Recomendaciones para prevenir ciberataques.

Juan Manuel Alsina Rodríguez
Especialización Seguridad Informática.
Universidad Piloto de Colombia.
Bogotá, Colombia
Juanmanuel.alsina@gmail.com

Abstract - *Cybersecurity is one of the most important aspects to be taken into account when implementing a software solution, which is why the development of this documents some possible vulnerabilities that companies have expressed that although they are known by many not all take measures to prevent them.*
The document recommendations for cyber-attacks and prevent cybercriminals are aware that all companies take no matter their size or economic activity can occur attacked.

Resumen - *La Ciberseguridad es uno de los aspectos más importantes que se debe tener en cuenta al momento de implementar una solución informática, por eso en este documento se expresan algunas vulnerabilidades a los cuales se enfrentan los usuarios de internet y las empresas, que si bien estas vulnerabilidades son conocidas, no todos toman las medidas para prevenirlas.*
Adicionalmente en el documento se realizan recomendaciones para que se prevengan ciberataques de los ciberdelincuentes y se tome conciencia de que todos los usuarios de internet, sin importar su actividad económica, pueden ser atacados.

***Palabras Clave* - Ciberataque, Ciberdefensa, Ciberdelincuente, Ciberseguridad, Cibernético.**

INTRODUCCIÓN.

¿Sabemos que es la ciberseguridad?, ¿podrían ser atacadas las empresas por ciberdelincuentes desde su interior?, ¿están protegidos los usuarios de internet de ataques informáticos?, ¿se pueden prevenir los ciberataques?, estos son algunos de los interrogantes que se responden en el desarrollo de este documento, los cuales podrán ser utilizados para implementar medidas y prevenir posibles ataques informáticos.
Es importante precisar que siempre se podrá ser vulnerable a ciberataques si no se aplican las políticas de seguridad informática adecuadas, sin embargo, se puede llegar a prevenir, minimizar el riesgo y el impacto negativo que los ciberdelincuentes puedan causar aplicando las controles correctos, por lo cual el efecto será haber salvaguardado la información y minimizar las vulnerabilidades en cuanto a la pérdida o robo de la misma.
Se debe tener comprensión que no siempre adquiriendo el *firewall* de la mejor marca, las herramientas tecnológicas más costosas que se encuentren en el mercado o escribiendo el libro de políticas de seguridad más robusto se podrá salvaguardar la información de robo, secuestro o como usuarios de internet seremos menos vulnerables a los ataques de un ciberdelincuente, debemos saber que ellos no siempre se encuentran fuera de las oficinas con un computador y gafas oscuras tratando de ingresar a la red, ellos pueden trabajar en la empresa, llevar corbata y extraer información o pueden planear un ciberataque a la infraestructura tecnológica de la empresa con el fin de robar información o implantar un virus informático.
El gobierno Colombiano ha sumado esfuerzos y ha avanzado creando instituciones y grupos como el Centro Cibernético Policial (CCP) o el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) los cuales se encuentran dedicados a monitorear la red nacional para combatir a estos Ciberdelincuentes e incidencias de seguridad informática.

I.CARACTERÍSTICAS.

Es importante conocer la definición de Ciberseguridad y por qué se encuentra compuesta, esta definición es dada por la Unión Internacional de Telecomunicaciones *ITU-T*[1], quien dice que *"La ciberseguridad es la colección de los instrumentos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques de gestión de riesgos, acciones de formación, las mejores prácticas, de aseguramiento y las tecnologías que se pueden utilizar para proteger el medio ambiente cibernético y la organización y los activos de los usuarios.*
La organización y los activos de los usuarios conectados incluyen dispositivos de informática, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones, y la totalidad de la información transmitida y / o almacenada en el entorno cibernético. La ciberseguridad se esfuerza por garantizar la consecución y el mantenimiento de las propiedades de seguridad de la organización y los activos de los usuarios contra los riesgos de seguridad pertinentes en el entorno cibernético.". Teniendo en cuenta la anterior definición se debe entender que un ciberdelincuente es quien realiza acciones ilegales utilizando una computadora o dispositivo móvil conectados una red

privada o pública para cometer un delito cibernético y atacar todas y cada una de las vulnerabilidades expuestas, la gran compañía desarrolladora de antivirus *Kaspersky lab*[2] encaja a los ciberdelincuentes en cuatro tipos de atacantes como *estudiantes, jóvenes sin experiencia, desarrolladores profesionales e investigadores*.

Ahora bien, ¿será que los usuarios de internet pueden tomar medidas e implementar controles para prevenir ataques de los ciberdelincuentes?, la respuesta es Sí, para aplicar esto los usuarios deben conocer el *modi operandi* de un ciberdelincuente, cuál es el tipo de daño que pueden llegar a causar y como poder llegar a evitarlo.

El primer aspecto que debe tener presente es que todos los usuarios de internet se encuentran expuestos a cualquier tipo de ataque de un delincuente cibernético, en el reporte entregado por el fabricante de antivirus *Symantec*[3] en junio de 2014, los incidentes que más se reportan a nivel nacional son los que involucran a los *Keyloggers* (registradoras de claves), en segundo lugar se encuentra los incidentes de *Spyware* (programa espía que recopila información sin el consentimiento del usuario) y otros programas maliciosos como los *troyanos*, *caballos de Troya y gusanos*, sin embargo, los ataques que más aquejan a los usuarios de internet en Colombia son los que tienen que ver con el *ransomware* (secuestro informático) el cual consiste en impedir el acceso a ficheros con información en una computadora infectada ya que este ejecuta un algoritmo que encripta la información y para poder acceder nuevamente ellos genera un mensaje solicitando que un monto determinado de dinero sea consignado en una cuenta bancaria y poder obtener un código para acceder a los ficheros.

Otro de los ataques más comunes de un ciberdelincuente tiene que ver con el software malicioso *Criptolocker* quien hace algo muy parecido que el *ransomware*, solo que a diferencia del anterior este encripta el disco duro de la computadora infectada y su *modi operandi* es el mismo. El estudio de *Symantec* además revela que la comunidad de usuarios de internet con mayor ataque son las *Pymes*, sin embargo este no deja por fuera a las grandes y medianas empresas, que también son vulnerables a estos tipos ataques ya que no implementan los controles necesarios para prevenir los ataques.

Otro de los ciberataques que se debe tener en cuenta por parte de los usuarios de internet y es considerado como uno de los ciberdelitos que más compromete a las empresas es el *phishing* o suplantación de identidad, en el cual los cibercriminales utilizan las vulnerabilidades que ofrecen los portales corporativos y cuentas de correos electrónicos además de la inocencia de los usuarios para engañar y poder así obtener claves de cuentas bancarias, acceso a cuentas de correo electrónico para posteriormente cometer fraudes.

Según el reporte de *Symantec* generado para Latinoamérica, las industrias que más se ven afectadas por el ciberdelito del *phishing* las podemos observar en la figura 1.

Ahora bien, ¿cómo puede un delincuente cibernético lanzar ataques y alcanzar sus objetivos sin que los usuarios se den por enterados y el daño causado sea casi irreversible?, esto se analizará en el siguiente capítulo.

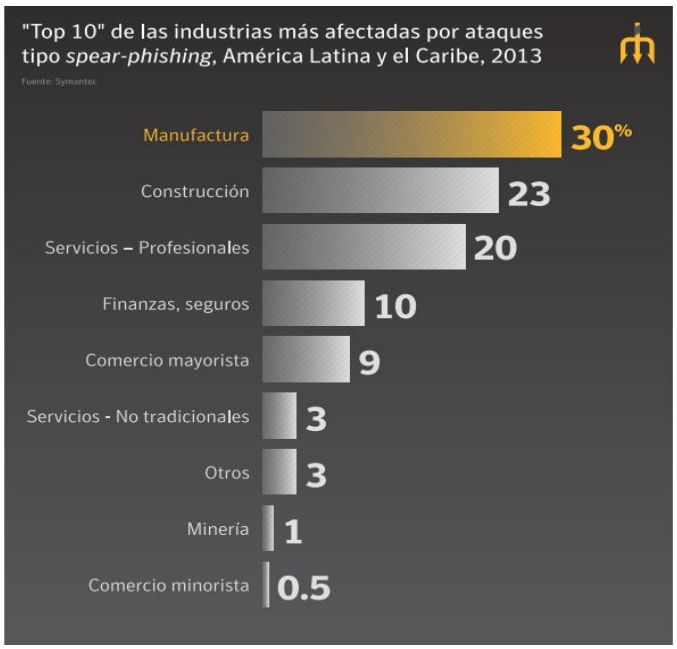

Figura 1. Industrias más afectadas por phishing en L.A
Symantec-Junio de 2014

II. TEORÍA DE UN ATAQUE DE UN CIBERDELINCUENTE.

Una de las formas más sencillas para que un ciberdelincuente puede lograr sus objetivos es transferir un *keylogger* por medio de una usb a la red o a un computador que haya identificado, normalmente el objetivo es el computador que usan los niños para jugar o se encuentra en los rincones de una empresa, el de la secretaria o aun siendo más crítico el computador del vendedor estrella para que este se expanda, capture las contraseñas y luego poder acceder a sus cuentas y obtener información valiosa que podrá ser vendida o usada en contra del usuario como lo muestra la figura 2.

Figura 2. Robo de información mediante infección.
Symantec-Junio de 2014

Otra de las formas más comunes que usa un ciberdelincuente para llevar a cabo sus ataques es mediante el ya conocido método de Denegación de Servicio *DDoS*, el cual consiste en inundar de peticiones de conexión a un servidor objetivo con el fin de que este deje de responder y quede fuera de servicio, este ataque no se realiza desde una o dos computadoras, si no que puede ser ejecutado desde cientos o miles de computadoras a nivel mundial, a estas máquinas se les conoce como *maquinas zombis*, las cuales el atacante previamente ha infectado con un *malware (software malicioso que puede acabar con el correcto funcionamiento de una computadora)* que le permitirá controlarlas y lanzar el ataque a su objetivo así como lo muestra la figura 3.

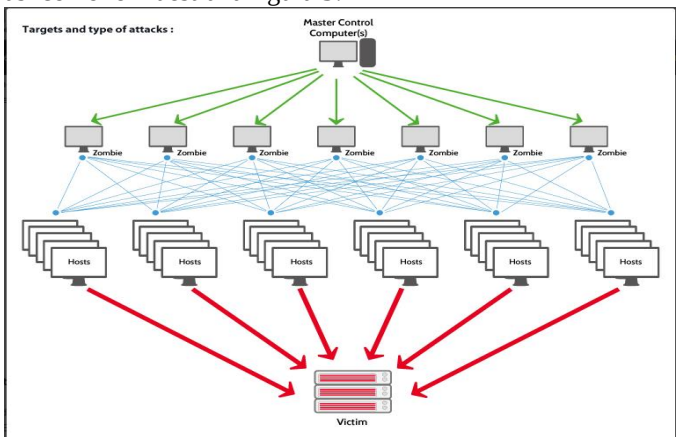

Figura 3. Estructura de ataque de denegación de servicio OVH.com

Según la compañía fabricante de antivirus *Eset*[4] en su más reciente reporte del año 2014, en donde se analizan los incidentes reportados por las compañías de Latinoamérica, se muestra que en primer lugar se encuentran los incidentes que tienen que ver con *malware* el cual se da por infección de las computadoras, en segundo lugar se encuentra el *phishing* que se da por suplantación de identidad para robo de información, en tercer lugar se encuentra la *falta de disponibilidad* que puede darse por un ataque de denegación de servicio a un servidor y en cuarto lugar se encuentra el *fraude interno* el cual es una de las amenazas y ataques preferidos de los cibercriminales que consiste en el robo de información por medio de correos electrónicos, extracción por medios magnéticos como usb y cd de información o por el auto robo de los computadores destinados para el uso del empleado en sus labores diarias.

Estas vulnerabilidades aprovechadas por los ciberdelicuentes también aquejan a las grandes empresas que como se sabe cuentan con todo el recurso financiero y tecnológico pero no realizan las implementaciones de seguridad apropiadas en su infraestructura tecnológica.

A continuación en la figura 4 se muestran las tendencias de ataques cibernéticos y aprovechamiento de las vulnerabilidades por parte de los ciberdelincuentes en *Pymes* y grandes empresas, reporte publicado por la compañía fabricante de antivirus *Eset*.

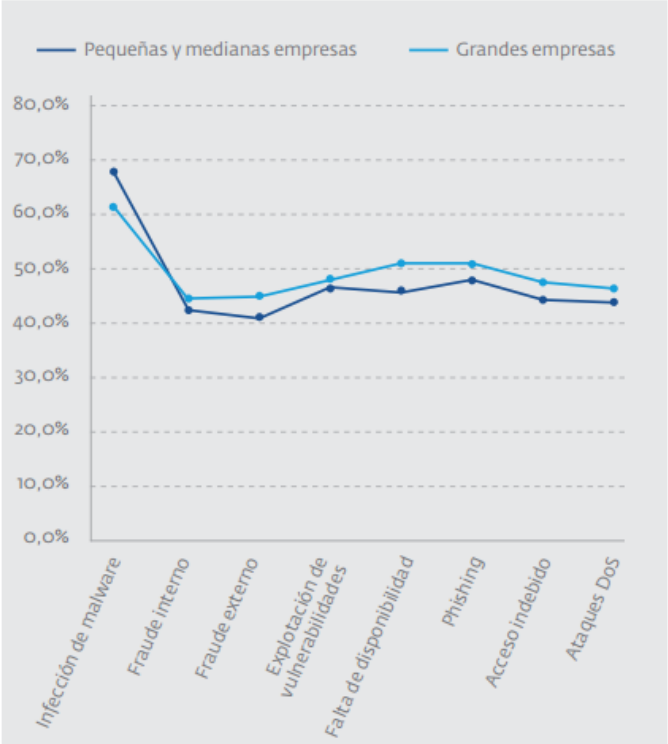

Figura 4. Tendencias de ataques a empresas Reporte Eset - Junio de 2014

En el último año se ha escuchado hablar de Edward Snowden[5] ex agente de seguridad de la Agencia Nacional de Seguridad de Estados Unidos NSA[6], quien ha sido acusado de espionaje, robo y otros cargos más por filtrar información confidencial a agencias de seguridad de diferentes países y publicar en internet y en diferentes medios información de cómo, a que empresas y que personas *EEUU* vigila.

Lo que realizo Snowden, que es censurable, fue tomar información confidencial como procesos, investigaciones a figuras públicas, grabaciones, documentaciones y hacerlas públicas lo cual es lo mismo que una persona tome información que no le pertenece como una base de datos clientes, estados financieros, la forma en que se desarrollan productos, fotos privadas y las entregue o publique a cambio de dinero o de nada.

Como se puede observar, las grandes agencias de seguridad nacional tampoco pueden protegerse de los ciberdelicuentes y proteger todas las vulnerabilidades, pero lo que si podrán es tomar medidas para minimizar el riesgo de fuga de información sin que la implementación de controles de seguridad sea un obstáculo y más que un gasto se proyecte como una inversión.

III. RECOMENDACIONES PARA IMPLEMENTAR LA CIBERSEGURIDAD Y PROTEGERSE DE LOS CIBERDELINCUENTES.

En Colombia la mayoría de las usuarios de internet y empresas no se encuentran preparados para salvaguardar la información de los ciberdelincuentes, por ese motivo se realizan algunas recomendaciones para que sean tenidas en cuenta al momento de realizar la implementación de la ciberseguridad.

En el reporte de seguridad de la fabricante de antivirus *Eset* se indica que la mayoría de las empresas y usuarios de internet en lo primero que piensan al momento de implementar medidas de seguridad es en un antivirus, en segundo lugar tenemos un firewall y en tercer lugar un backup de la información así como se observa en la figura 5.

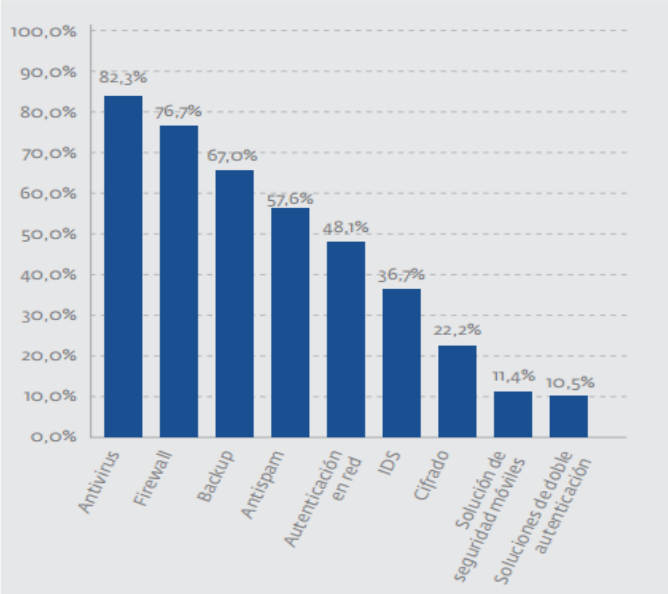

Figura 5. Implementaciones de controles
Reporte Eset - Junio de 2014

La primera recomendación es que se realice un listado de las necesidades y activos que se requieren proteger, con esta tarea se podrá generar un listado de posibles vulnerabilidades y elaborar las políticas de seguridad que se implementaran, recuerde "*que la seguridad no se convierta en el palo en la rueda de su negocio*", Esto ayudará, apalancará y generará confianza de todos los usuarios, clientes, empleados e inversionistas. Se recomienda que las políticas creadas sean avaladas por todos los interesados, hacerlos partícipe en la construcción y lo más importante, realizar la evangelización de las políticas a de todos los usuarios.

La segunda recomendación es *mantener actualizado los sistemas* con las versiones disponibles publicadas por los fabricantes, se recomienda que estas sean ejecutadas de manera inmediata y escalonada para evitar que alguna dañe el normal funcionamiento de las plataformas informáticas, con estas actualizaciones se podrá evitar que los ciberdelincuentes generen ciberataques a vulnerabilidades conocidas las cuales no se corrijan con las actualizaciones y les permitan lograr su objetivo, adicionalmente es indispensable que los antivirus se encuentren activos en cada una de las computadoras y servidores ya que así se podrá minimizar la entrada de *malware* a la red y prevenir el robo de información.

La siguiente recomendación es *sensibilizar a los usuarios de una navegación segura en internet*, si bien se puede controlar a que grupos y categorías de páginas web pueden navegar los usuarios no todos toman las precauciones debidas y algunos toman el riesgo de acceder a páginas no seguras o prohibidas, las cuales pueden contener código malicioso como *malware* en su código fuente y este podría ejecutarse en la computadora logrando así una infección a toda la red, además existe el riesgo de que alguna página web visitada contenga lo que se conoce como *defacement* (cambio producido intencionadamente por un ciberdelincuente a la interfaz de una página web) y los usuarios sean víctimas de *phishing* para robar nombres, claves de bancos u otras importantes cuentas que contenga información valiosa.

Otra de las recomendaciones es *proteger la Red de wifi o infraestructura física* de usuarios fraudulentos, muchos de los usuarios tienen la cultura de llevar sus dispositivos móviles (Smartphone, Tablet, Ipad, etc.) a las empresas y conectarlos a la red *wifi*, lo que se conoce como *BYOD (trae tu propio dispositivo)*, con el pretexto de utilizarlo para sus labores. Esta es una de las vulnerabilidades más exitosas que explotan los ciberdelicuentes ya que hasta el día de hoy se han detectado más de 143 mil virus para móviles así como nos lo hace saber la empresa especializada *Viruslist.com[7]* quien en su reporte anual de 2014 nos indica que el 98% de los virus existentes para móviles se encuentran para dispositivos con sistema operativo *android* como se observa en la figura 6, lo que hace suponer que a muchas empresas y usuarios de internet los ciberataques los están realizando desde sus propias instalaciones y utilizando su propia red, para lo cual se aconseja separar la red Wifi y ofrecerles otra posibilidad de conexión para sus dispositivos.

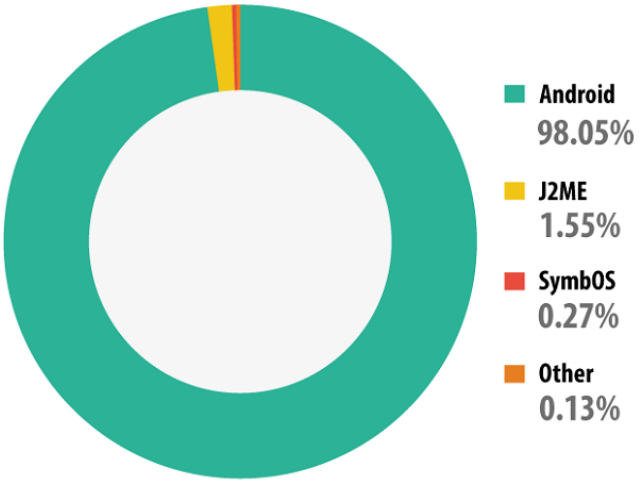

Figura 6. Distribución Virus para plataformas móviles
Reporte viruslits.com - Febrero de 2014

La recomendación general que se realiza es se pueda proteger la infraestructura tecnológica, que todos los esfuerzos se encuentren encaminados a cuidar lo más preciado para los usuarios y las empresas, La Información, para ello se puede iniciar por revisar en el mercado un antivirus, escoger uno que le brinde seguridad según se requiera, instalar un Firewall que le permita proteger la red de la navegación en internet de los usuarios y de ataques de ciberdelincuentes, implementar políticas de seguridad, realizar actualizaciones de los sistemas operativos rutinariamente con el fin de evitar vulnerabilidades y que estas sean aprovechadas por los atacantes, concientizar a todos los empleados que *la ciberdelincuencia no es un juego*,

es una amenaza en la cual todos estamos involucrados y pueden ser víctimas de los ciberdelincuentes, crear mejores prácticas de aseguramiento de las plataformas tecnológicas y del entorno informático, además de unir esfuerzos de todas las partes para mejorar y proteger los activos.

IV. CONCLUSIONES

- En la investigación realizada se observa que las empresas y usuarios de internet no están preparados para resistir ataques a las vulnerabilidades detectadas por los ciberdelincuentes debido a que no están realizando las mejores prácticas de implementación de las políticas de seguridad.
- La ciberseguridad en las empresas y en los usuarios de internet ha avanzado en los últimos años, pero así como se han adoptado medidas, los delincuentes cibernéticos cada día evolucionan descubriendo nuevas vulnerabilidades del entorno cibernético de las empresas y usuarios para lograr su objetivo.
- Se deben crear para las empresas y usuarios de internet políticas que permitan la conexión segura de dispositivos móviles a la red wifi, ya que tanto empleados como usuarios no son conscientes que estos dispositivos son altamente peligrosos y pueden poner en riesgo la seguridad de la información.

V. REFERENCIAS

1] ITU-T telecommunication standardization sector of itu. v. x.1205 04-2008, disponible en http://handle.itu.int/11.1002/1000/9136-en?locatt=format:pdf&auth , cybersecurity , pp 2, April 2008.

2] Kaspersky lab - Cibedelincuencia, disponible en http://www.kaspersky.es/internet-security-center/threats/computer-vandalism

3] Symantec - reports on cyber vulnerabilities in the Americas - disponible en http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf , Página 46-49, 3 de Juny de 2014

4] Eset - Reporte de seguridad para Latinoamérica 2014, disponible en http://www.welivesecurity.com/wp-content/uploads/2014/06/informe_esr14.pdf , pp 4, junio de 2014.

5] Edward Snowden, disponible en http://es.wikipedia.org/wiki/Edward_Snowden

6] National Security Agency - disponible en https://www.nsa.gov/

7] Viruslist - amenazas para dispositivos móviles en 2013, disponible en http://www.viruslist.com/sp/analysis?pubid=207271246 , feb 2 2014.

8] Microsoft - The Link between Pirated Software and Cybersecurity Breaches , disponible en http://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf

9] CCIT - Cámara Colombiana de Informática y Telecomunicaciones , disponible en http://www.ccit.org.co/

10] ColCERT- Grupo de Respuesta a Emergencias Cibernéticas de Colombia, disponible en http://www.colcert.gov.co/

11] Centro Cibernético Policial - CCP, disponible en http://www.ccp.gov.co/ciberseguridad.php 24 de april de 2013

12] Red Iberoamericana de Protección de Datos - RedIPD, disponible en http://www.redipd.org/

13] Trendmicro - las pequeñas empresas son el negocio de la ciberdelincuencia , disponible en http://www.trendmicro.es/media/misc/small-business-is-big-business-in-cybercrime-es.pdf