CIBERCUIDADO: LOS NIÑOS Y LA SEGURIDAD INFORMÁTICA

Vargas Caleño, Luis Orlando
Especialización en Seguridad Informática, Universidad Piloto de Colombia
Bogotá, Colombia
luis.ovargas@hotmail.com

***Abstract*: At the University, some professors said in class that we, the next Specialists Security, we share our knowledge, be restless, research, practice and always be at the forefront of technological advances, vulnerabilities, threats that every day, that we should not sit still they occur. Something that struck me and I enjoyed it, referred to start with Information Security in our homes, in our families. Those words made me to start teaching my daughter Computer Security; she is 5 years, a process that is excellent so far.**

But what about the other kids asked me, and to consult the Political Constitution of Colombia, Article 44 read that talks about the rights of children, and mentioned that should be protected, there is where you apply everything related to Information Security knowledge acquired to work towards the implementation of that article; and thus contribute in any way to comply with Article 44.

In itself, that is why the realization of this article, to publicize the dangers, the risks to which a child may be exposed when browsing the Internet and interact through social networks, show what tools exist for parents and mothers used as methods of protecting their children by making use of technology, and what to do if they are victims of harassment or incidents on the web.

Keywords: cyber care, cyber crime, cyberspace, grooming, computer security.

***Resumen:* En la Universidad, varios profesores decían en sus clases, que nosotros, los próximos especialistas en seguridad informática, debemos compartir nuestros conocimientos, ser inquietos, investigar, practicar y estar siempre a la vanguardia de los avances tecnológicos, de las vulnerabilidades, de las amenazas que se presentan día a día, que no nos debemos quedar quietos.**

Algo que me impacto y gusto mucho, hacía referencia a iniciar con la seguridad informática en nuestras casas, en nuestras familias. Esas palabras hicieron que yo empezara a enseñarle seguridad informática a mi hija de 5 años, proceso que va excelente hasta el momento. Y el resto de niños, me preguntaba, y al consultar en la Constitución Política de Colombia, leí el Artículo 44 que habla sobre los derechos de los niños, y se menciona que ellos deberán ser protegidos, ahí, es donde se debe aplicar todo lo relacionado con los conocimientos en seguridad informática adquiridos, para trabajar en pro del cumplimiento de ese artículo; y de esta manera contribuir de alguna manera con el cumplimiento del artículo 44 de nuestra Constitución.

Este es el motivo de la realización de este artículo, dar a conocer los peligros y riesgos a los cuales puede estar expuesto un niño cuando navega en internet e interactúa a través de redes sociales, mostrar qué herramientas existen para que padres y madres utilicen como métodos de protección de sus hijos al hacer uso de la tecnología, y saber qué hacer en caso de ser víctimas de acoso o incidentes en la web.

Palabras Clave: cibercuidado, ciberdelito, ciberespacio, grooming, seguridad informática.

I. INTRODUCCIÓN

La Real Academia Española, RAE, define al ciberespacio como el ámbito artificial creado por medios informáticos; de igual manera, la definición de cuidado, como la acción de cuidar, que es poner diligencia, atención y solicitud en la ejecución de algo. Con base en estas definiciones, aparece el término cibercuidado, al que se hace referencia como el cuidado que deben tener los padres, y no solo ellos, cada uno de nosotros como especialistas en seguridad informática, de los peligros que se encuentran en internet, ya que una vez inmersos en la web, niños y adolescentes pueden correr algún tipo de peligro.

Al estar en línea puede ocurrir lo mismo que estando fuera de ella, los niños y adolescentes socializan a través de redes sociales, salas de chat, comunidades virtuales, blogs, etc., es importante ayudarlos enseñándoles a navegar de forma segura por estos sitios.

Entre los peligros que se pueden encontrar en la web se pueden mencionar hechos como el de compartir demasiada información personal, publicar comentarios, fotos o videos que dañen la reputación de otras personas; de igual manera, existen riesgos como el ciberbullying, el

grooming, el sexting, el ciberacoso y la ciberdependencia, que pueden llegar a tocar a niños o adolescentes.

Por otro lado, se encuentra la infección local de computadores por malware a través del uso de internet y el correo electrónico.

Por estas razones, es importante que como padres y/o profesionales, se construyan metodologías, relaciones sociales y/o familiares donde prevalezca la confianza, el acompañamiento y la enseñanza, sobre todo con los usuarios más pequeños, para que la navegación en internet sea segura, responsable y respetuosa.

Por tanto, la Seguridad Informática deberá empezar en cada uno de nuestros hogares y círculos sociales en el que habitamos, de esta manera, el cuidado a tener con niños y adolescentes, debe traducirse en **cibercuidado**.

II. EL PAPEL DEL ESPECIALISTA DE SEGURIDAD INFORMÁTICA

Los celulares inteligentes, las tabletas, los videojuegos, los computadores, los portátiles y muchas otras aplicaciones; hacen uso de internet, sin embargo, hay que saber usarlo y aprovecharlo al máximo y de forma segura, es importante conocer que existen riesgos a los que cualquier usuario se expone al navegar en esta red de redes, sobre todo los niños, que pueden ser más vulnerables.

En Internet se puede encontrar mucha información y de todo tipo: videos, fotografías, animaciones, textos, chats, redes sociales, etc. para investigar o simplemente buscar entretenimiento, del mismo modo, hay sitios con contenido inapropiado, y que de alguna manera están al alcance de todos; incluso de los menores. Dentro de este contexto, si no se cuenta con la compañía de un adulto o con las medidas adecuadas que garanticen la navegación segura, los niños estarían corriendo riesgos dentro del inmerso mundo de Internet, donde podrían llegar a ver sitios y consultar información que esta fuera de contexto y posiblemente errónea; lo cual sería nocivo y podría generar cualquier tipo de dudas e interrogantes; además, no se sabe con certeza, quién y cómo resuelva esas inquietudes a los menores.

Los profesionales en Seguridad Informática, debemos estar al tanto de este tipo de situaciones, debemos saber cuidar a los miembros de nuestras familias en el uso de la tecnología, de Internet, es obligación el compartir la información que tenemos y conocemos, con los vecinos, amigos, padres de familia, etc., con el objetivo de que la Seguridad Informática empiece por nosotros mismos y en cada uno de los hogares que hace uso de Internet, mediante la interacción segura de dispositivos tecnológicos que son de uso diario en niños y adolescentes.

Durante el desarrollo de la Especialización, al ingresar a las instalaciones de la universidad, destinadas a estudiantes de Seguridad Informática, al inicio de clase y en el computador que iba a usar, muchas veces encontré sesiones de Facebook, cuentas de correo de Gmail, Hotmail y cuentas de Dropbox abiertas, con gran cantidad de información personal expuesta: fotografías, archivos, mensajes, contactos, números de celular, etc.

Mientras revisaba toda esa información, me preguntaba asimismo: ¿Qué clase de ingeniero estuvo usando este equipo de cómputo? y si ese era un salón para la preparación de especialistas en Seguridad Informática, ¿Qué se puede ofrecer al mundo en materia de seguridad, si no se cuidan las cuentas personales al dejarlas abiertas en esos equipos?

Lo importante realmente es que todos seamos conscientes de la necesidad de Seguridad Informática que se requiere hoy en día en muchos lugares, no solo en grandes corporaciones, sino también en cada hogar que hace uso de la tecnología y la web, y que es necesaria para cuidar la información personal y la integridad de las personas.

La Seguridad Informática debe empezar con cada uno de nosotros y en nuestras familias, debemos ser muy cuidadosos con la información que manejamos al interactuar en Internet, y al hacer uso de los diferentes dispositivos y aplicaciones de uso diario.

III. AMENAZAS PARA LOS NIÑOS EN INTERNET

Educar a los niños para que realicen una navegación segura en el ciberespacio, es fundamental para protegerlos de los riesgos que existen y que se pueden presentar en este ámbito.

Es importante concientizar a los padres acerca de las amenazas que hay en Internet, y enseñarles cómo protegerse y proteger a sus niños.

A continuación, una serie de delitos y peligros que existen en Internet contra los menores de edad:

A. Ciberacoso

Conocido también como ciberbullying, es una conducta hostil que puede ser usada contra los niños. La víctima es sometida a amenazas, chantajes y humillaciones en la web, a través de imágenes de carácter sexual, montajes o historias inventadas, que pueden llevar a un menor a un estado psicológico de profunda depresión y un quiebre emocional, en último instancia al suicidio en algunos casos.

Estas prácticas pueden ser llevadas a cabo a través de Internet, teléfonos celulares, videoconsolas. Muy frecuente entre adolescentes, razón por la cual no siempre son realizadas por adultos.

B. Grooming

Son las acciones de persuasión de un adulto hacia un niño con el fin de obtener lazos de amistad y una conexión emocional para generar confianza y hacer que el niño realice actividades sexuales mediante imágenes eróticas o pornográficas, incluso encuentros sexuales.

Estos individuos se hacen pasar por niños, tienen perfiles falsos y contactan a otros niños para invitarlos a intercambiar material erótico, y posteriormente extorsionarlos.

C. Sexting

Acrónimo formado entre las palabras sex y texting. Inicialmente trataba del envío de mensajes con contenidos eróticos. Hoy en día, y con el avance tecnológico, la modalidad evolucionó al intercambio de imágenes y videos a través de celulares o tabletas. A veces son usados para el ciberbullying o chantaje con fines sexuales.

D. Robo de Información

Toda la información viaja a través de la web, y si no se cuenta con las medidas de precaución necesarias, ésta puede ser interceptada por un tercero. De igual manera, existen ataques con este fin, así, la información buscada, apunta a datos personales. Un paso en falso en este incidente puede exponer al menor con pérdida de dinero familiar o robo de identidad.

E. Pornografía Infantil

Hace referencia al abuso y a la explotación sexual de los niños con fines lucrativos. Considerado como un delito transnacional y castigado con cárcel.

F. Spam

Es todo aquel correo basura y todos los mensajes recibidos en la bandeja de entrada que no fue solicitada por el usuario, donde existe el riesgo de engaños o estafas a través de Internet.

G. Malware

Hace referencia al software malicioso, son aplicaciones que tienen como fin dañar equipos informáticos, robar información personal o dinero a una persona o usuario.

IV. DELITOS Y ABUSOS, ALGUNOS CASOS RECIENTES

En los últimos meses se ha visto en los canales de televisión nacional, que se están presentando noticias de grooming en Colombia y en otras partes del mundo. A continuación se mencionan algunos casos:

A. Caso Guajira

Este caso se presentó en Riohacha, Guajira, el pasado 11 de junio donde un joven de 22 años engañó por medio de la red social Facebook a una niña de 12 años, él se hizo pasar por otro menor, y ejerció el sexting, hizo que la niña le enviara fotos desnuda, para luego chantajearla y extorsionarla, hasta llegar al punto de violarla.

Fig. 1. Caso de grooming en la Guajira[1].

El padre de la menor, al enterarse, se hizo pasar por la niña, citando al joven de 22 años a su casa, y junto a un hermano de la niña y un conocido, amordazaron y golpearon al agresor.

Esta historia termina contando que la familia fue capturada para que respondan por el empalamiento del que fue víctima el agresor. [1].

B. Caso en Mar de Plata, Argentina

Casos de grooming, ocurren en cualquier lugar del planeta, en Argentina por ejemplo, el pasado abril, se vio un caso similar al de la Guajira, un ciudadano argentino de 37 años, engañó y citó a una niña de 14 años mediante el uso de la red social Facebook a un motel local donde forzadamente la viola y agrede. [2].

El padre de la niña, localizó al agresor y lo apuñaló en dos ocasiones, causándole graves heridas, pero sin ocasionar su muerte.

Fig. 2. Noticia del caso de Grooming en Mar de Plata, Argentina[2].

C. Aumento de ciberdelitos contra menores

El 10 de agosto de 2015, se publica en el diario nacional El Tiempo, otro artículo relacionado con Seguridad Informática, allí se indica que los casos de ciberdelitos están en aumento en nuestro país, y que los padres están fallando en materia de educación y cibercuidado en la atención de sus hijos.

Concuerdo con la policía al indicar que: "el desconocimiento y a veces la inocencia de los menores de edad en el uso y detección de peligros en línea, hacen que terminen como víctimas en los casos delictivos en Internet". [3].

Fig. 3. Artículo sobre aumento de ciberdelitos en Colombia[3].

El grooming, que es muy usado por los ciberacosadores, va en aumento, es una técnica ampliamente usada por personas para engañar a niños y menores. Al realizar la consulta de incidentes reportados durante julio en el Centro Cibernético Policial (CCP) [4], se observa en el ranking de *sectores*, que el segundo lugar lo ocupa la categoría *menor de edad*, mediante modalidades de sexting y grooming por medio de las redes sociales.

Fig. 4. Ranking de Incidentes reportados al centro Cibernético Policial durante julio de 2015[4].

Estos datos hacen referencia a los incidentes reportados, sin tener en cuenta aquellos no reportados o desconocidos por padres, quienes por falta de educación en temas digitales y uso de tecnología de forma responsable, no logran estar atentos y pendientes de sus niños en la web.

[1] PrintScreen tomado de www.eltiempo.com. Agosto de 2015.
[2] PrintScreen tomado de www.clarin.com. Agosto de 2015.
[3] PrintScreen tomado de www.eltiempo.com. Agosto de 2015.
[4] PrintScreen tomado de http://www.ccp.gov.co. Agosto de 2015.

Creo que con estos tres ejemplos son muy dicientes sobre los delitos y peligros que suceden no solo en Colombia, sino en el mundo entero, donde se observa que el ciberacoso, el robo de identidades digitales, las amenazas, los chantajes y sobre todo el grooming están en incremento, además trae como consecuencias: violaciones, asesinatos, venganzas, cárcel y sobre todo; sufrimiento de los niños.

Esto sirve para darnos cuenta de la necesidad que existe para que los profesionales en Seguridad Informática compartan su conocimiento en busca de la protección de los niños, y guíen a los padres, con el fin de acompañar y proteger a los niños en el uso de redes sociales y así tratar de evitar o mitigar este tipo de delitos y abusos.

V. QUÉ SE PUEDE HACER

Ya se ha mencionado que es necesario educar a padres y menores para un buen uso de la tecnología de manera responsable, que es deber nuestro el de compartir el conocimiento en Seguridad Informática, enseñar medidas de control que sirvan para mitigar riesgos que pueden enfrentar los niños al navegar por Internet.

Es importante mostrar las herramientas que existen en línea para la prevención y seguridad en las redes sociales más usadas actualmente:

A. Centro de seguridad para familias en Facebook

Facebook cuenta con el Centro de Seguridad para Familias, donde explican a padres, profesores y niños sobre seguridad, creación de entornos seguros, allí ofrecen herramientas y recursos para configurar cuentas y hacer uso de las mejores prácticas de seguridad, se enseña a los niños y adolescentes a usar Facebook sin riesgos, a usar los medios sociales de forma responsable y aplicar criterios e inteligencia al estar en línea. [5].

Este recurso debería ser consultado por cualquier persona que tenga una cuenta en Facebook y enseñado por los profesionales de Seguridad Informática al mundo, para adquirir las mejores prácticas de seguridad al estar conectado en esta red social.

El sitio se puede consultar en https://es-es.facebook.com/safety

Fig. 5. Centro de seguridad para familias[5].

B. Google: Centro de Seguridad

El Centro de Seguridad de Google ofrece consejos prácticos a padres, profesores y comunidades para que sepan cómo proteger la seguridad de la familia en Internet, brinda ayudas sobre como navegar en línea de forma segura y proteger los datos personales. Explica de forma clara y sencilla las funcionalidades de seguridad de Google. Se encuentra por ejemplo la forma de obtener resultados aptos para toda la familia, establecer filtros para excluir contenidos inadecuados, supervisar usuarios en chromebook compartidos, limitar el acceso a aplicaciones y juegos y guías para elegir aplicaciones adecuadas para cada edad. Dentro de sus herramientas de seguridad, explican la manera de utilizar los servicios de Gmail, Chrome, Youtube de forma segura.

Este portal es una gran herramienta de información para mantener una web segura, administrar la privacidad de datos personales y desarrollar hábitos de seguridad en línea. El sitio se puede consultar en https://www.google.com/safetycenter/

[5] PrintScreen tomado de https://es-es.facebook.com/safety. Agosto 2015

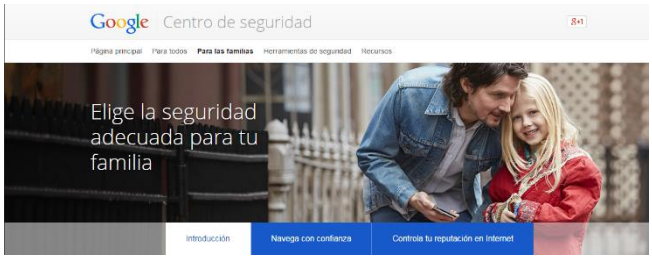

Fig. 6. Centro de Seguridad de Google para familias[6].

C. Twitter y sus consejos para las familias

El centro de seguridad de Twitter tiene su espacio dedicado a la seguridad familiar, para mantener una navegación segura.

Fig. 6. Presentación del Centro de Seguridad de Twitter[7].

En este portal se encuentra información, herramientas, políticas y en una sección para familias donde se hace la invitación a padres y tutores a ser conscientes de los riesgos existentes y problemas que se pueden presentar al estar en línea. Se invita a conversar con los hijos adolescentes sobre seguridad on line, resuelven inquietudes del tipo ¿Con quién compartir contenido? y ofrece la guía sobre qué hacer en caso de requerir ayuda, bloquear a una persona y presentar denuncias. El portal y los recursos adicionales de twitter se pueden consultar en https://about.twitter.com/es/safety.

D. En Tic Confio

En Colombia hay varios portales que se pueden visitar para consultar información referente a seguridad en la web, uno de ellos es enTicconfio; que promueve la confianza y seguridad en el uso de las TIC.

Allí se encuentra gran cantidad de información útil e interesante, como los consejos para el uso de las TICs, la identificación de riesgos en la web y la forma de prevenirlos. Este portal contiene artículos y sesiones muy interesantes, respecto al cuidado que se debe tener en Internet, temas como el sexting y el grooming son tratados, al igual que herramientas y tips para evitar ser víctimas en la red.

El sitio puede ser visitado en la URL http://www.enticconfio.gov.co/ una opción muy interesante es que ofrecen conferencias a colegios, universidades, empresas para compartir escenarios de aprendizaje en el uso responsable de Internet.

Fig. 7. Portal Colombiano En Tic Confío[8].

E. PaPaz

El portal PaPaz pertenece a una entidad que representa a padres y madres en el país, buscando el alcance de la responsabilidad social en la ciudadanía, el Estado y en los medios de comunicación, teniendo dentro de su visión la protección de la adolescencia en Colombia.

Fig. 8. Portal de Red PaPaz[9].

Una de sus estrategias, denominada Tecnologías de la Información y las Comunicaciones TICs, trabaja para que los niños tengan acceso y uso sano y seguro en estas tecnologías de manera constructiva

Es un sitio donde se pueden afiliar instituciones educativas, asociaciones de padres de familia y personas en general, cuenta con un boletín virtual, para que los usuarios registrados reciban noticias,

[6] PrintScreen tomado de https://www.google.com/safetycenter/. Agosto 2015.
[7] PrintScreen tomado de https://about.twitter.com/es/safety. Agosto de 2015
[8] PrintScreen tomado de www.enticconfio.gov.co. Agosto de 2015
[9] PrintScreen tomado de www.redpapaz.org. Agosto de 2015.

consejos y notas de seguridad, de igual manera, ofrecen contenidos a padres para que cuenten con herramientas para educar mejor a sus hijos.

Estos son solo algunos sitios que se sugieren para que padres y madres puedan iniciar con un proceso de aprendizaje y obtención de herramientas que ayuden con la protección de la identidad virtual de sus hijos, la protección de datos personales, y en fin, para tener medidas de control contra cualquier riesgo y peligro que se pueda presentar en Internet que amenacen a sus hijos y a sus propios datos.

VI. CONCLUSIONES

1. Es importante enseñar tips de Seguridad Informática a la comunidad en general, empezando por casa, para acompañar a los niños y velar por su seguridad cuando acceden a Internet y a redes sociales, ya que no es posible saber todo lo que puede pasar en la vida de niños y niñas, pero es indispensable enseñarles claramente cuáles son los riesgos que existen y qué hacer ante la presencia de alguno de éstos, pues con el tiempo y con los avances tecnológicos, no será tan fácil controlar las herramientas de comunicación que se usan. Los menores están expuestos a múltiples escenarios que pueden llevarlos al peligro o a la vulneración de sus derechos.

2. Es importante tratar de evitar que los adolescentes acceden a Internet sin supervisión, sin control, es importante aplicar configuraciones que permitan crear filtros en el computador para bloquear sitios obscenos, términos como el de drogas y pornografía por citar algunos ejemplos.

3. Existen varios portales para reportar delitos o sospechas a nivel informático, sitios que mucha gente podría desconocer, páginas web como la del Centro Cibernético Policial, el Caí Virtual de la Policía Nacional, teprotejo.org, enticconfio.gov.co son sitios donde es posible solicitar información y realizar denuncias sobre abusos contra menores, nosotros, como especialistas en Seguridad Informática, debemos compartir y expandir esta información para que muchas personas a nuestro alrededor conozcan de la existencia de estos sitios y su importancia.

4. El 4 de agosto de 2015, la corte Suprema de Justicia, en el Comunicado 03 de la Sala Penal, publicó un fallo, donde indican que los padres de familia pueden ver las cuentas de correo y redes sociales de sus hijos menores de edad para velar por su seguridad y de esta manera protegerlos [6], además, no se viola la intimidad de los niños al tratar de garantizar su educación, protección y orientación. Esto es una medida desesperada, para que los padres estén atentos y ayuden, orienten, acompañen y enseñen a sus hijos, para que no los descuiden y dejen navegar en Internet de una manera vaga y libre, sin ninguna restricción, pudiendo consultar páginas de pornografía, aceptar solicitudes de amistad de personas desconocidas en las diferentes redes sociales, descargar e instalar cualquier aplicación; por eso la importancia de que personas como nosotros, que contamos con el conocimiento en Seguridad Informática, seamos conscientes de este escenario y aportemos nuestro grano de arena, para contrarrestar este tipo de cosas que suceden a diario en Internet y a nuestro alrededor.

REFERENCIAS

[1]. Periódico digital El Tiempo. Familia, presa por empalar a violador de niña de 12 años. [En línea]. Colombia, 17 de junio de 2015. Disponible en http://www.eltiempo.com/politica/justicia/familia-presa-por-empalar-a-violador-de-nina-de-12-anos/15965261

[2]. Diario digital El Clarín. Engañó a una adolescente de 14 por Facebook y la violó. [En línea]. Mar de Plata, Argentina, 21 de abril de 2015. Disponible en http://www.clarin.com/policiales/Engano-adolescente-Facebook-violo_0_1343865653.html

[3]. Periódico digital El Tiempo. Aumentan casos de ciberdelitos contra menores en el país. [En línea]. Colombia, 10 de agosto de 2015. Disponible en http://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-es-cada-vez-mas-peligroso-para-los-ninos/16207955?hootPostID=5da346e4b8275f31e8c6710239727217

[4]. Centro Cibernético Policial. Ciberincidentes, visualización Mapa Tiempo Real. [En línea].

Colombia, julio de 2015. Disponible en http://www.ccp.gov.co/ciberincidentes/tiempo-real/

[5]. Facebook. Centro de seguridad para familias. [En línea]. España, agosto de 2015. Disponible: en https://es-es.facebook.com/safety

[6]. Corte Suprema de Justicia. Comunicado del 4 de agosto de 2015. [En línea]. Colombia, agosto de 2015. Disponible en: http://190.24.134.121/webcsj/Documentos/ComuniCorte/Penal/2015/Comunicado%20Sala%20Penal%2003%20de%202015.pdf

Autor

Luis Orlando Vargas Caleño. Ingeniero en Redes de Computadores, egresado de la Universidad Distrital Francisco José de Caldas en el año 2012. Actualmente se encuentra finalizando estudios de Postgrado en Seguridad Informática en la Universidad Piloto de Colombia.

Desde el año 2008 hasta el año 2013 trabajó como Ingeniero de Soporte en Infraestructura para Xerox, en la ciudad de Bogotá, luego ejerció como Director de Infraestructura en Dasigno SAS durante 15 meses, y actualmente se desempeña como PCN Support Engineer y Líder de Proyectos para Chevron Petroleum Company.