentes en la actualidad y a su uso masivo, resultaría casi indispensable.

FoCoS sería la integración de todo esto, a través de FoCos la comunidad podrá tomar conciencia de los riesgos que se presentan en Internet.

FoCoS es un Sitio Web que se enfoca exclusivamente en la seguridad en Internet, desarrolla una gran variedad de temas, dando consejos y sugerencias, presentando herramientas para la protección y control, etc. Con este sitio también es posible compartir y comunicarse, ya que cuenta con el soporte de una Red Social en la cual uno no sólo puede pasar el tiempo y divertirse con un grupo de amigos, sino que también puede expresar ideas, sugerencias, consejos, recomendaciones y todo tipo de información útil.

Por último, FoCoS cuenta con un módulo que identifica desde dónde accede el usuario y qué características tiene el equipo del cual accede, y a partir de esto, brinda consejos, sugerencias o recomendaciones determinando de esta forma distintas condiciones de uso y seguridad. Este módulo puede ser accedido tanto por PCs como por dispositivos móviles (las interfaces están adaptadas a ellos).

En este capítulo se presentará FoCoS, se mostrarán los módulos que contiene, las funciones que brinda y las actividades que se pueden realizar en él. Adicionalmente, se entrará en detalle de las tareas que fueron realizadas para alcanzar lo que hoy es esta herramienta de difusión de contenidos sobre Privacidad y Seguridad de la Información

Entonces, primero analizaremos FoCoS como Sitio Web, luego hablaremos sobre el módulo de identificación de dispositivos que tiene integrado, y por último entraremos en detalle sobre la Red Social que da soporte.

Para acceder a FoCoS y conocerla en detalle pueden abrir su navegador y acceder a la dirección <http://focos-seguridad.no-ip.org/>.

FoCoS: el Sitio Web.

Tras el análisis realizado en el Capítulo 2 de los sitios web en español orientados a la Seguridad y Privacidad en Internet, y las falencias halladas en dichos Sitios, surge la necesidad de Implementar un entorno de difusión de contenidos sobre Privacidad y Seguridad de la Información, con orientación a los distintos tipos de usuarios: jóvenes, padres y docentes. Este entorno reuniría todos los aspectos positivos y tendría en cuenta aquellos puntos negativos detectados, con la intención de ofrecer un sitio más adecuado.

Para la construcción de FoCoS se recabó información de las páginas web analizadas en el capítulo 2, de libros, informes, monografías, etc (ver bibliografía), como así también del proyecto Caperucita.

Aspectos que se tuvieron en cuenta a la hora de implementar FoCoS:

- El lenguaje utilizado depende exclusivamente de la sección en la que nos encontremos. Es decir, no se utilizó la misma forma de expresión para dirigirse a los jóvenes, padres y docentes; la división en secciones no es sólo para dar una orientación de cuáles son los temas que les podrían interesar o ser útil a uno o a otro (dependiendo de la edad) si no para mostrar contenido de forma tal que si un adolescente lee pueda comprender sin ningún problema y no tenga que buscar palabras que desconoce o no tenga que releer varias veces porque no puede entender lo que se le está explicando.
- En cuanto al contenido de información, se tratan todos los temas con un buen nivel de detalle. En algunos casos fue necesario profundizar aún más para que se pueda comprender el grado de importancia de ciertos temas.
- La información está dividida en tres secciones: Jóvenes, Padres y Docentes. Esto es muy útil ya que existen ítems que pueden ser de interés para los jóvenes y no para los adultos, y viceversa. Mantener la información organizada en un Sitio es importante.

A continuación presentamos la página de inicio de la Web FoCoS (<http://focos-seguridad.no-ip.org/>). En la misma podemos observar las tres secciones desarrolladas: Jóvenes, Adultos y Docentes.

FoCoS

Inicio Comunidad Recomendar Buscar

Jóvenes

Padres

Docentes

Consejos y sugerencias útiles para vos...

Clickea este globo y nosotros detectaremos que inseguridades hay en tu maquina y te daremos soluciones claras y precisas para que puedas aplicarlas sin inconvenientes.

¡¡Suerte!!

Bienvenidos

FoCoS es un nuevo espacio creado para brindar información a Jóvenes, Padres y Docentes sobre Seguridad en Internet. Este sitio brinda información en forma libre y gratuita y fue pensado con el objetivo de apoyar y acompañar a la familia y a los educadores. El nacimiento de FoCoS se debe a la gran cantidad de riesgos existentes en Internet y a la necesidad de crear concientización y educación sobre las formas de prevención y protección, haciendo uso responsable de las tecnologías existentes. Los invitamos a conocer FoCoS y a dejarnos sus experiencias para que sigamos creciendo juntos en la red.

Política de privacidad | Acerca de | Formulario de contacto

Figura 23: Página de inicio FoCoS - <http://focos-seguridad.no-ip.org/>

Ingresando en alguna de las secciones se despliega el menú con todos los ítems que se desarrollan. A continuación se presentan las imágenes con los temas presentes en cada sección.



Figura 24: Sección para Jóvenes en FoCoS

Sección Jóvenes:

- Las Contraseñas
- Las Redes Sociales
- El Chat
- El Correo Electrónico
- El Cyber
- Los Virus
- El Blog y Fotolog
- Foros y Grupos
- Consejos



Figura 25: Sección para Padres en FoCoS

Sección Padres:

- Cyberbullying y Ciberacoso
- Grooming
- La Pedofilia
- El Correo Electronico
- El Cyber
- Los Virus
- El Blog y Fotolog
- Foros y Grupos
- Consejos



Figura 26: Sección para Docentes en FoCoS

Sección Docentes:

- Edad de los menores
- Intimidad y Privacidad
- Organizaciones
- Preguntas Frecuentes
- Material de apoyo
- Los Virus
- Estadísticas

Como pudimos observar, el sitio abarca una gran variedad de temas importantes que la comunidad debe conocer e informarse.

FoCoS: el modulo de identificación de dispositivos.

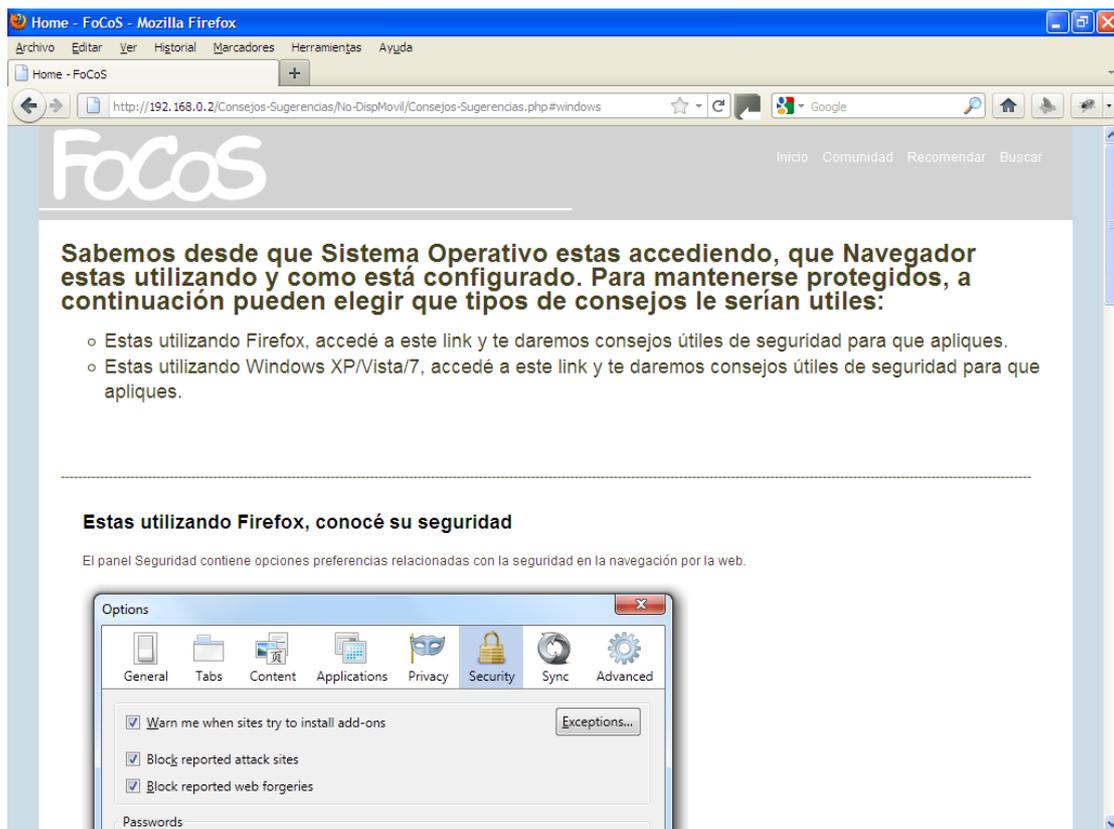
Tomando como base el análisis realizado sobre herramientas o métodos para la detección del tipo de acceso en el Capítulo 5, se implementó un módulo que reconoce desde donde está accediendo el usuario, ya sea desde una PC o un dispositivo móvil, y brinda consejos, sugerencias o recomendaciones para el mismo.

El módulo entra en acción cuando accedemos a FoCoS. El mismo funciona de la siguiente forma:

- Si una persona accede al sitio desde su computadora de escritorio o desde una computadora portátil la primera página que le aparecerá será la página de inicio de FoCoS (ver figura 23).

En la página de inicio se presenta un cuadro que dice “Consejos y sugerencias útiles para vos”, si accedemos aquí se nos presentarán consejos y sugerencias útiles para nuestra computadora (recuerden que estamos accediendo desde nuestra computadora).

La siguiente imagen es un ejemplo de lo que nos mostraría el sitio al acceder desde una computadora que tiene instalada Windows XP y el navegador Mozilla Firefox.



- Si una persona accede al sitio desde un dispositivo móvil, por ejemplo desde un teléfono inteligente, la primera página que se le mostrará será otra.

A continuación podemos observar cómo se muestran los datos accediendo a FoCoS desde un Nokia. Se le agregó un Plugin (User

Agent Switcher Ref[20]) al navegador para poder simular el acceso desde el Nokia, es decir, con este plugin le hacemos creer a FoCoS que estamos accediendo desde un teléfono celular Nokia.



Figura 27: Página de inicio FoCoS accediendo desde un dispositivo móvil

Como podemos observar, ya no tenemos las opciones de Jóvenes, Padres y Docentes que teníamos al ingresar desde una computadora de escritorio. Esto es así por que cuando accedemos desde un dispositivo móvil el sitio automáticamente lo detecta a través del modulo implementado y nos muestra directamente los consejos, sugerencias y recomendaciones para dicho dispositivo.

Sólo esta sección está adaptada para ser vista correctamente desde un dispositivo móvil, por ese motivo cuando accedemos al sitio desde un celular nos envía automáticamente a esta sección. De todos modos es posible navegar el sitio completo desde un dispositivo móvil. Hoy en día contamos con una gran variedad de celulares inteligentes que nos permiten navegar sitios que no están adaptados a ellos.

Implementación

Para la implementación de dicho módulo se utilizó la función estándar de PHP `Get_Browser` y el script de `Detect Mobile Browser` (en el capítulo 5 se explica cómo funcionan ambas).

A continuación se muestra una imagen donde podemos observar el código desarrollado para la implementación del módulo. Este código define si el acceso es realizado desde un dispositivo móvil o no. Se usan ambas, la función `get_browser` y el script de `Detect Mobile Browser` (marcado en color gris), para generar más confianza a la hora de definir si el acceso es desde un dispositivo móvil. En caso de que una de las funciones falle (por falta de actualización por ejemplo) la otra puede responder identificando correctamente el tipo de acceso.

```
1 <?php
2 $useragent=$SERVER['HTTP_USER_AGENT'];
3 $navegador = get_browser(null, true);
4
5 If ( ($navegador["ismobiledevice"]== 1) ||
6 preg_match('/android|mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)
7 iris|kindle|lge |maemo|midp|mmp|netfront|opera m(ob|in)|palm| os) ?phone|p(ixi|re)\/|plucker|pocket|ppap|symian
8 treo|up\.(browser|link) |vodafone|wap|windows (ce|phone)|xda|xiino\/', $useragent) || preg_match('/1207|6310|6590|3gso
9 4thp|50|1-6|1770s|802s|a wa|abac|ac(er|oo|s\-)|al(ko|rn)|al(av|ca|co)|amoi|an(ex|ny|yw)|aptar|chigo|as(tel|us)
10 attw|au(di|v)-m|r |s |avan|be(ck|llinq)|bi(lbrd)|bl(ac|az)|br(e|v)w|bumb|bw-(n|u)|c55\/|cpai|ccwa|cdm-|cell|cht
11 dld|cmd|-|co|mpnd|crawida|it|ll|ng|dte|dov-s|devi|dica|dmob|do(c|p)|ods(12|d)tel(49|ai)|em(12|ul)|er(ic|k0)
12 es|l|ez([4-7]0|os|wa|ze)|fetc|fly(\-|_) |g| ui|g560|gene|gf(-5)g|moigo(\.w|od) |gr(adi|un)|hail|hcit|hd|-|mpit|hei\=
13 |hi(pt|ta)|hp( i|ip)|hsv-c|ht(c|v-|_)|s|g|p|s|t|tp)|hu(aw|tc)|i(\-|20|go|ma)|i230|iac( |\/-|\/)|ibro|idea|ig01|ikom|
14 imk|inno|ipaq|iris|ja(t|v)a|jbro|jemu|jigs|kddi|keji|kgt( |\/)|klon|kpt |kwc|-|kyo(c|k)|le(no|xi)|lg( g|\/|k|ll)u|50
15 |54|e(-|e|\/|\/-|a-w)|l1bw|lynx|m1\-\-wim|qa|m50\/|ma(te|ui|xo)|mc(01|2i|oa)|m(-cr|me|di|rc|r)|mi(o8|oa|ts)|mmef|mo(01
16 |02|bl|de|do|t(\-)|oiv)|n2|n3|n5|n7|n9|p1|v |mmp|mywa|n10|2-|n20|2-3|n30|012|n50|012|5)|n7(0|0|1)|10)|ne( (cim|\/-|
17 |nt|wf|w|vt)|nok(6|l)|nzh|o2im|op(ti|wv)|oran|owg|p800|pan(a|id|t)|pdk|pg(13|\/-|[1-5]|c)|phil|pire|pl ay|uc)
18 |pn-2|po(c|k|rt|se)|prox|psio|pt-\-|qa|-|s|qc(07|12|21|32|60|\-|2-7)|t(\-)|tqek|r380|r600|raks|rim9|ro(ve|zo)|s55\/|sa
19 |ge(ma|mm|ms|ny|va)|sc(01|h\-\-|oo|p|\-)|sdx|/|se(c|\-|0|1)|47|mc(nd|ri)|sgh|-|shar|sie(\-|m)|lak|-|o|el(45|id)|sm(al|ar
20 |b3|ic|c5)|so(ft|ny)|sp(01|h\-\-|v\-\-|v |sy(01|mb)|t2(18|50)|t6(00|10|18)|ta(gt|lk)|tcl(\-)|tdg|\-|tel(i|m)|tim\-\-|t\-\-|mo
21 |to(pl|sh)|ts(70|m\-\-|m3|m5)|tx\-\-9|up(\.b|g|l|a)|utst|v400|v750|veri|vi|rg|te)|vk(40|5(0-3)|\-\-v)|vm40|voda|vulc|vx(52
22 |53|60|61|70|80|81|83|85|88)|w3c(\-|_) |webc|whit|wi(g |nc|nw)|wmlb|wonu|x700|xda(\-|2|g)|yas\-\-|your|zeto|zte\-\-|/
23 substr($useragent,0,4)});
24
25 {
26 header('Location: ./Consejos-Sugerencias/DispMovil/DispositivosMoviles.php');
27
28 }
29 else
30 include("inicio-sitio.php");
31
32 ?>
```

Figura 28: Código implementado para detectar el tipo de acceso

Una vez identificado el dispositivo se utilizó la función `Get_Browser` para descifrar que plataforma utiliza dicho dispositivo, es decir, si se trata de un `Blackberry`, `Nokia`, `Motorola` o `Samsung`, y a partir de esto se brindarán los consejos, sugerencias o recomendaciones correspondientes. En la siguiente imagen se puede observar lo antedicho.

```
1 <?php
2
3 $navegador = get_browser(null, true);
4
5 If ( ($navegador["platform"]== "BlackBerry") {
6 include("BlackBerry.php");
7
8
9 If ( ($navegador["platform"]== "Nokia") {
10 include("Nokia.php");
11
12 If ( ($navegador["platform"]== "Motorola ") {
13 include("Nokia.php");
14
15
16 If ( ($navegador["platform"]== "Samsung") {
17 include("Samsung.php");
18
19
20 include("ConsejosGenerales.php");
21
22 ?>
```

Figura 29: Código implementado para detectar propiedades del tipo de acceso

Toda la información recabada y analizada, para ser ofrecida en FoCoS, fue obtenida de los Sitios oficiales de las marcas de celulares, de libros y de Sitios en internet que ofrecen este tipo de información (Seguridad informática sus implicancias e implementación, **Cristian F. Borghello**; *Como protegernos de los peligros de Internet*, **Gonzalo Álvarez Marañón**)

FoCoS: la Red Social

A partir del análisis realizado sobre las Redes Sociales Open Source en el Capítulo 4 se llegó a la conclusión que la mejor opción sin dudas es Mahara ya que es la que cumple en su totalidad con todos los requisitos que debe tener una herramienta para convertirse en la Red Social FoCoS y poder dar soporte al proyecto de Caperucita.

Mahara fue modificada para adaptarla a lo que hoy es FoCoS. A continuación se presentan las funcionalidades que brinda, pero antes daremos una breve descripción para conocer esta herramienta.

FoCoS es un sistema combinado de un Portafolio y una Red Social. Un portafolio es un sistema donde las personas pueden hacer una relación de "evidencias de aprendizaje permanente" como por ejemplo pueden realizar ensayos, informes, monografías, obras, o cualquier otra cosa que realicen y pueda ser almacenada en formato digital. Los sistemas de redes sociales necesitan una pequeña introducción, simplemente pensemos en Myspace, Facebook o Twitter. Básicamente, estos sistemas suministran un mecanismo para que la gente pueda interactuar con sus amigos y pueda crear sus propias comunidades en línea.

FoCoS se basa en un modelo de aprendizaje centrado en el alumno, donde éste dispone de un espacio online para exponer sus trabajos y crear comunidades virtuales.

Funcionalidades:

- **Portafolio electrónico:** El Portafolio es un método de enseñanza, aprendizaje y evaluación que consiste en la aportación de producciones de diferente índole por parte del estudiante a través de las cuáles se pueden juzgar sus capacidades en el marco de una disciplina o materia de estudio. Estas producciones informan del proceso personal seguido por el estudiante, permitiéndole a él y los demás ver sus esfuerzos y logros, en relación a los objetivos de aprendizaje y criterios de evaluación establecidos previamente. El portafolio como modelo de enseñanza/aprendizaje, se fundamenta en la teoría de que la evaluación marca la forma cómo un estudiante se plantea su aprendizaje. El portafolio del estudiante responde a dos aspectos esenciales del proceso de enseñanza/aprendizaje, implica toda una metodología de trabajo y de estrategias didácticas en la interacción entre docente y discente; y, por otro lado, es un método de evaluación que permite unir y coordinar un conjunto de evidencias para emitir una valoración lo más ajustada a la realidad.

Entonces, para el estudiante un Portafolio sería:

- Muestra de los logros individuales.
- Recopilación y reflexión sobre sus trabajos.
- Compartición de su experiencia educativa y sus trabajos.
- Creación de un plan de estudio en línea y trabajar con alguien que lo guíe.

Para el Docente sería:

- Creación de proyectos con calificación por medio de rúbricas.
- Creación de proyectos en conjunto con otros docentes.
- Revisión de comentarios y trabajos de los estudiantes.
- Exposición y explicación de temas.

En las imágenes que se presentan a continuación podemos observar como FoCoS maneja las diferentes vistas (las vistas son las producciones que un alumno, por ejemplo, puede realizar y que un docente evaluará) y colecciones (conjunto de vistas/producciones relacionadas). Como así también, los permisos que un usuario puede dar a una colección en particular.

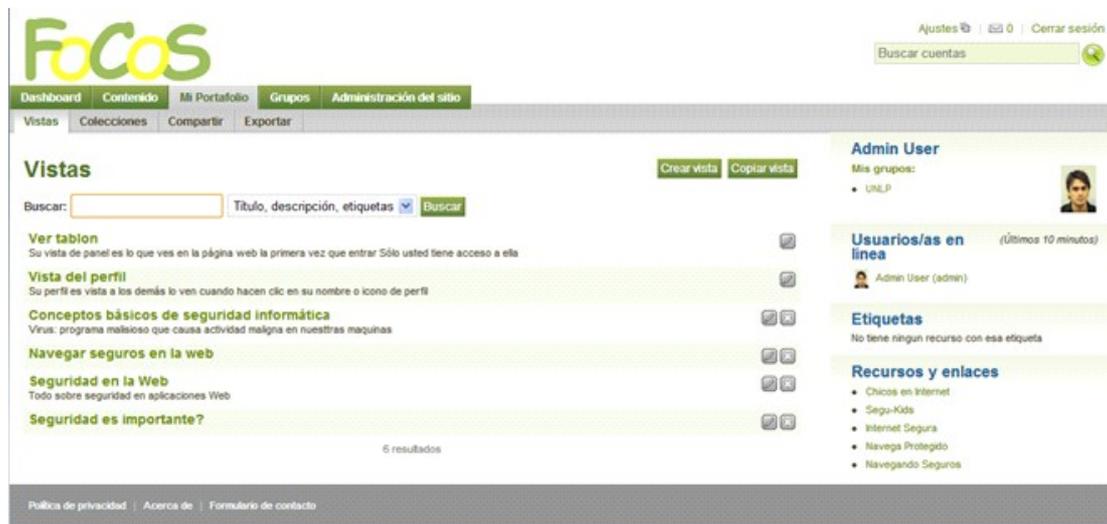


Figura 30: Vistas de un usuario.



Figura 31: Colecciones de vistas

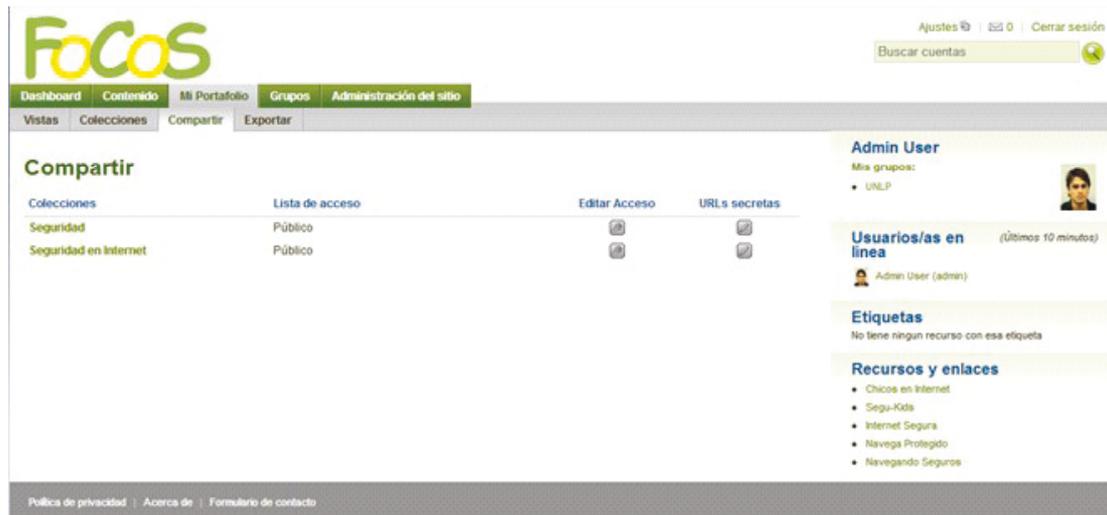


Figura 32: Accesos sobre las colecciones de vistas.

- **Repositorio de archivos:** FoCoS incluye un repositorio de archivos que permite a los usuarios:
 - Crear carpetas y subcarpetas estructuras.
 - Subir varios archivos de forma rápida y eficiente.
 - Dar a cada archivo un nombre y una descripción.
 - Gestionar el espacio de memoria para cada archivo.

En la siguiente imagen se presenta la sección donde podemos gestionar/administrar los ficheros que subimos.

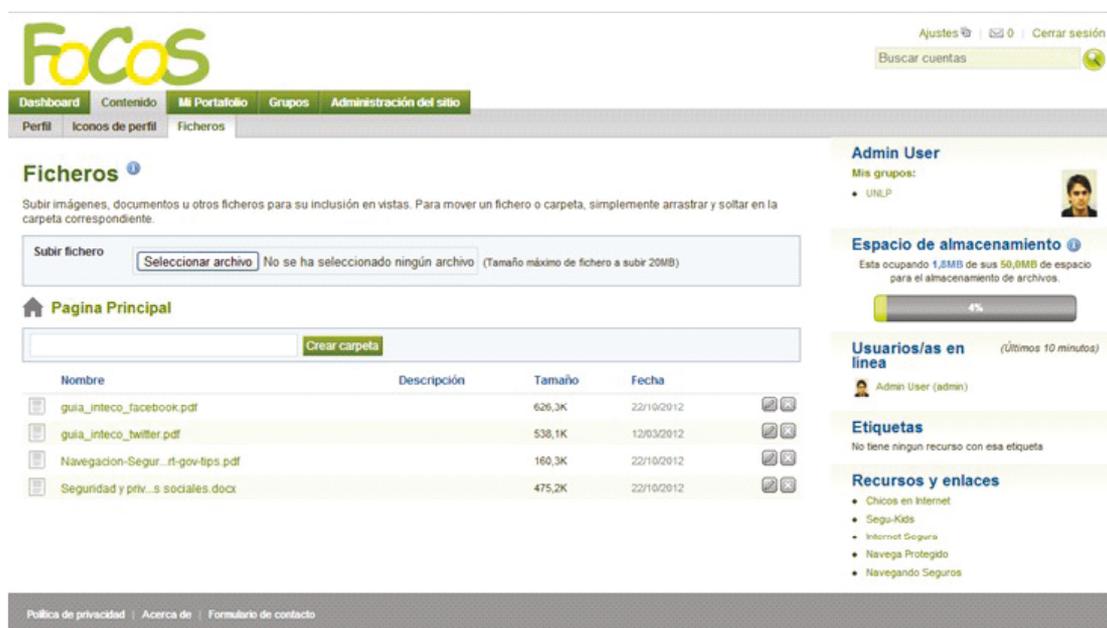


Figura 33: Gestión de ficheros.

- **Muro:** FoCoS cuenta con un muro en el cual los usuarios pueden compartir información que verán sus amigos, podrán mostrar sus fotos, las páginas que le gustan, videos, también podrán escribir en él por ejemplo alguna idea que tienen en mente o brindar algún consejo o

comentarios sobre temas de seguridad (o cualquier tema) a todos sus amigos.

En la imagen presente a continuación podemos observar como es el muro en FoCoS.

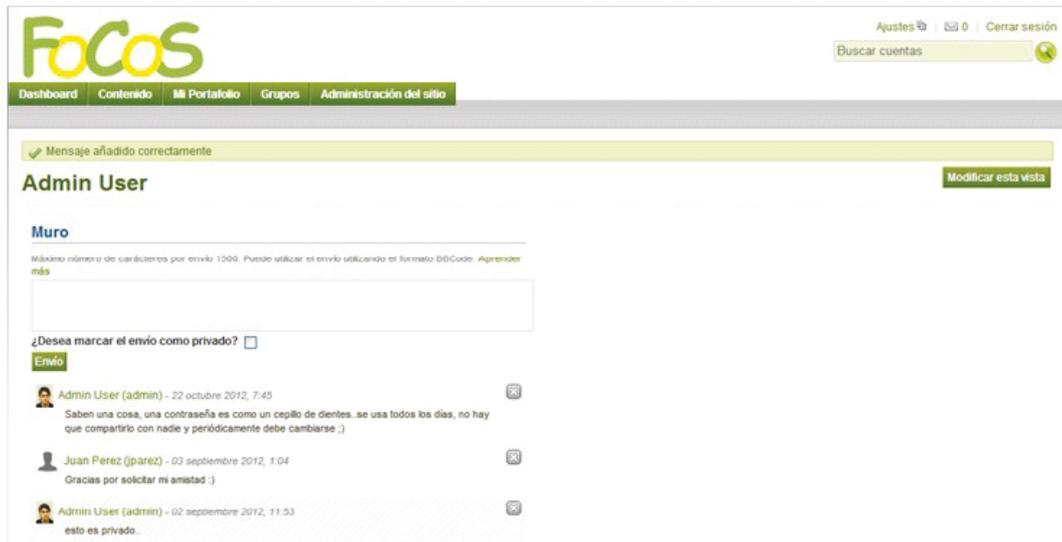


Figura 34: Muro

- **Red Social:** FoCoS proporciona la instalación de una Red Social donde los usuarios pueden crear y mantener una lista de amigos dentro del sistema. Se pueden crear grupos de amistades para compartir temáticas en común o para discutir temas puntuales.

En la siguiente imagen podemos observar lo antedicho.

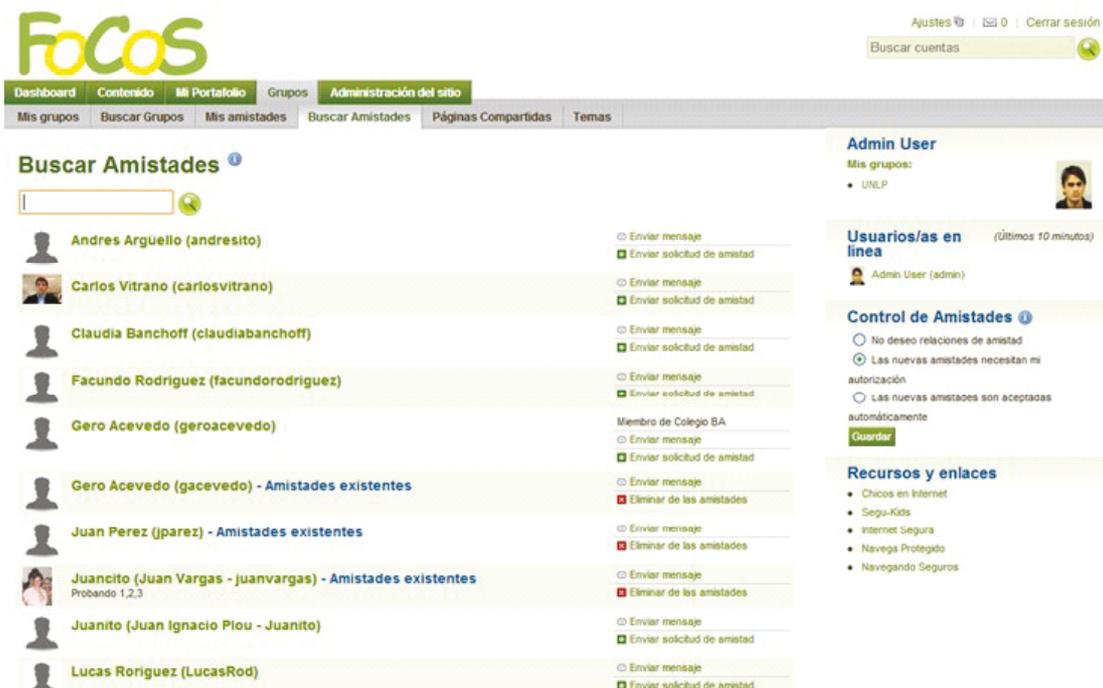


Figura 35: Amistades

- **Información de perfil:** Dentro de FoCoS los usuarios pueden compartir información personal a través de una variedad de campos opcionales que incluyen:
 - Nombre.
 - ID de estudiante.
 - Dirección postal.
 - Números de teléfono.
 - Skype, MSN, Yahoo y Jabber.

En la siguiente imagen podemos observar lo antedicho.

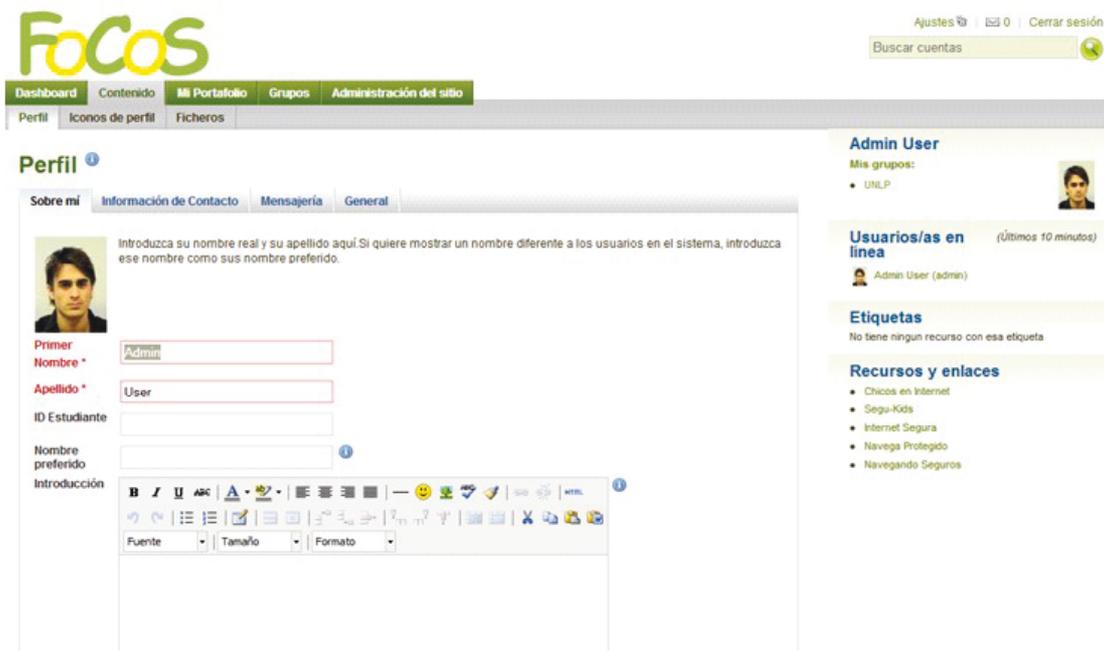


Figura 36: Perfil de usuario en FoCoS

- **Instituciones:** En FoCoS es posible crear instituciones. Una institución sería como un grupo gigante al cual se pueden asociar varios usuarios y grupos de usuarios y compartir temas en común. Estas instituciones pueden estar administradas por usuarios con privilegios para poder dar de baja o alta a otros usuarios pertenecientes a la misma, o para bloquear algún contenido/comentario indebido. Estos usuarios serían los administradores de institución. Por ejemplo, una institución puede ser un colegio, en donde sus usuarios serían todos los alumnos y los docentes serían los administradores de dicha institución.

En la imagen que se presenta a continuación podemos observar que un usuario con perfil de administrador de institución posee en su menú una solapa más que corresponde a la administración de las instituciones, “Administración de la Institución”.



Figura 37: Administración de la Institución

Y en la siguiente imagen podemos observar el panel de administración de un administrador de institución.

The screenshot shows the FoCoS administration interface. At the top left is the FoCoS logo. To the right, there are links for 'Ajustes', 'Ed 0', and 'Cerrar sesión', along with a search bar labeled 'Buscar cuentas'. Below the logo, there are navigation tabs: 'Gestionar usuarios', 'Instituciones', and 'Volver al sitio'. Underneath, there are sub-tabs: 'Buscar cuenta', 'Cuentas suspendidas', 'Cuentas nuevas', and 'Cuentas añadidas por CSV'. The main section is titled 'Buscar cuenta' and includes instructions: 'Puede buscar cuentas por las iniciales de su nombre o apellido, tecleando el nombre o su dirección de c/e en el cuadro de texto para la búsqueda.' Below this, there are dropdown menus for 'Nombre' and 'Apellidos', both set to 'Todo', with an alphabet 'A B C D E F G H I J K L M N N Ñ O P Q R S T U V W X Y Z' for selection. A 'Buscar' button is present. The results section, titled 'Resultados', displays a table with the following data:

Nombre	Apellidos	Cuenta	Correo electrónico (c/e)	Institución
Facundo	Rodriguez	facundorodriguez	iseka.87@gmail.com	FoCoS
Gero	Acevedo	geroacevedo	geronimo.acevedo@ar.ey.com	Colegio BA
Juan	Vargas	juanvargas	juanp_rey@hotmail.com	FoCoS
Marcela	Lopez	marce	marce@hotmail.com	FoCoS
Juan	cuervo	juancuervo	juanpi.cuervo@hotmail.com	Colegio BA
pablo	neruda	pablo	pablo@gmail.com	Colegio BA

Figura 38: Panel de administración de instituciones

- **Administración:** Los administradores pueden personalizar FoCoS a través de una serie de opciones de configuración que incluyen:
 - Paquetes de idiomas y temas.
 - Período de sesiones.
 - Métodos de autenticación.
 - Configuración de instituciones.
 - Editor de páginas.
 - Editor de menú principal.
 - Gestión de usuarios.
 - Administración de plugins
 - Gestión de grupos.
 - Configuración de la seguridad.
 - Entre otras.

En la imagen presente a continuación podemos observar los parámetros de configuración de FoCoS, es decir, todas aquellas funcionalidades que un usuario con perfil de administrador puede configurar.

Administración

Registre su sitio en Mahara

Puede optar por registrar su sitio con Mahara mahara.org, nos ayudan a construir una imagen de la base de instalación de Mahara en todo el mundo. El registro se retira este aviso.

Usted puede registrar su sitio, y vista previa de la información que se enviará en el [Página Web de Registro](#).

FoCoS: Información del Sitio

[Ver estadísticas completas del sitio](#)

Web instalada: 22 octubre 2011

Tamaño de base de datos: 5MB

Version de Mahara: 1.4.0

Cron: Cron no se ejecuta.

Ver la [guía de instalación](#) para obtener instrucciones sobre la forma de configurar.

Cerrar sitio

Cerrar el sitio a todo el mundo excepto a los administradores. Esto puede ser útil para prepararse para una actualización de la base de datos. Sólo los administradores podrán entrar hasta que se reabra el sitio, o se complete con éxito la actualización.

Cerrar

Ajustes globales

- **Opciones del sitio** - Ajustar la configuración básica del sitio como el nombre, paquete de lenguaje, tema
- **Editar las páginas del sitio** - Editar el contenido de varias páginas en este sitio
- **Menús** - Administrar los enlaces y archivos dentro de los enlaces y recursos y de los menús pie de página
- **Red** - Configuración de la red 'Mahara'
- **Páginas del sitio** - Gestionar páginas y Plantillas de página para todo el sitio
- **Archivos del sitio** - Gestión de archivos que pueden ser colocados en las vistas del sitio o en el menú de recursos y enlaces

Gestionar usuarios

- **Buscar cuenta** - Buscar en todas las cuentas para concederles responsabilidades de administración
- **Cuentas suspendidas** - Suspendir o reactivar cuentas de este sitio
- **Plantilla del Sitio** - Asignar permisos a Plantilla
- **Administradores del Sitio** - Conceder derechos de acceso a la administración del sitio
- **Gestionar avisos** - Visión general de como se reciben los avisos en el perfil de administración
- **Cuentas nuevas** - Crear una cuenta nueva

Administrar grupos

- **Administrar grupos** - Los administradores del grupo Nombrar y eliminar los grupos
- **Categorías de Grupo** - Agregar y editar las categorías de grupos

Instituciones

- **Gestionar Instituciones** - Permite crear o modificar instituciones
- **Cuentas activas de la Institución** - Inscribir cuentas en instituciones
- **Plantilla de la Institución** - Asignar permisos a Plantilla
- **Cuentas de Administración** - Conceder privilegios de administración
- **Vistas de la Institución** - Gestión de vistas y plantillas de una institución
- **Archivos de la Institución** - Gestión de los archivos disponibles en las vistas

Extensiones

- **Administrar Plugins** - Instalar y configurar Plugins
- **Filtros de HTML** - Activar los nuevos filtros para la codificación pura en HTML

Figura 39: Panel de administración

Tareas realizadas para poner en marcha a la Red Social FoCoS

Para que FoCoS funcione correctamente fue necesario realizar las siguientes tareas:

- **Instalación de un Servidor Apache:** la instalación de un Servidor fue necesaria para montar todos los servicios que se describen a continuación.
- **Instalación de una base de datos MySQL:** FoCoS requiere de una base de datos para su funcionamiento, en la misma almacena todos los datos del Sitio.
- **Instalación del intérprete para el lenguaje PHP:** ya que FoCoS está desarrollado en PHP fue necesario instalar un intérprete para dicho lenguaje.
- **Instalación de un servicio de Correo:** FoCoS requiere de un Servidor de correo para poder enviar correos electrónicos a sus usuarios cada vez que realizan alguna actividad importante (cambio en algún parámetro de seguridad) o cuando reciben un mensaje. Adicionalmente, para poder crearse una cuenta, un usuario debe ingresar su cuenta de correo, y FoCoS envía a dicha cuenta un link para poder finalizar el proceso de registración. Sin un Servidor de correo no era posible la registración de los usuarios al Sitio, salvo que el administrador lo realice.

Seguridad en FoCoS

Ya que FoCoS será utilizado como medio para impartir conocimientos y concientizar sobre la seguridad en Internet, resultaría absurdo si el mismo no contara con las reglas básicas de seguridad y no proporcionara al usuario un medio seguro de comunicación.

Por esta razón, se realizó una evaluación del Nivel de Seguridad imperante en FoCoS a través de la ejecución de Pruebas de Intrusión (Ethical Hacking) con el propósito de identificar la existencia de debilidades y/o vulnerabilidades que podrían permitir el acceso no autorizado a los recursos del Sitio. Y a partir de los resultados obtenidos, efectuar las remediaciones necesarias respecto de las acciones que podrían mitigar los riesgos asociados a las debilidades y/o vulnerabilidades identificadas.

A continuación se describen algunas de las técnicas evaluadas manualmente con el objeto de lograr la identificación de vulnerabilidades. Dichas técnicas fueron tomadas del Proyecto OWASP (la comunidad libre y abierta sobre seguridad en aplicaciones Ref[21]), el cual define los diez riesgos más críticos sobre seguridad en aplicaciones:

1. **Inyección:** Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.
2. **Secuencia de comandos en sitios cruzados (XSS):** Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.
3. **Pérdida de Autenticación y Gestión de Sesiones:** Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, llaves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.
4. **Referencia Directa Insegura a Objetos:** Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder a datos no autorizados.
5. **Falsificación de Peticiones en Sitios Cruzados (CSRF):** Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificada, incluyendo la sesión del usuario y cualquier otra información de autenticación, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima para generar

pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la víctima.

6. **Defectuosa configuración de seguridad:** Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.
7. **Almacenamiento Criptográfico Inseguro:** Muchas aplicaciones web no protegen adecuadamente los datos sensibles, tales como tarjetas de crédito, NSSs, y credenciales de autenticación con mecanismos de cifrado o hashing. Atacantes pueden modificar o robar tales datos protegidos inadecuadamente para conducir robos de identidad, fraudes de tarjeta de crédito u otros crímenes.
8. **Falla de Restricción de Acceso a URL:** Muchas aplicaciones web verifican los privilegios de acceso a URLs antes de generar enlaces o botones protegidos. Sin embargo, las aplicaciones necesitan realizar controles similares cada vez que estas páginas son accedidas, o los atacantes podrán falsificar URLs para acceder a estas páginas igualmente.
9. **Protección Insuficiente en la capa de Transporte:** Las aplicaciones frecuentemente fallan al autenticar, cifrar, y proteger la confidencialidad e integridad de tráfico de red sensible. Cuando esto ocurre, es debido a la utilización de algoritmos débiles, certificados expirados, inválidos, o sencillamente no utilizados correctamente.
10. **Redirecciones y Reenvíos no validados:** Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

Hallazgos y Remediaciones

A continuación se resumen los principales hallazgos que resultaron del desarrollo de las pruebas de intrusión realizadas y remediaciones que deberían aplicarse con el objetivo de mejorar la seguridad de FoCoS.

Para la detección de las vulnerabilidades se realizaron las pruebas manuales mencionadas anteriormente y se corrieron herramientas específicas que detectan posibles debilidades en el Sitio. Las herramientas utilizadas fueron Acunetix Web Vulnerability y Nessus. A continuación se muestra una captura de pantalla de los resultados arrojados por ambas.

Resultados alcanzados por Acunetix

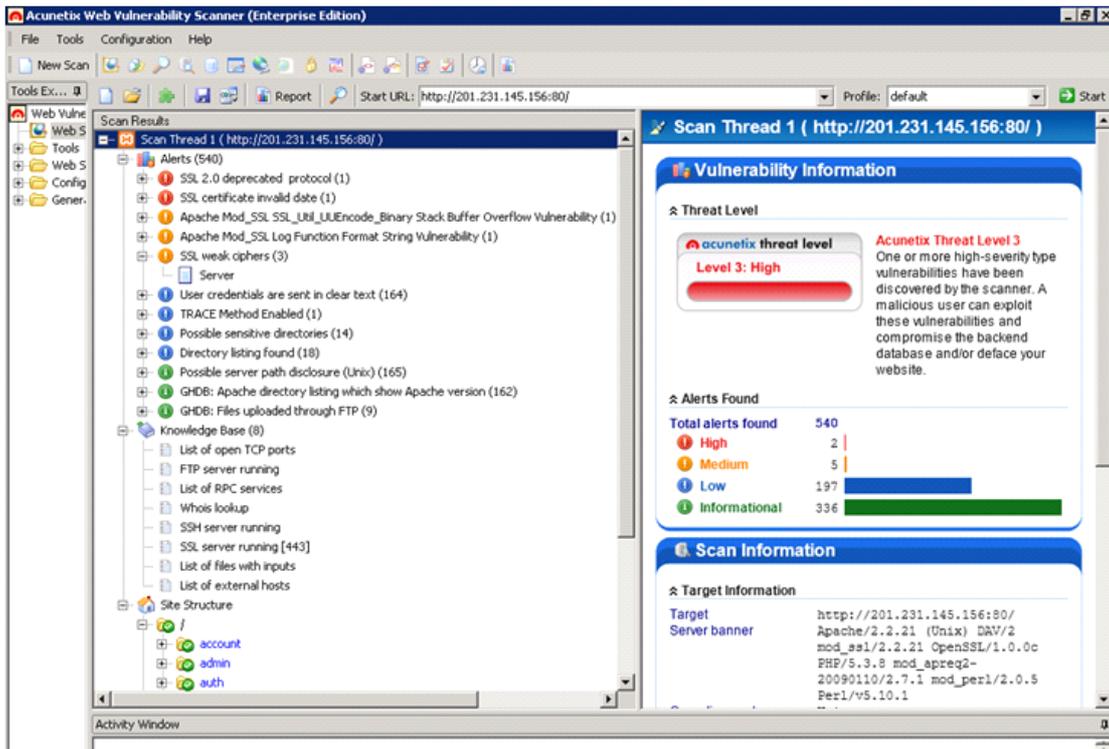


Figura 40: Acunetix – Resultados del escaneo

Resultados alcanzados por Nessus

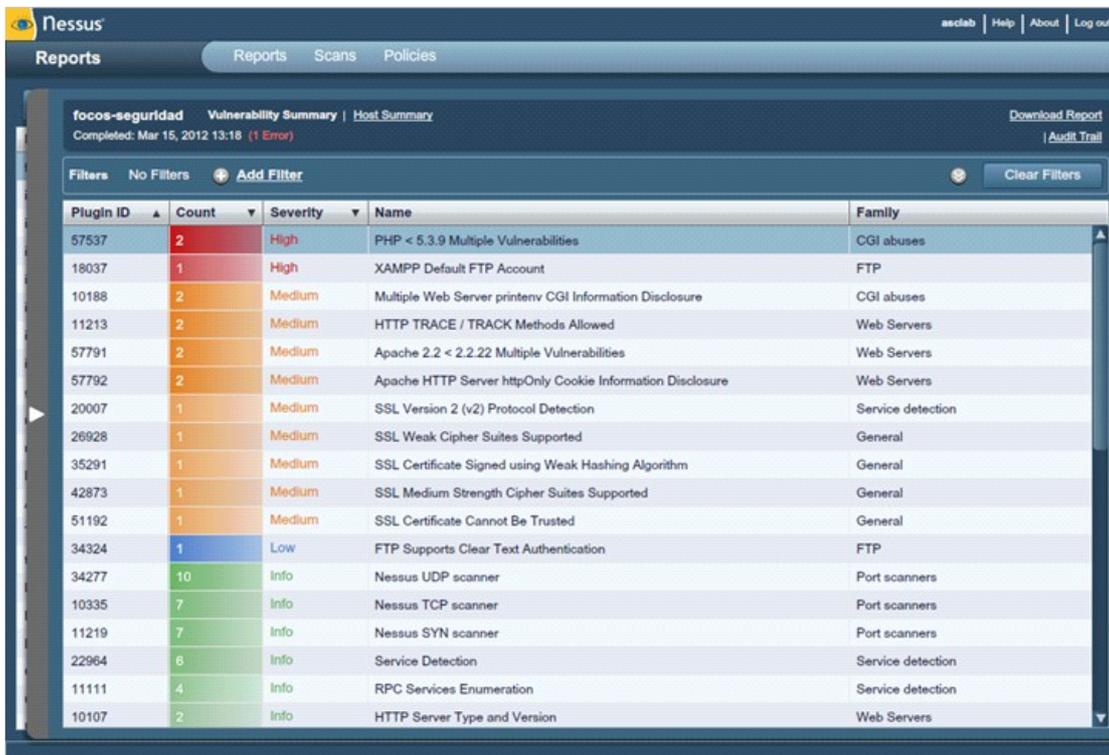


Figura 41: Nessus – Resultados del escaneo

Descripción de las debilidades halladas por ambas herramientas:

- **SSL certificate invalid date:** El certificado SSL que utiliza el Sitio está caducado o no es válido. Este hecho provoca que los usuarios desconfíen de la autenticidad del Sitio y anula la validez de la conexión SSL permitiendo un ataque del tipo “Man in the Middle”.
- **SSL 2.0 deprecated protocol:** El Servidor cifra el tráfico utilizando un protocolo muy antiguo en desuso. Esta situación podría permitir a un atacante interceptar la comunicación entre clientes y el Servidor, mediante ataques de tipo MiM (Man in the Middle) y vulnerar la encriptación, logrando de esta forma acceso a información confidencial.
- **Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability:** El módulo de autenticación mod_ssl del Servidor HTTP Apache es vulnerable a un desbordamiento de búfer causado por una vulnerabilidad en la función ssl_util_uencode_binary. Un atacante podría explotar esta vulnerabilidad para provocar un desbordamiento de búfer y posiblemente causar una denegación de servicio o ejecutar código arbitrario en el sistema.
- **User credentials are sent in clear text:** Las credenciales de usuario no están siendo cifradas cuando se transmiten.
- **TRACE Method Enabled:** el Servidor Web posee habilitado el método TRACE, el cual podría permitir ataques de cross-site tracing. Esta situación posibilita a un atacante a obtener información de los usuarios, tales como cookies e información de autenticación al Sitio.
- **Directory listing found:** El Servidor web está configurado para mostrar la lista de archivo contenidos en los directorios. Esto no es recomendable ya que el listado de directorios brinda a un posible atacante mayores conocimientos sobre la estructura del Sitio. Adicionalmente, archivos de configuración o datos confidenciales pueden ser expuestos.

La mayor parte de las vulnerabilidades encontradas impactan directamente sobre el Servidor donde se encuentra alojado FoCoS, por lo que está fuera del alcance de este trabajo. En particular los siguientes:

- SSL certificate invalid date
- User credentials are sent in clear text

Se resolvería instalando un certificado digital provisto por una autoridad de certificación de confianza, para la comunidad que usará FoCoS.

FoCoS en el Proyecto Caperucita y el Lobo en el Ciberespacio

El proyecto de Caperucita y el Lobo en el Ciberespacio es un proyecto de la Facultad de Informática de la Universidad Nacional de la Plata (UNLP) que trata sobre la implementación de talleres de seguridad informática dirigida a jóvenes, padres, docentes y personas de la tercera edad. El proyecto se orienta principalmente a niños/jóvenes y adultos de edad avanzada, por considerar ambos grupos como los más vulnerables a acciones maliciosas llevadas por terceros en la Red. En el caso de los niños/jóvenes, se propone la realización de talleres en escuelas de la zona. A su vez se organizarán encuentros con padres y docentes. En cuanto al sector de la tercera edad, se propone incluir en el convenio ya existente con U-PAMI, un módulo de concientización que prevenga sobre malas prácticas que deriven en ataques que puedan ser aprovechados por ciberdelincuentes. El objetivo de estas actividades es enseñar a disfrutar de Internet de una forma segura y responsable.

El nombre del Proyecto viene del cuento de “Caperucita roja y el lobo” que es conocido por todos. En él, un lobo malintencionado se vale de artimañas y engaños para lograr su cometido. Sus intenciones, eran comerse a la abuelita de Caperucita, y a la misma Caperucita. Pero, ¿qué tiene que ver esto con los peligros de Internet? Hoy día, el ciberespacio está colmado de personas malintencionadas que de la misma manera que el lobo, se valen de engaños combinados con herramientas tecnológicas para engañar a los internautas (millones de Caperucitas navegando por la red) y de esa manera poder robarles información confidencial. La motivación de este proyecto es concientizar a las personas sobre los riesgos que existen, de manera que pueda disfrutar su travesía por la red practicando un uso más consciente y seguro de sus servicios para evitar caer en las manos de algún lobo.

Entonces, los aportes que realizaría FoCoS al proyecto serian los siguientes:

- Una fuente de conocimientos para que los jóvenes, padres, docentes y personas de la tercera edad puedan informarse sobre los peligros que hay en Internet y concientizarse sobre las formas de protección y prevención.
- Una herramienta para que todos podamos comunicarnos, intercambiar ideas, compartir experiencias, informarnos, aprender, etc. Por ejemplo, cada vez que se visite un colegio para dar una charla sobre Seguridad en Internet, se podrá crear una institución en FoCoS que represente a dicho colegio y que esté administrada por el docente a cargo. Así, los alumnos podrán seguir aprendiendo bajo la supervisión de un docente.
- Un sitio en el cual la comunidad pueda conocer las inseguridades o peligros que acechan a todos aquellos dispositivos o equipos que utilizamos para acceder a internet y comunicarnos con los demás.



Caperucita y el Lobo se iluminan con FoCoS

Los Guardianes del Ciberespacio necesitaban de una luz que los guíe en la oscuridad para encontrar a Caperucita y salvarla del Lobo maligno... FoCoS se ofreció a dar luz... y fue de esta manera como "Caperucita y el Lobo en el Ciberespacio" conocen a "FoCoS"

¿Por qué el proyecto se llama "Caperucita y el lobo en el ciberespacio"?

Sin duda el cuento de Caperucita roja y el lobo es conocido por todos. En él, un lobo malintencionado se vale de artimañas y engaños para lograr su cometido. Sus intenciones, eran comerse a la abuelita de Caperucita, y a la misma Caperucita. Pero, ¿qué tiene que ver esto con los peligros de Internet? Hoy día, el ciberespacio está colmado de personas malintencionadas que de la misma manera que el lobo, se valen de engaños combinados con herramientas tecnológicas para engañar a los internautas (millones de Caperucitas navegando por la red) y de esa manera poder robarles información confidencial. La motivación de este proyecto es concientizar a las personas sobre los riesgos que existen, de manera que pueda disfrutar su travesía por la red practicando un uso más consciente y seguro de sus servicios para evitar caer en las manos de algún lobo.

El proyecto trata sobre la implementación de talleres de seguridad informática dirigida a jóvenes, padres, docentes y personas de la tercera edad. El proyecto se orienta principalmente a niños/jóvenes y adultos de edad avanzada, por considerar ambos grupos como los más vulnerables a acciones maliciosas llevadas por terceros en la Red. En el caso de los niños/jóvenes, se propone la realización de talleres en escuelas de la zona. A su vez se organizarán encuentros con padres y docentes. En cuanto al sector de la tercera edad, se propone incluir en el convenio ya existente con U-PAMI, un módulo de concientización que prevenga sobre malas prácticas que deriven en ataques que puedan ser aprovechado por ciberdelinquentes. El objetivo de estas actividades es enseñar a disfrutar de Internet de una forma segura y responsable.

Responsables del Proyecto y equipo de trabajo

Ideas y realización

- Lia Molinari
- Paula Venosa
- Nicolás Macía
- Raúl Benencia

Abrir sesión

Cuenta: *

Introduzca el nombre de identificación de su cuenta

Contraseña: *

Introduzca la contraseña que utilizó al abrir su cuenta

Recursos y enlaces

- Charla a Docentes
- Charla a Chicos
- Charla a Padres y Docentes
- Charla a UPAMI
- Proteja sus datos
- Proteja a sus hijos
- Atrapado en la red
- Segu-Kids
- Chicos en Internet
- Internet Segura Para Todos
- Internet Segura
- Navega Protegido
- Navegando Seguros

Figura 42: FoCoS y Caperucita y el Lobo en el Ciberespacio

Esta propuesta fue presentada en el Congreso de Tecnología en Educación y Educación en Tecnología (Ref[22]) y aceptada para su publicación.

Capítulo 6

Conclusiones

Conclusión

Los objetivos planteados al comienzo del trabajo se alcanzaron al lograr la implementación de un entorno de difusión de contenidos sobre Privacidad y Seguridad de la Información, con orientación a los distintos tipos de usuarios. Integrando al mismo, una red social de manera tal de generar una comunidad alrededor de la temática, incorporando el manejo de roles, enfocado al proyecto “Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos”. Adicionalmente, se integró al mismo un módulo que permite reconocer desde donde accede el usuario para poder adecuar los consejos y recomendaciones al tipo de acceso.

Para alcanzar dicho objetivos fue necesario realizar las siguientes tareas:

- Analizar sitios web en español orientados a la Seguridad y Privacidad en Internet focalizados en la comunidad en general: niños, jóvenes y adultos. Y evaluar los contenidos, la población a la cual están dirigidos y los servicios brindados por dichos sitios.
- Analizar herramientas para la detección del tipo de acceso y los distintos mecanismos para adaptar y adecuar las recomendaciones, sugerencias o consejos a los mismos.
- Investigar, analizar y probar herramientas Open Source disponibles para implementar redes sociales. Los análisis se realizaron teniendo en cuenta la estructura, el mantenimiento (si es que lo tiene), las funcionalidades y contenidos posibles, la seguridad, la facilidad de adecuación, etc.

Próximos Pasos

Completar la integración con el proyecto de “Caperucita fue víctima de la Ingeniería Social: Concientización en seguridad informática para todos”, para dar soporte tanto en lo referido a la documentación como a la plataforma de comunicación.

Al momento de cerrar este trabajo el Gobierno Nacional lanzó el portal “Con vos en la web [Ref25]” con la finalidad crear un espacio para la comunicación, el asesoramiento y la participación de niños y jóvenes en temas vinculados con las nuevas tecnologías y la protección de los datos personales. Por cuestiones de tiempo el mismo no fue incluido en este informe, pero quedaría como trabajo futuro el análisis de dicho sitio para sumar al relevamiento ya realizado en el capítulo 2.

Referencias

- Ref1** Sitio con el mapa actualizado de las redes sociales en el mundo. <http://www.whatsnew.com/2011/03/08/mapa-actualizado-de-las-redes-sociales-en-el-mundo-2/>
- Ref2** <http://www.hoytecnologia.com/noticias/estudio-advierte-riesgos-cyberbullying/76380> Noticias sobre el cyberbullying
- Ref3** Sitio con noticias actuales sobre la seguridad en internet. <http://radio.uchile.cl/noticias/88812/>
- Ref4** Sitio con noticias y artículos sobre el Grooming. <http://www.internet-grooming.net/noticias.html>
- Ref5** <http://www.impre.com/laopinion/noticias/primerapagina/2010/4/21/cyberbullying-es-el-rival-de-mo-184393-1.html#commentsBlock> Noticias sobre el cyberbullying.
- Ref6** Redes Sociales Open Source. <http://www.vivalogo.com/vl-resources/open-source-social-networking-software.htm>
- Ref7** Sitio Segu-Info. <http://www.segu-info.com.ar/menores/>
- Ref8** Sitio Segu-Kids. <http://www.segu-kids.org/>
- Ref9** Sitio Chicos-Internet. <http://www.chicoseninternet.com.ar/>
- Ref10** Sitio Internet Segura Para Todos. <http://www.enlaces.cl/index.php?t=44>
- Ref11** Sitio Chicos en internet. <http://www.chicos.net.ar/internetsegura/>
- Ref12** Sitio navegando Protegido. <http://www.navegaprotegido.org/>
- Ref13** Sitio Internet Segura. <http://www.internetsegura.net>
- Ref14** Sitio Navegando Seguros. <http://www.navegandoseguros.org/>
- Ref15** Sitio de PHP. <http://php.net/manual/es/function.get-browser.php>
- Ref16** <http://browsers.garykeith.com/downloads.asp>
- Ref17** <http://www.quirksmode.org/js/detect.html>
- Ref18** Sitio Detect Mobile Browser. <http://detectmobilebrowsers.com/>
- Ref19** Sitio JQuery. <http://jquery.com/>
- Ref20** Sitio de Firefox. <https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/>
- Ref21** Sitio OWASP. <https://www.owasp.org>
- Ref22** Gerónimo Acevedo, Paula Venosa, Claudia Banchoff. Redes Sociales Open Source: una comunidad para Caperucita. TEyET 2012. Junio 2012 - ISBN 978-987-28186-0-9. <http://teyet2012.et.unnoba.edu.ar/>
- Ref23** Sitio de Microsoft. <http://www.microsoft.com/es-xl/security/default.aspx>
- Ref24** Sitio de Segu-Info. <http://www.segu-info.com.ar/>
- Ref25** Sitio Con vos en la Web. <http://www.convosenlaweb.gob.ar>

Bibliografía

- <http://www.ciberbullying.net/> Sitio destinado a combatir el cyberbullying.
- <http://www.pedofilia-no.org/> Sitio destinado a combatir la pedofilia.
- <http://elgg.org/> Página oficial de la herramienta Open Source Elgg.
- <http://www.barnraiser.org/> Página oficial de la herramienta Open Source Barnraiser.
- <http://www.socialengine.net/> Página oficial de la herramienta Open Source Socialengine.
- <http://jamss.sourceforge.net> Página oficial de la herramienta Open Source Jamss.
- **Gonzalo Álvarez Marañón.** Como protegernos de los peligros de Internet. *Información de seguridad para el internauta domestico, Editorial Catarata ISBN: 978-84-8319-449-2*
- **Cristian F. Borghello.** Seguridad informática: sus implicancias e implementación.
- **Francesc Perendreu i Mata.** Juego y conducta responsable en adolescentes. *Jóvenes sus conductas y sus consecuencias en Internet.*
- **Sacha Fuentes Gatiús.** Defiende tu PC. *Guía de seguridad para ordenadores personales 2005*
- **Eugenio Siccardi.** Guía de uso del correo electrónico. *Pautas de comportamiento para una comunicación electrónica grata y productiva. 1ª edición - Julio 2002 ISBN 987-43-4880-1*
- **Gonzalo Asensio.** Seguridad en Internet. *Una guía práctica y eficaz para proteger su PC con software gratuito. Ediciones Nowtilus, 2006 -320 páginas*
- **Pablo Santiago.** Alicia en el lado oscuro. *La pedofilia desde la antigua Grecia hasta la era internet.*
- **Juan José De - Haro Ollé.** Redes Sociales para la Educación. *Manual imprescindible. Anaya Multimedia, 06/09/2010 - 432 páginas*
- **Ana Martos Rubio.** Redes Sociales. *Informática para Mayores. 128 páginas Noviembre 2006.*
- www.php.net Página oficial de php.
- <http://php.net/manual/es/function.get-browser.php> Función estándar get_browser.
- <http://www.apachefriends.org/es/xampp.html> Entorno XAMPP, Apache con MySQL, PHP y Perl.

- <http://www.w3c.es/> Página oficial de la w3c.
- <http://www.elgg.org/download.php> Herramienta Open Source Elgg.