

Seguridad en las páginas web

Clave del proyecto: CIN2015A30089

Colegio Anglo Mexicano de Coyoacán

Autores:

Cuéllar Cruz Daniela Itzel

Minquini Merino Sabrina

Minquini Merino Marianne

Asesora:

Salvador Sierra Guiomar Ivonne

Área de conocimiento: Ciencias Sociales

Disciplina: Sociología

Tipo de investigación: Documental

México D. F. a 05 de diciembre del 2014

Resumen

Una página web es un documento electrónico que contiene información, se encuentra en un servidor y se accesa por navegadores, por lo que existe el riesgo de encontrar contenido malicioso y es una amenaza para los usuarios. Gracias a esto existen botones de seguridad con los cuales se puede identificar si una página es de dudosa procedencia. Se realizó una encuesta en el Colegio Anglo Mexicano de Coyoacán (sección preparatoria). Con las preguntas evaluadas en las encuestas se pudo verificar que al no conocer los botones de seguridad, los alumnos pueden ser vulnerables a cualquier tipo de amenaza que se presente en las páginas web.

A web page is an electronic document that contains information , is on a server and is accessed by browsers, so there is the risk of finding malicious content and is a threat to users . Thanks to this there are safety buttons with which you can identify if a page has a dubious origin . A survey in the Mexican Anglo College of Coyoacán (preparatory department) was performed . With the answers it was verified that not knowing the safety buttons, students may be vulnerable to any type of threat that is present in the web pages.

Introducción

Planteamiento del problema

¿Qué riesgos enfrentan los alumnos de preparatoria cuando acceden a páginas web sin tomar en cuenta las advertencias de los botones de alerta?

Hipotesis

Las páginas web proponen botones de alerta y seguridad que permiten acceder a la leyenda que dice “es posible que la página web que intentas visitar contenga información riesgosa” o en algunos de los casos hay botones que significan que el “contenido es potencialmente peligroso” de esta manera al insistir en abrir, automáticamente se genera un código malicioso que infecta el ordenador, sin embargo debido a que esta información no menciona el riesgo de estos botones para acceder a páginas de información los alumnos pueden estar en situaciones de riesgo y visitar sitios que pongan en peligro su integridad.

El grado de inseguridad que puede presentar un sitio web para los usuarios puede implicar vulnerabilidad y poca seguridad para estos y así los intrusos y desconocidos aprovecharse, los diferentes tipos de problemas, peligros y amenazas a la seguridad de un sitio web o la adicción a internet puede guiarnos a páginas de poco uso lúdico¹

Una página web se define como un documento electrónico el cual contiene información textual, visual y/o sonora que se encuentra alojado en un servidor y puede ser accesible mediante el uso de navegadores. Una página web forma parte de una colección de otras páginas webs dando lugar al denominado sitio web el cual se encuentra identificado bajo el nombre de un dominio.

La creación y desarrollo de una página web se realiza bajo un lenguaje de programación capaz de ser interpretados por los navegadores, lenguajes como el HTML, PHP, ASP, JSP, entre otros ejemplos.

Al inicio de la era de internet, sobre los años 90, era necesario el conocimiento de algún lenguaje de programación para el desarrollo de una web, siendo una tarea encomendada a personas con altos conocimientos informáticos, hoy en día contamos

¹ El ICANN, órgano de gestión administrativa que no puede impedir el acceso a internet ni legal técnicamente, “autoridad central”

con software especializado capaz de trabajar como un editor de texto, estilo Word, que transforman toda la información insertada en un lenguaje de programación capaz de ser interpretado por los navegadores, de esta forma se liberalizó y se globalizó la creación de páginas webs con apenas unos escasos conocimientos informáticos, programas como Dreamweaver, Amaya, Sharepoint Designer o Mozilla Composer son entre otros los denominados WYSIWYG (acrónimo del inglés " lo que ves es lo que obtienes") capaces de crear complejas páginas webs con el entorno de un simple editor de texto².

Navegador o buscador conocido en Ingles como web browser.

- Un Explorador Web o Navegador es un programa que permite visualizar páginas web en la red además de acceder a otros recursos como documentos almacenados y guardar información.
- El Navegador se comunica con el servidor a través del protocolo http y le pide el archivo solicitado en código HTML, después lo interpreta y muestra en pantalla para el usuario.
- Un navegador también nos permite almacenar información o acceder a diferentes tipos de documentos en el disco duro, acceder a redes privadas y crear marcadores (bookmarks).
- El acceso a otras páginas web a través de los hiperenlaces (hipervínculos o enlaces) se llama navegación, término del que deriva el nombre de navegador, aunque una minoría prefieren llamarlo hojeador que sería la traducción literal de la palabra browser.
- Los más populares navegadores vienen incorporados a sus sistema operativo como es el caso de Internet Explorer (Windows), Mozilla, Firefox, Safari (Mac OS), Opera y Google Chrome.

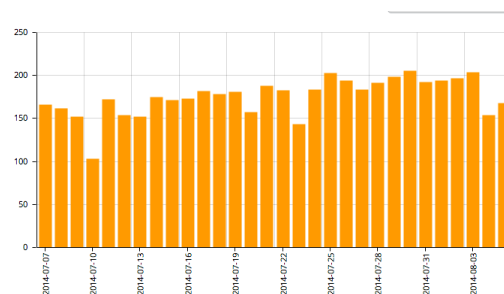
Clasificación de las páginas webs:

Las webs estáticas son aquellas cuya información no varía en un tiempo a medio o a corto plazo, también se las reconoce puesto que no interactúan con el usuario o

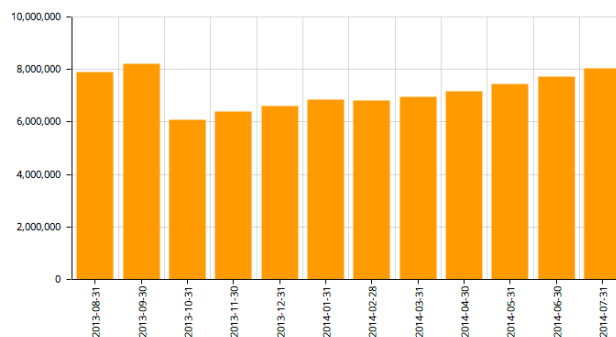
² Comité federal de coordinación de investigación sobre internet.

navegante, su lenguaje de programación está basado en HTML y están compuestas principalmente de textos e imágenes.

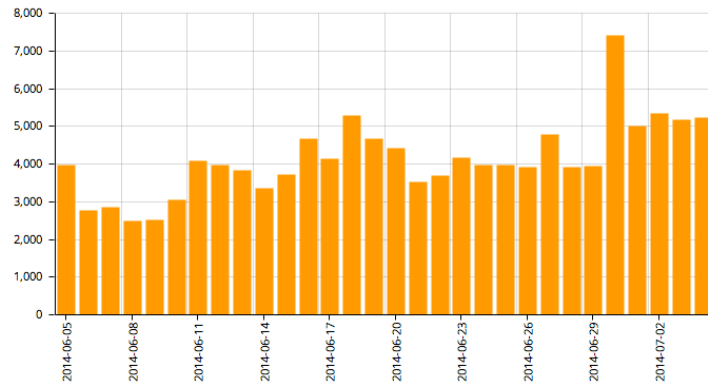
Las webs dinámicas son aquellas que son capaces de interactuar con el usuario o navegante dado a que están conectadas con bases de datos que permiten el desarrollo de aplicaciones webs, su principal ventaja es la personalización de la web en función del usuario así como modificación de los contenidos. Este tipo de webs están desarrolladas bajo lenguajes de programación como PHP, ASP, JSP u otros, el manejo de dichos lenguajes requiere de ciertos conocimientos informáticos. Actualizaciones de la Base de Datos de Virus en los dispositivos del usuario (OCDE en ciberseguridad).



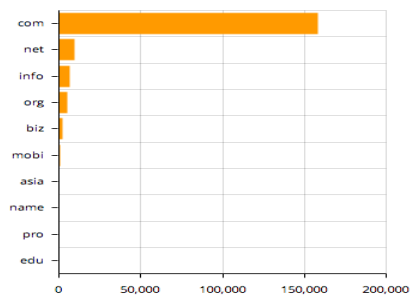
Definiciones de virus añadidas mensualmente (últimos 12 meses)



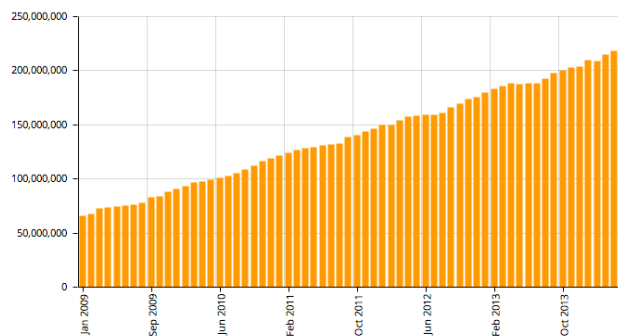
Sitios web infectados descubiertos



Lista de los 10 dominios de nivel superior geográfico genéricos más infectados (último mes)



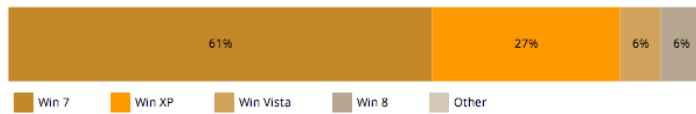
Dispositivos protegidos 226,229,993 PCs, Macs y Androids protegidos



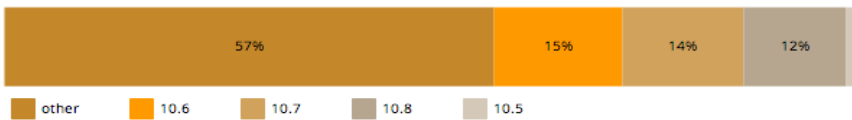
Dispositivos protegidos activamente por Sistema Operativo



Usuarios de PC por sistema operativo



Usuarios de Mac por sistema operativo



Objetivo general

Conocer los riesgos a los que se enfrentan los alumnos de preparatoria cuando acceden a páginas web.

Objetivo específico

Determinar las características de las páginas web y los botones de seguridad de un sitio web que son más visitadas por los alumnos de preparatoria.

Botón de identidad de sitio

Cuando ves el icono del escudo en la barra de direcciones, significa que navegador bloqueó contenido inseguro en la página que visitas.

¿Que contenido no es seguro?

Cuando visitas una página que utiliza HTTP, tu conexión no está protegida contra ataques. La mayoría de los sitios web utilizan HTTP porque no conllevan tráfico de información sensible y no necesitan ser seguras. Cuando visitas una página que utiliza HTTPS (candado gris o candado verde en la barra de direcciones).

Botones y simbolos de identidad de un sitio web ³

El botón de identidad del sitio es un componente de seguridad de que te proporciona más información acerca del sitio que visitas. Puedes descubrir de forma rápida y

³ Aviso de privacidad sobre sitios web, mensajes y cookies “mozilla”.

sencilla si el sitio que visitas ha sido verificado (y por quién) y quién es su dueño. Esto puede ayudarte a evitar navegar por sitios maliciosos que intentan engañarte para obtener tu información personal.

El botón de Identidad de sitio está ubicado justo a la izquierda de la barra de direcciones.



Cuando navegas por un sitio, el botón de Identidad de sitio se convertirá en uno de estos cinco iconos: un globo gris, un triángulo de advertencia naranja, un triángulo de advertencia gris, un candado gris o un candado verde. Si haces clic en alguno de esos iconos te aparecerá información de identidad y de seguridad sobre la página web en la que estés en ese momento.

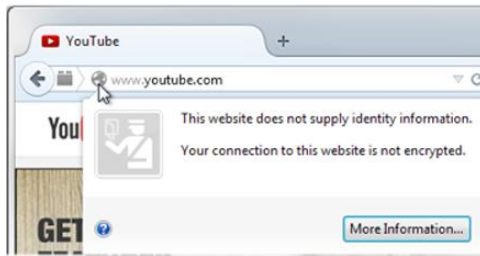


Si haces clic en [Más información](#), en el panel emergente que aparece, obtendrás más detalles sobre la configuración de privacidad y seguridad de esa página web: certificado de información, cookies e historial de contraseñas guardado.

Globo de color gris

Un globo de color gris indica que:

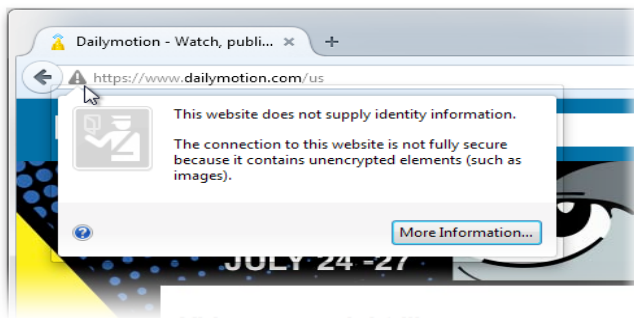
- El sitio web no proporciona ninguna información de identidad.
- La conexión entre Firefox y el sitio web no está cifrada, o está cifrada parcialmente y no debes considerarlo segura ya que no previene el espionaje de tus datos o la suplantación de identidad.



En la mayoría de los sitios actuales se mostrará el botón gris, debido a que no necesitan transmitir información sensible, como tampoco necesitan estar verificados o usar conexiones cifradas. Esto se aplica a páginas web con servidor HTTP (aquellas que no están cifradas) o HTTPS (parcialmente cifradas).

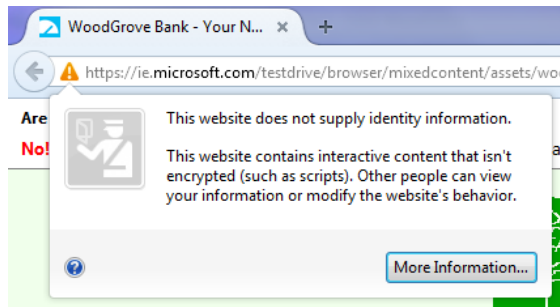
Triángulo de advertencia. Un triángulo gris de advertencia indica lo siguiente:

- La página web no proporciona información de identidad.
- La conexión a esta página no es totalmente segura porque tiene elementos no cifrados (como por ejemplo, imágenes).



Triángulo naranja de advertencia. El triángulo naranja de advertencia indica lo siguiente:

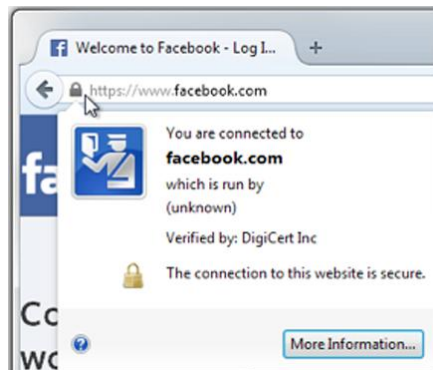
- La página web no proporciona información de identidad.
- La conexión entre Firefox y la página web solo está cifrada parcialmente y no previene el espionaje.



Esto significa que previamente has permitido que el servidor HTTPS pueda mostrar contenido mixto activo a través de esa página web a pesar de los riesgos que implica. Si recargas la página, se volverán a bloquear ciertas peticiones HTTP para amenazas menores, se cambiará el icono y volverá al que estaba antes (globo gris para contenido pasivo mixto y candado gris para cualquier otro tipo de contenido) y se mostrará el contenido.⁴

Candado gris. Un candado de color gris indica que:

- La dirección del sitio web ha sido verificada.
- La conexión entre Firefox y el sitio web está cifrada para prevenir el espionaje.



Cuando se ha comprobado un dominio, significa que las personas que dirigen el sitio web han comprado un certificado que demuestre que son los propietarios del dominio y que no es falso. Por ejemplo, Facebook tiene este tipo de certificado y una conexión cifrada, por lo que el botón de Identidad del sitio muestra un candado gris. Al hacer clic

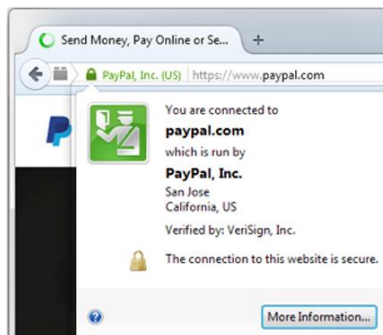
⁴ Kitsune es la plataforma que le da poder al soporte para los botones de seguridad.

en el candado, te indica que en realidad, te estás conectando a facebook .com y que ha sido certificado por VeriSign Inc. También te asegura que la conexión está cifrada para que nadie pueda interceptar la conexión y robar tu información de inicio de sesión de Facebook.

Sin embargo, no se ha verificado quién posee realmente el dominio en cuestión. No hay ninguna garantía de que facebook.com sea actualmente propiedad de la compañía Facebook. Lo único que se garantiza es que el dominio es válido y que la conexión está cifrada.

Candado de color verde. Un candado de color verde indica que:

- La dirección del sitio web ha sido verificada mediante un certificado del tipo Extended Validation (EV).
- La conexión entre Firefox y el sitio web está cifrada para prevenir el espionaje.



Un candado de color verde junto con el nombre de la empresa u organización también en color verde significa que el sitio web está utilizando un Certificado de Validación Extendida (Extended Validation (EV) certificate, en inglés). Los certificados EV son un tipo especial de certificado para los sitios que requieren un proceso de verificación de identidad mucho más riguroso y complejo que otros tipos de certificados. Mientras que el candado gris indica que un sitio web utiliza una conexión segura, el candado verde indica que la conexión es segura "y" que los dueños del dominio son los que el usuario espera que sean.

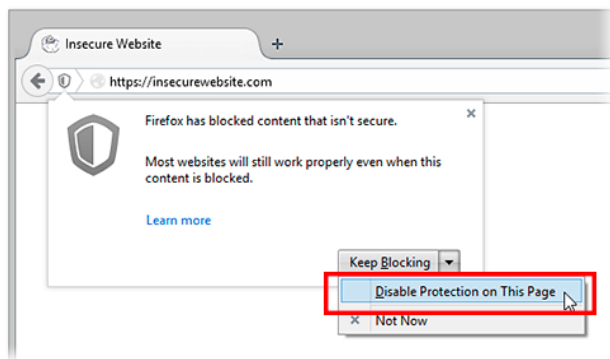
Con el certificado EV, el botón de Identidad del sitio te asegura es propiedad de PayPal Inc., por ejemplo. No solo el candado se vuelve de color verde en el sitio de Paypal, también se expande y muestra el nombre del propietario en el propio botón. Por lo que es importante conocer como proteger mi ordenador con un antivirus que incluya un escudo de red y te muestra este tipo de mensajes y que al momento que detecta una aplicacion maliciosa advierte al usuario y le recomienda abortar la conexcion de cierta pagina web.

Todos los usuarios en línea se enfrentan a una variedad de peligros y amenazas que deben comprenderse y evaluarse.

¿Cuales son los riesgos y tipos de amenazas de los sitios web?

Un atacante puede sustituir el contenido HTTP de la página que estás visitando para robar tus credenciales, acceder a tu cuenta, hacerse con datos sensibles sobre ti o tratar de instalar malware en tu ordenador pero si aun se insiste en abrir estos sitios es importante que realices lo siguiente:

- Haz clic en el icono del escudo  en la barra de direcciones y escoge Desactivar protección en esta página en el menú desplegable.



El icono en la barra de direcciones cambiará a un símbolo de advertencia naranja  para recordarte que se está mostrando contenido no seguro.

Para deshacer la acción anterior (volver a bloquear el contenido mixto), vuelve a visitar

esa página en una pestaña nueva.

Tipos de Amenazas y peligros en las páginas web

* Seguridad informática general

- Utilice tecnología de seguridad informática acreditada y procure mantenerla actualizada. Instale siempre software de cortafuegos y detección de intrusiones y manténgalo actualizado.
- Utilice los navegadores Web más recientes e instale los parches de seguridad. Utilice un servicio de reputación de sitios Web (para una comprobación rápida de la seguridad de una URL,
- Extreme la atención en sitios Web que requieren instalación de software. Lea siempre los acuerdos de licencia detenidamente y cancele el proceso de instalación si se pretende instalar otro programa además del deseado.
- Facilite información personal solo en sitios Web que muestren un icono con forma de candado en la parte inferior del navegador.

* El robo de identidad y las estafas en línea⁵

- Utilice software de seguridad acreditado en su equipo.
- Esté totalmente seguro de lo que descarga de Internet.
- Sea cauto en sus compras en línea.
- Conserve la privacidad de su información personal.
- Mantenga la privacidad. Aprenda cómo utilizar la configuración de la privacidad de los sitios
- Hable sobre lo que es adecuado compartir. Advierta a sus hijos que publiquen únicamente datos que no les importe que vean profesores, familiares o futuros empleadores. Todo lo que publiquen puede ser público para siempre.
- Enseñe a sus hijos a tratar a las personas con respecto y a contarle si están siendo acosados en la red.

⁵ Guía de seguridad informática general. Web Threats.

- Respete los derechos de autor y evite el uso o distribución no autorizados de material con copyright en sus perfiles.
- Denuncie los problemas. Informe al sitio de cualquier contacto no deseado o contenido inapropiado.

* Ciberacosadores y Depredadores de la red

- Piensa bien qué vas a publicar. Utiliza sitios y servicios que permitan definir una configuración de la privacidad. No compartas información personal.
- No te tomes la revancha. Si alguien dice o hace algo en la red que te molesta, es mejor ignorarlo o bloquearlo directamente. La revancha puede animar al acosador a seguir el juego.
- Denuncia los comportamientos inadecuados a una persona conocida. Si alguien te está acosando en la red o por teléfono, cuéntaselo a una persona de confianza.
- Denuncia los comportamientos inadecuados al proveedor de servicios. Denuncia cualquier tipo de acoso al proveedor del servicio de correo electrónico, teléfono, mensajería instantánea o red social utilizado por el acosador. Visita la sección de Ayuda inmediata.
- La amenaza más generalizada, sin embargo, parece ser el acoso cibernético (conocido como ciber-bulling): amenazas, humillaciones, hostigamiento, etc. a través de tecnologías como mensajes de texto, correo electrónico o mensajería instantánea.
- Guarda las pruebas. Si el comportamiento continúa, pide ayuda a tus padres u otro adulto para guardar los mensajes y las imágenes ofensivas así como copias de las conversaciones en línea. Otras formas más graves de ciberacoso deben ser denunciadas a la policía.

Metodología

Mediante una revisión bibliográfica y electrónica se revisarán las características de los botones de seguridad y su uso por medio de una encuesta se determinarán las páginas que más frecuentemente visitan los alumnos de preparatoria en el Colegio Anglo

Mexicano de Coyoacán y el conocimiento que tienen al ingresar a páginas de dudosa procedencia y los riesgos a los que se enfrentan.

Resultados

En el Colegio Anglo Mexicano de Coyoacán se realizó una encuesta a los alumnos de preparatoria en donde sólo el 47% de los alumnos conocía que era una página web y el 85% de los alumnos conocía los tipos de delitos que ocurrían en las páginas web, contestando así que el 48% conocía algunos y 37% los conocía completamente.

En la actualidad, la mayoría de los adolescentes utilizan el internet como herramienta, siendo así que el 95% de los alumnos sabe que es una página web, como consecuencia el navegador que más utilizaban fue Safari, que como sabemos es el navegador de Apple el cual todos los usuarios de esta empresa pueden utilizar como navegador.

Uno de los principales objetivos de esta investigación es que los jóvenes conozcan los botones de seguridad. Estos botones sirven para diferentes cosas, por ejemplo, un globo de color gris indica que el sitio web no proporciona ninguna información de identidad. Un triángulo de advertencia indica que la conexión no es totalmente segura, por lo que existen otros tipos de seguridad y por lo tanto ayudan a identificar cuando se está en una página segura o no. En nuestra encuesta los resultados arrojaron que un 42% del alumnado conoce cuales son estos botones.

Las amenazas de una página web y sus peligros pueden tener consecuencias graves, ya que este tipo de amenazas dañan tu integridad y tu seguridad como persona, por lo que se cree que la mayoría de los usuarios de internet deben conocer los peligros y amenazas de una página web, las encuestas arrojaron que el 89% de los alumnos conocen este tipo de peligros que se encuentran en una página web que pueden ser robo de identidad y estafas en línea, robo de seguridad informática general y ciberacosadores y depredadores de la red.

El abrir una página que tenga contenido malicioso, puede afectar tanto a tu máquina, como a tu persona. Entonces, teniendo una información adecuada sobre el contenido de las páginas web y analizando las encuestas se conoce que el 54% de los alumnos de preparatoria conoce lo que puede suceder al momento de abrir una página web con

contenido malicioso, esto quiere decir que es mayor el número de alumnos que lo saben que los que no saben.

Las leyendas de las páginas web pueden incluir que mientras estés en dicha página web los datos son personales, mensajes engañosos, y amenazas en general. Por lo que el 49% de los encuestados contestó que conocía estas leyendas al entrar en una página web.

Una página web se realiza bajo un lenguaje de programación capaz de ser interpretados por los navegadores, lenguajes. La encuesta arrojó que el 49% del alumnado conoce como se desarrolla una página.

Existen medidas preventivas para proteger tu equipo de ataques de páginas web bloqueando una página para así no encontrar algún daño o amenaza que se presente en alguna página web. Las encuestas dieron como resultado que el 77% de los alumnos encuestados sabe cómo proteger su equipo de ataques.

Las gráficas que arrojaron los resultados se encuentran en el apartado Anexo.

Conclusiones

Al realizar las encuestas en el Colegio Anglo Mexicano de Coyoacán, observamos que un porcentaje alto del alumnado conoce pero no identifica los botones de seguridad de las páginas web, lo que los pone en peligro ya que se pueden enfrentar a riesgos cibernéticos como programas de virus enlace no deseados de sobreestructura y residente, no leer las leyendas que se encuentran en cada página ni conocer los botones de seguridad como el del triángulo de advertencia al indicar que la página no es totalmente segura, el candado gris que indica que la conexión de Firefox está cifrada para prevenir el espionaje, o un candado de color verde que indica que el sitio web está utilizando un Certificado de Validación Extendida. Como consecuencia éste genera un código malicioso y al forzarlo se abren páginas teniendo así el riesgo de tener problemas de integridad por no conocer los botones de seguridad que existen.

Fuentes Bibliográficas

- Gunter, Wielage. (2000). *Gran libro Windows 2000 profesional*, BOIXAREU EDITORES.

- Caballero, Uri.(2013). *Manual Básico de Seguridad Informática para Activistas*. Menalklawn. Versión pgp desktop. Barcelona-Agosto, 2013.

-*Ethical hacking. Seguridad informática*. nueva edición. Editorial ENI.

-Cano, M. Jeimy J. Cano. *Inseguridad de la información*. (2000). Editorial MARCOMBO, 2013.

- García, Moran Jean Paul. *Hacking y Seguridad en Internet*. (2011). Hacking y Seguridad en Internet. Editorial Ra Ma

<http://www.quees.info/que-es-una-pagina-web.html>

<http://www.psicologia-online.com/colaboradores/nacho/ainternet.htm>

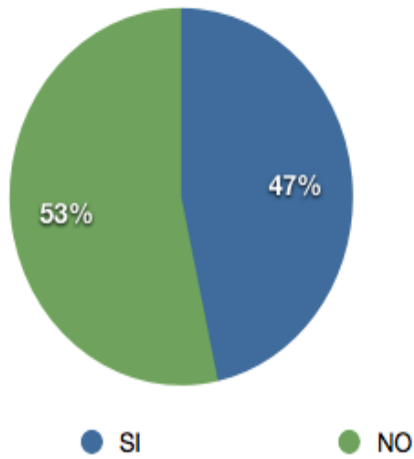
<http://www.trendmicro.es/uso-domestico/seguridad-internet-para-ninos/peligros-en-linea/#redes-sociales>

https://support.mozilla.org/es/kb/boton-de-identidad-de-sitio#w_globo-de-color-gris

<http://www.avast.com/es-mx/stats>

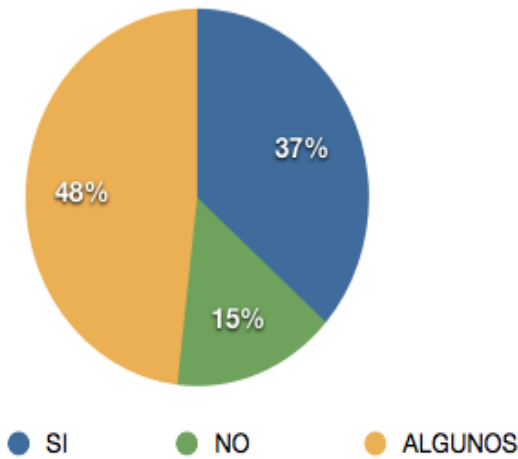
Anexo

¿Conoces los símbolos de seguridad de una página web?



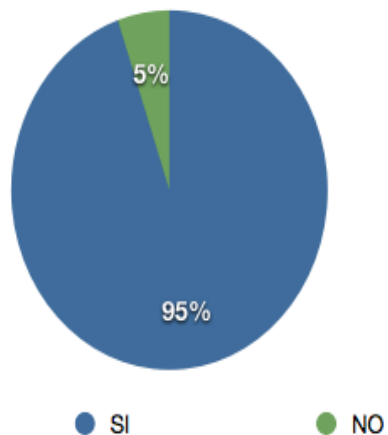
SI	NO
88	101

¿Conoces los tipos de delitos de las páginas web?



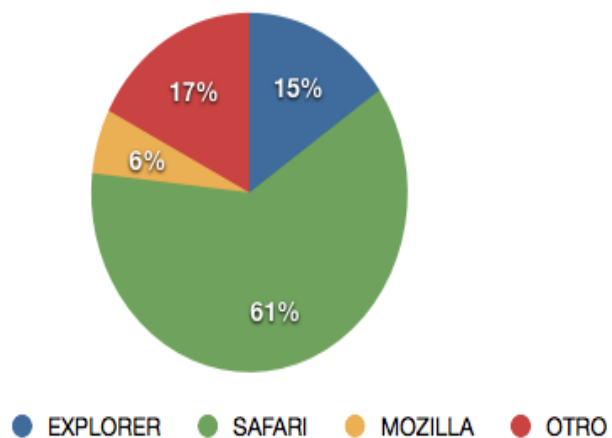
SI	NO	ALGUNOS
69	29	91

¿Sabes qué es una página web?



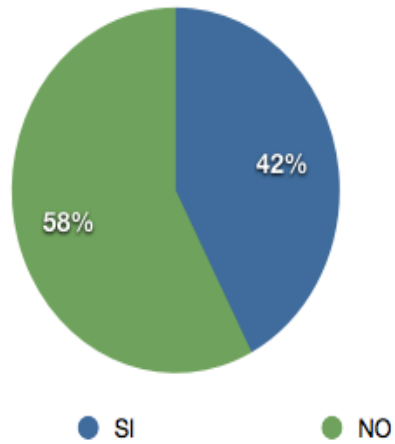
SI	NO
179	10

De la lista ¿Qué navegador usas más?



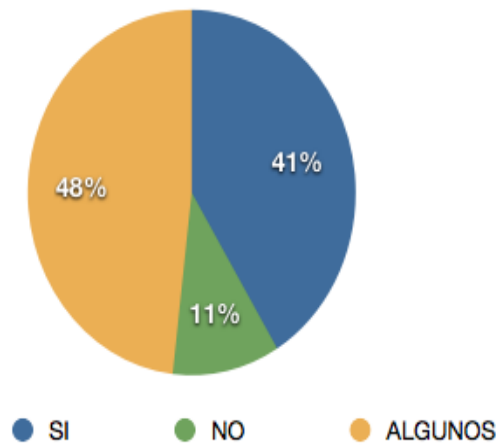
EXPLORER	SAFARI	MOZILLA	OTRO
29	116	11	33

¿Sabes para qué sirven los siguientes botones de seguridad?



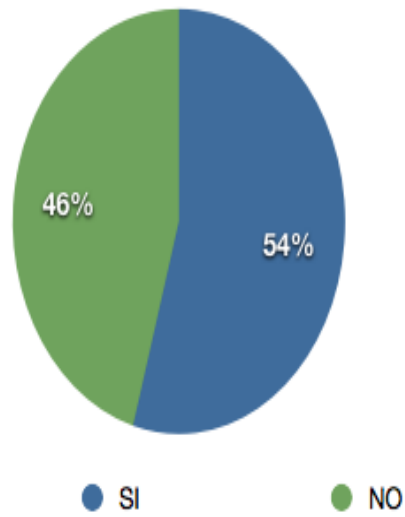
SI	NO
80	109

¿Sabes cuáles son los tipos de amenazas y peligros de una página web?



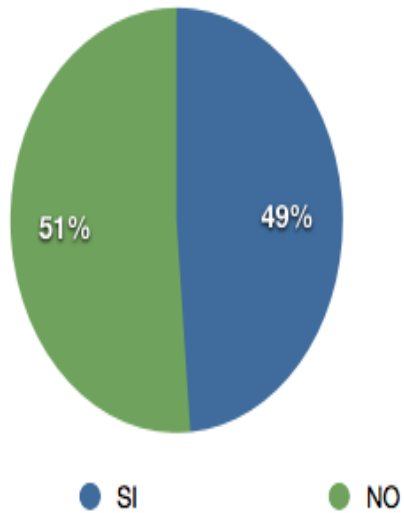
SI	NO	ALGUNOS
78	20	91

¿Sabes qué sucede si abres una página web con contenido malicioso?



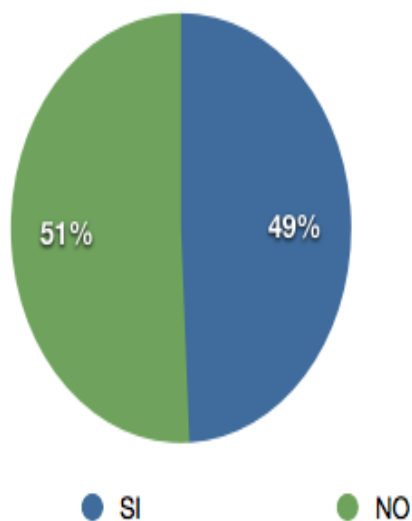
SI	NO
55	46

¿Conoces las leyendas cuando intentas visitar una página web con contenido dudoso?



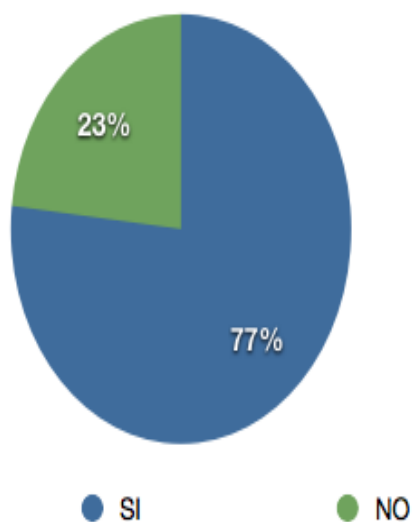
SI	NO
92	97

¿Sabes cómo se desarrolla una página web?



SI	NO
93	96

¿Sabes cómo proteger tu equipo de ataques de páginas con virus?



SI	NO
145	44