S.O. usados por los clientes de la red de la Universidad Cooperativa de Colombia campus Villavicencio

OS used to connect to the network of University Cooperativa de Colombia campus Villavicencio

Carlos Ignacio Torres Londoño[1]
[1]*Programa Ingeniería de sistemas, Facultad de Ingeniería, Universidad Cooperativa de Colombia sede Villavicencio, Grupo de investigación GIPIS*
[1] *carlos.torreslo@campusucc.edu.co*

Resumen– *El Propósito de este investigación fue el de generar una estrategia de sensibilización en los estudiantes, administrativos y docentes del programa de ingeniería de sistemas de la Universidad Cooperativa de Colombia sede Villavicencio, sobre los riesgos presentes en el momento en el que se conectan con sus dispositivos informáticos a las redes de la universidad. Para esto se realizó una caracterización piloto, en la cual se inspeccionó que conocian los usuarios de algunos terminos de seguridad informatica. Mediante el análisis de los datos obtenidos se puedierón identificar cuáles eran los posibles riesgos a los que se sometian los usuarios de las redes de la UCC. En este trabajo se plantea una estrategia para mitigar los riesgos detectados y se socializan estos resultados a la comunidad académica afectada por el piloto. Como conclusión, se pueden observar muchas similitudes en los datos obtenidos en la encuesta realizada y las estadísticas disponibles en Internet sobre dispositivos y sistemas operativos que se conectan a internet. Aunque no se puede garantizar una seguridad total al conectarse a una red, la educación y conocer sobre los riesgos que generamos sigue siendo la forma más eficiente de fortalecer el eslabón más débil de la cadena, permitiendo minimizar este riesgo mediante el uso de unas buenas prácticas de seguridad informática.*

Palabras claves– *Gestión de la seguridad ,Ingeniería del conocimiento, Seguridad de la información, Seguridad de la red, Vulnerabilidad de los sistemas operativos.*

Abstract– *The objective of the present study is to develop a sensitizing strategy for the computer science program users of the Universidad Cooperativa de Colombia (UCC) at the Villavicencio's campus about the risks involved when they paired their electronic devices with the university network. In order to develop the strategy, it is necessary to develop a pilot characterization. A data analysis of the collected information elucidates the potential risks. The present studies targets to develop an integral strategy to mitigate these risks and its discussion with the academic community involved in the pilot survey. As conclusion, it is possible to observe a high correlation between the present study and the statistics available in internet regarding the kind of device and operating system used to connect into internet. Despite it is not possible to guarantee complete security when a user join a network, education and a wider knowledge of the risks generated during a connection, are the most effective way to strong the weaker link of the process by minimizing the risks by adopting a good informatics security practices.*

Keywords– *Information security, Knowledge engineering, Network security, Operative systems vulnerability, Security management*

1. Introducción

Cada día, tenemos más cantidad de dispositivos que se conectan a internet. Se estimaba que en 2003 existían cerca de 500 millones de dispositivos conectados[1], [2], mientras que se estima que para el año 2020 la cantidad será de 50 mil millones de dispositivos conectados a Internet. Si vemos la evolución de los dispositivos con los que se realizan las conexiones a internet, se puede decir que en principio las conexiones se realizaban desde computadores de mesa o portátiles, después llegan los teléfonos, siguen los Smartphone, televisores, tabletas y dispositivos wearables; por lo que se estima que cada persona en este momento puede tener entre tres y cuatro distintos dispositivos para conectar a internet.).

Los sistemas operativos de todos estos dispositivos pueden ser vulnerables y presentar vulnerabilidades no detectadas hasta el momento (Día cero)[3]. Estas vulnerabilidades son el punto de partida para generar

ataques mal intencionados como el que sucedió el pasado 14 de octubre de 2016 contra DynDNS y que dejo sin acceso a los principales sitios en internet[4]–[6]. Este ataque se dio desde dispositivos wearables.

En los últimos 15 años se han presentado muchos y distintos tipos de ataques, como el que realizo en represalia por el cierre de WikiLeaks[7], o problemas de seguridad con gusanos como sasser[8]–[10], los secuestros realizados por medio de ransomware[11], [12] en diferentes partes del mundo[12]–[14] o el negocio que representa el phishing[15] a las personas del común[16] o a hasta las campañas políticas[17]

El usuario es el eslabón más débil de la cadena y por lo tanto es el principal riesgo para cualquier organización, en este caso para la Universidad Cooperativa de Colombia (UCC). Dado además el gran flujo de dispositivos es cada vez más difícil controlar y prevenir ataques en la red. Una forma de disminuir o minimizar algunos de estos riesgos es el generar conciencia de lo que sucede y hacer campañas para prevenir este tipo de incidentes. En este aspecto este trabajo busca realizar una primera caracterización de los dispositivos con los cuales se conectan a la UCC, los diferentes integrantes del programa de Ingeniería de Sistemas.

Analizando los datos de esa caracterización debe generarse una serie de acciones que permitan mitigar los diferentes riesgos. Esta estrategia debe ser socializada a la comunidad para que sea ejecutada como medio de prevención y conocimiento.

Este documento toma algunas de las sugerencias presentadas en los diferentes informes de empresas de seguridad,[3], [18], [19] que hacen de alguna manera énfasis en lo importante de la educación, como primera herramienta para la prevención y minimización de los riesgos asociados a este tipo de eventos no deseados[20].

La problemática de la seguridad está dada por los posibles riesgos que se pueden presentar al hacer uso no apropiado de la redes (UCC Estudiantes, UCC Docentes, UCC Salas), siendo los usuarios el eslabón más débil de la cadena, es preciso dar una serie de medidas que prevengan posibles vulnerabilidades en las redes, para evitar así problemas relacionados con la seguridad.

La universidad es un espacio, al cual los diferentes miembros de la academia acceden con diferentes dispositivos de diferentes tipos, no existe un control para acceder y conectarse a las redes de la universidad. La única característica de seguridad es el de un usuario y contraseña, en algunas de las redes de la universidad se puede ingresar con el usuario por defecto como invitado y sin contraseña y en las otras debido a la poca formación de la comunidad académica en este tema, suelen conocerse y circular las claves de las diferentes redes como UCC Docentes o UCC Salas.

Todos estos factores hacen que además de problemas con los rendimientos de la red se puedan presentar focos de infección y propagación de virus y malware en la universidad, además de todos los riesgos que se pueden presentar como perdida de información.

2. Materiales y métodos

Para la investigación se plantea el desarrollo de una encuesta piloto, con el fin de determinar las características de los diferentes dispositivos con los cuales se conectan a la red de la Universidad Cooperativa de Colombia los diferentes usuarios del programa de Ingeniería de Sistemas.

El universo de este piloto es toda la comunidad universitaria (estudiantes, docentes y administrativos y visitantes) de la universidad Cooperativa de Colombia sede Villavicencio, la muestra de este estudio son los miembros (estudiantes, docentes y administrativos) de la comunidad universitaria que pertenecen al programa de ingeniería de sistemas, con los datos proporcionados por estos últimos se realiza la caracterización de esta investigación

Las principales características que se quieren establecer son:

- Las redes a las cuales se conectan los diferentes usuarios del programa de Ingeniería de sistemas en el momento que acceden a la Universidad Cooperativa de Colombia.
- Los diferentes dispositivos que utilizan cuando acceden a las redes de la Universidad Cooperativa de Colombia.
- Cuáles son los sistemas operativos de esos dispositivos y si los tienen actualizados a la última versión disponible.
- Si utilizan programas como antivirus en los diferentes dispositivos con los cuales se conectan a las redes de la Universidad Cooperativa de Colombia.
- Si saben que es una red privada virtual (vpn) y si las utilizan en las conexiones a las diferentes redes de la Universidad cooperativa de Colombia.
- Si tienen instalado un firewall, en los dispositivos

con los que se conectan a la red de la Universidad Cooperativa de Colombia.

- Si han realizado operaciones bancarias (consulta de saldo, transferencias, etc.) o compras o pagos desde Internet o desde la red de la Universidad Cooperativa de Colombia.
- Si conocen algo sobre la DeepWeb, si ingresan a ella desde la red de la Universidad Cooperativa de Colombia.

La encuesta completa fue la siguiente:

1 Se conecta a la red de la universidad Cooperativa de Colombia con algún dispositivo (Portátil, Tablet, Smartphone, otro)

Si o No

2 ¿A que red de la Universidad Cooperativa de Colombia se Conecta?

Ucc Estudiantes, Ucc Docentes, Salas, Otra?

3 Utiliza portátil, para conectarse a la red de la UCC

Si o No

4 Que sistema operativo tiene?

Windows, Linux, Mac OS, Otro

5 Conteste Si o No para cada una de las siguientes preguntas según sea el caso para su portátil

A [Tiene actualizado el sistema operativo de su portátil]

B [Tiene instalado un antivirus en su portátil]

C [Esta actualizado su antivirus]

D [Ha tenido alguna vez un virus]

E [Ha tenido malware en su portátil]

6 Utiliza tablet, para conectarse a la red de la UCC

Si o No

7 Que sistema operativo tiene su tablet?

Windows Phone, iOS, Firefox, Android, Chrome, Otro

8 Conteste Si o No para cada una de las siguientes preguntas según sea el caso para su tablet

A [Tiene actualizado el sistema operativo de su tablet]

B [Tiene instalado un antivirus en su tablet]

C [Esta actualizado su antivirus en su tablet]

D [Ha tenido alguna vez un virus en su tablet]

E [Ha tenido malware en su tablet]

9 Utiliza Smartphone, para conectarse a la red de la UCC

Si o No

10 Que sistema operativo tiene su Smartphone?

Windows Phone, iOS, Firefox, Android, Chrome, Otro

11 Conteste Si o No para cada una de las siguientes preguntas según sea el caso para su Smartphone

A [Tiene actualizado el sistema operativo de su Smartphone]

B [Tiene instalado un antivirus en su Smartphone]

C [Esta actualizado su antivirus en su Smartphone]

D [Ha tenido alguna vez un virus en su Smartphone]

E [Ha tenido malware en su Smartphone]

12 Utiliza otro tipo de dispositivo para conectarse a la red UCC

Si o No

13 Responda Si o No a cada una de las siguientes preguntas:

A [Sabe que es una VULNERABILIDAD]

B [Sabe que es un Firewall]

C [Usa Firewall en su portátil]

D [Sabe que es una VPN]

E [Utiliza VPN al conectarse a la UCC]

F [Sabe que es la Deep Web]

G [Ha navegado en la Deep Web desde la UCC]

H [Ha realizado operaciones bancarias (Consulta de saldo, ingreso a la cuenta) desde Internet]

I [Ha realizado compras desde Internet]

J [Ha hecho pagos por Internet]

K [Ha realizado operaciones bancarias o compras o pagos desde la red de la UCC]

14 Quiere informarnos sus datos

Si o No

15 Correo

16 Tipo Participante

Estudiante, Docente, Administrativo

17 Si es estudiante cuál es su semestre actual

La encuesta se realizó utilizando google forms y se difundió a través del Facebook oficial del programa, en el cual están registrados todos los estudiantes, docentes y administrativos del mismo.

3. Resultados

Después de que los miembros del programa de ingeniería de sistemas respondieron a la encuesta se procedió al análisis de las respuestas dadas en la encuesta que fueron los siguientes:

1) Para la primer pregunta "1 Se conecta a la red de la universidad Cooperativa de Colombia con algún dispositivo (Portátil, Tablet, Smartphone, otro)" el resultado muestra como más del 90% de la población que

respondió la encuesta se conecta de alguna manera a la red de la universidad

2) Para la segunda pregunta, "2 ¿A qué red de la Universidad Cooperativa de Colombia se Conecta?" la mayoría de la población que respondió a la encuesta se conecta a la red UCC Estudiantes cerca del 80% mientras que le siguen: UCC Docentes , Salas.

3) Para la tercera pregunta "Utiliza portátil, para conectarse a la red de la UCC", los resultados son que prácticamente tres de cada cuatro de los que se conecta a la red lo hace a través de su portátil.

4) Para la cuarta pregunta "¿Qué sistema operativo tiene?", la mayoría acceden desde sistemas Windows, después Mac OS y finalmente Linux

5) La quinta pregunta tiene cinco partes:

a) Para la primera de las partes "Tiene actualizado el sistema operativo de su portátil", solo los equipos con el sistema Linux se encuentran actualizados, después los con Mac OS, se encuentran la mitad actualizados y la mitad sin actualizar; finalmente casi uno de cada cinco portátiles con Windows se encuentran sin actualizar.

b) Para la segunda de las partes "Tiene instalado un antivirus en su portátil", para el sistema operativo Linux no tienen instalado un antivirus, para Mac OS la mitad tienen instalado el antivirus y para Windows más del 90% tiene antivirus.

c) Se puede ver que en los portátiles con sistema operativo Windows los usuarios tienen actualizado en mayor porcentaje el antivirus, mientras que en sistemas como Linux al no tenerlo instalado no lo actualizan.

d) Más del 50 % de los encuestados dicen nunca haber tenido un virus en sus portátiles, se tiene una mayor percepción de seguridad para sistemas como Linux, después para Windows y finalmente para Mac OS

e) La inmensa mayoría dice que sus equipos no han tenido Malware, es interesante realizar un test de malware para demostrar si esta aseveración es correcta o falsa.

6) Sexta pregunta, solo el 9% de los que contestaron la encuesta indican que acceden a la red de la UCC utilizando una Tablet.

7) Séptima pregunta, se observa como las Tablet que acceden a la red en la universidad tiene el sistema operativo Android.

8) En cuanto a si el sistema operativo de las Tablet esta actualizado se detecta que el 50% de los usuarios con Tablet así lo indican, mientras que el otro 50 dicen que no. Valores muy similares se han obtenido para cada uno de los ítems preguntados (Tiene Antivirus, esta actualizado, ha tenido virus, ha tenido malware), a los miembros del programa que indican que acceden con Tablet a la red de la UCC

9) En cuanto a la pregunta si se conecta con su Smartphone a la red de la universidad, se puede ver como claramente se da una conexión masiva de estos dispositivos cada vez más generalizados en el medio y que permiten hacer una variedad de tareas, por su fácil portabilidad, con lo que el 83% de los encuestados dicen ingresar a la red de la UCC con este tipo de dispositivo.

10) En cuanto a los sistemas operativos de los Smartphone con los que se conectan a la red de la UCC, se puede apreciar que casi tres de cada cuatro tiene un dispositivo con el sistema operativo Android, principalmente por su gran cuota de mercado; algo más del 20 % tienen dispositivos con sistema operativo iOS y uno de cada 20 tiene dispositivo con sistema operativo Windows Phone.

11) Para esta pregunta se analiza cada una de las diferentes sub preguntas:

a) En general un porcentaje cercano al 80 % es decir, cuatro de cada cinco dicen tener el Smartphone actualizado el S.O.

b) Más de la mitad de los Smartphone carecen de antivirus y es especialmente preocupante en dispositivos con sistema operativo iOS y Android.

c) De los pocos Smartphone que tienen antivirus, solo el 32% se encuentra actualizado.

d) La gran mayoría dicen no haber tenido nunca un virus en sus Smartphone.

e) En cuanto a lo referido con malware, es mayor la percepción de este entre los encuestados y uno de cada cuatro usuarios de iOS ha tenido malware.

12) Los miembros dicen no utilizar otros dispositivos para conectarse a la red de la universidad.

13) Respecto a las preguntas de conceptos de seguridad la encuesta muestra que:

a) Más del 90% de los encuestados dicen saber que es una vulnerabilidad.

b) ¿Sabe que es un Firewall? Más del 80% de los que respondieron la encuesta dicen saber que es

c) el 71% de los encuestados dice que tiene activo el firewall.

d) ¿Sabe que es una VPN? Tres de cada cuatro respondieron que saben que es.

e) Sin embargo, en el mento de utilizar las redes virtuales privadas, se invierten los porcentajes, ni uno de cada cuatro, Utiliza VPN.

f) ¿Sabe que es la Deep Web? Un 57% de los encuestados dicen saber que es y el 43% restante lo desconocen.

g) ¿Ha navegado en la Deep Web desde la UCC? Solo el 9% de los que respondieron la encuesta dicen que sí.

h) ¿Ha realizado operaciones bancarias (Consulta de saldo, ingreso a la cuenta) desde Internet? algo más de la mitad de los que respondieron la encuesta dicen que en alguna ocasión han realizado una operación bancaria desde internet.

i) como el 52% de los encuestados, dicen que si a la pregunta ¿Ha realizado compras desde Internet? En algún momento de sus vidas.

j) ¿Ha hecho pagos por Internet? Casi tres de cada cinco los han realizado.

k) Respecto a la pregunta ¿Ha realizado operaciones bancarias o compras o pagos desde la red de la UCC? solo el 22% respondió que sí.

5.2 Reflexión de la caracterización de los datos

Dada la versatilidad y la gran penetración en el mercado local de los Smartphone cerca de 14 millones al finalizar el año 2015 según el ministerio de las tics en Colombia[21], [22], se observa que el dispositivo con mayor número de conexiones a la red de la Universidad Cooperativa de Colombia. Como era de esperar al ser mayor la cantidad de estudiantes entre los miembros del programa de ingeniería de sistemas (en una relación de 30 a 1), esta hace que la red a la que más se conecten en la Universidad cooperativa de Colombia sea la denominada UCC estudiantes.

Cuando se habla de sistemas operativos se pueden ver dos tendencias claras: en los portátiles el sistema predominante es Windows y en los Smartphone el sistema predominante es Android.

Si se analizan los datos recogidos y los se comparan con los de gs.statcounter.com, se puede ver que el programa de ingeniería de sistemas, conserva la relación entre los sistemas operativos Linux y Mac OS, por ordenador con Linux existen dos con Mac OS, también se aprecia que son casi un 83 % los equipos con Windows como se puede ver en la figura 1.

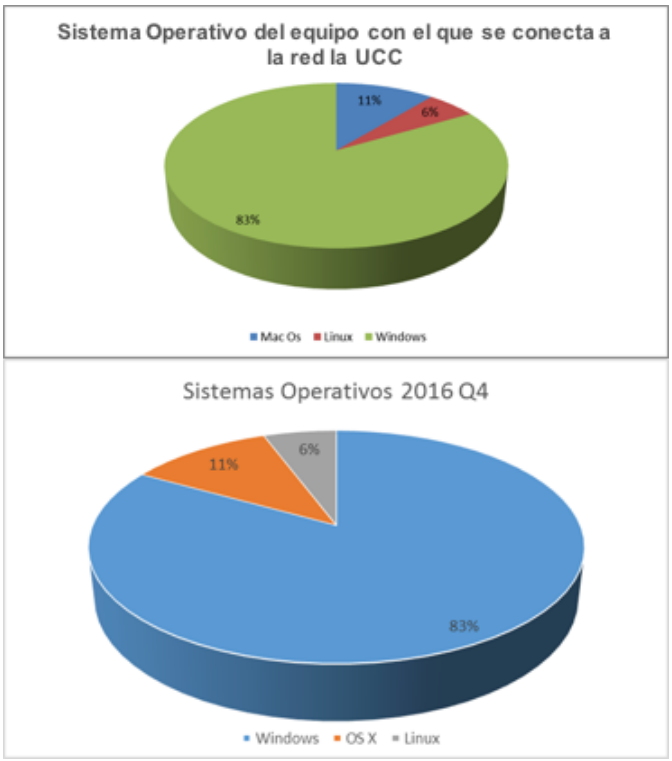

Figura 1. Comparación de los datos obtenidos y los datos de mercado. Arriba son los datos obtenidos en la encuesta y abajo los datos del mercado obtenidos de la web gs.statcounter.com

Al encontrar muchas similitudes entre los datos obtenidos por los miembros del programa de ingeniería de sistemas y los datos del mercado, se opta por generar una capacitación mostrando a la comunidad cuales son los principales riesgos que se pueden presentar por no tener actualizados de forma correcta y puntual los sistemas operativos de sus dispositivos.

Para esto se toman las vulnerabilidades indexadas durante el último año de la base de datos de vulnerabilidades "The National Vulnerability Database", la cual es mantenida por el Instituto Nacional de Estándares y Tecnología (NIST) [23]. Esta base de datos incluye detalles sobre cada CVE que ha sido emitido. Realiza un seguimiento de su estado, estandarizando un reporte de seguridad de la sobre la vulnerabilidad, para proporcionar la forma de detectar la vulnerabilidad, qué se debe realizar si se detecta, el riesgo asociado y cómo hacer referencia a cada vulnerabilidad.

Para este trabajo se ha generado una serie de estadísticas donde se muestra en tres niveles de riesgos (Bajo, medio y alto) la cantidad de vulnerabilidades detectadas para cada uno de los sistemas operativos usados por los

diferentes miembros del programa de ingeniería de sistemas durante el último año 2016. Además de mostrar el incremento constante en el número de vulnerabilidades. Se les muestran una serie de vulnerabilidades de nivel alto que pueden afectar de forma crítica no solo sus ordenadores, sino los ordenadores de una red, para escoger las principales vulnerabilidades, se accede a la base de datos de vulnerabilidades

4. Conclusiones

- Cada día existen más dispositivos que se pueden conectar a internet, los miembros del programa de ingeniería de sistemas no son ajenos a estas circunstancias y en promedio cada uno se conecta con más de un dispositivo (80% Smartphone, 75% Portátil personal y 9% Tablet) aproximadamente 1,6 dispositivos por integrante.
- El dispositivo predilecto para conectarse por parte de los miembros del programa de ingeniería de sistemas son los Smartphone, más de un 80% de los miembros lo utilizan para conectarse a la red de la universidad.
- Las vulnerabilidades analizadas, con calificación 10 en los diferentes sistemas operativos, generalmente tienen varios efectos y son registradas con diferentes tipos de vulnerabilidades, con lo que el riesgo en mayor, en general pueden ser generadas desde accesos remotos, esto hace que el riesgo sea muy alto.
- El principal factor de riesgo puede estar precisamente, en la combinación Smartphone con sistema operativo Android, por ser el dispositivo más utilizado para conectarse (83%) y ser el sistema operativo con más vulnerabilidades durante el último año con: 10 vulnerabilidades de bajo riesgo, 164, vulnerabilidades de medio riesgo y 349 vulnerabilidades de alto riesgo.
- Si hablamos de portátiles, el sistema operativo con más vulnerabilidades es Linux, sin embargo el con una mayor cantidad de vulnerabilidades de alto riesgo es Mac OS. Para los sistemas operativos Microsoft encontramos una gran cantidad de vulnerabilidades comunes entre las diferentes versiones; y al ser este el sistema más utilizado por los miembros es el que más riesgo genera en la red de la Universidad Cooperativa de Colombia.
- Aunque no se pueda garantizar una seguridad total al conectarse a una red, la educación y conocer sobre los riesgos que generamos siendo el eslabón más débil de la cadena, esto va permitir minimizar este riesgo. Por esta razón es muy importante generar campañas para generar una conciencia de tener el sistema operativo actualizado y también las herramientas de trabajo.

5. Referencias

[1] M. Santos González, “Historia de Internet - Nacimiento y evolución | Redes Telemáticas,” Septiembre 17, 2013. [Online]. Available: http://redestelematicas.com/historia-de-internet-nacimiento-y-evolucion/. [Accessed: 28-Dec-2016].

[2] D. Evans et al., “Internet de las cosas: Cómo la próxima evolución de Internet lo cambia todo,” J. Food Eng., vol. 49, no. Emim, pp. 314–318, 2011.

[3] “Boletín de seguridad Panorama del año . Seguridad estadísticas generales de 2016 Resumen ejecutivo cosas que no sabíamos antes :,” pp. 1–18, 2016.

[4] US-CERT, “Heightened DDoS Threat Posed by Mirai and Other Botnets.” [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA16-288A. [Accessed: 16-Dec-2016].

[5] E. Arcos, “Mirai e internet de las cosas responsables del ataque DDoS de octubre 21.” [Online]. Available: https://hipertextual.com/2016/10/mirai-ddos-internet-de-las-cosas. [Accessed: 16-Dec-2016].

[6] FP_Analyst, “Flashpoint - Mirai Botnet Linked to Dyn DNS DDoS Attacks.” [Online]. Available: https://www.flashpoint-intel.com/mirai-botnet-linked-dyn-dns-ddos-attacks/. [Accessed: 16-Dec-2016].

[7] E. Dans, “Tiempo de DDoS » Enrique Dans,” Enrique Dans, 2010. [Online]. Available: https://www.enriquedans.com/2010/12/tiempo-de-ddos.html. [Accessed: 28-Dec-2016].

[8] T. BBC NEWS, “BBC NEWS | Technology | Sasser net worm affects millions,” BBC NEWS, 2004. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/3682537.stm. [Accessed: 29-Dec-2016].

[9] M. P. C. Microsoft, “Worm: Win32/Sasser.A,” Malware Protection Center, 2007. [Online]. Available: https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Worm%3AWin32%2FSasser.A&753b39b

0-1a28-4269-90a7-1e0a868b281d=True. [Accessed: 29-Dec-2016].

[10] W. Hasselbring and R. Reussner, "Toward Trustworthy Software Systems," Computer (Long. Beach. Calif)., vol. 39, no. 4, pp. 91–92, 2006.

[11] G. O. Gorman and G. McDonald, "Ransomware : A Growing Menace," Symantec, vol. 1, p. 16, 2012.

[12] A. Gazet, "Comparative analysis of various ransomware virii," J. Comput. Virol., vol. 6, no. 1, pp. 77–90, 2010.

[13] T. BBC mundo, "El pueblo de Estados Unidos que pagó un rescate para poder seguir usando sus computadoras - BBC Mundo," BBC, 2015. [Online]. Available: http://www.bbc.com/mundo/noticias/2015/08/150803_tecnologia_eeuu_pueblo_pago_rescate_malware_computadoras_lv.shtml. [Accessed: 29-Dec-2016].

[14] R. BBC Mundo, "El hospital de Estados Unidos secuestrado por piratas informáticos - BBC Mundo," BBC, 2016. [Online]. Available: http://www.bbc.com/mundo/noticias/2016/02/160216_tecnologia_hospital_eeuu_hackers_ransomware_piratas_informaticos_lb. [Accessed: 29-Dec-2016].

[15] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," Proc. SIGCHI Conf. Hum. Factors Comput. Syst. - CHI '06, no. November 2005, p. 581, 2006.

[16] R. BBC Mundo, ""12 ataques por segundo": cuáles son los países de América Latina más amenazados por "malware" - BBC Mundo," BBC, 2016. [Online]. Available: http://www.bbc.com/mundo/noticias-37286420. [Accessed: 29-Dec-2016].

[17] R. BBC Mundo, "Cómo fue el 'hackeo' de piratas informáticos de Rusia durante las elecciones de Estados Unidos - BBC Mundo," BBC, 2016. [Online]. Available: http://www.bbc.com/mundo/noticias-internacional-38350244. [Accessed: 29-Dec-2016].

[18] "Informe de Amenazas a la Seguridad de Internet," 2016.

[19] A. Ivanov, D. Emm, F. Sinitsyn, and S. Pontiroli, "Boletín de seguridad de Kaspersky 2016 . La revolución del ransomware Story of the Year," pp. 1–21, 2016.

[20] Hewlett Packard Enterprise, "HPE Security Research Cyber Risk Report 2016," Febrero 2016, p. 96, 2016.

[21] MinTic, "Cifras Cuarto Trimestre de 2015," pp. 1–44, 2016.

[22] A. M. LUZARDO, "¿Es Colombia un país innovador? • ENTER.CO," enter.co, 2016. [Online]. Available: http://www.enter.co/especiales/claro-negocios/es-colombia-un-pais-innovador/. [Accessed: 29-Dec-2016].

[23] C. Manes, "Most vulnerable operating systems and applications in 2015," 2016. [Online]. Available: http://techtalk.gfi.com/2015s-mvps-the-most-vulnerable-players/. [Accessed: 29-Dec-2016].