MEDIOS SOCIALES. UNA PERSPECTIVA DE RIESGO Y RESPONSABILIDAD

Deivy Arley Torres Carreño

RESUMEN

El siguiente análisis se enfoca en determinar la perspectiva que tienen las empresas acerca de los medios sociales, cómo estos se han convertido en un elemento estratégico del *marketing* a la vez que se han generado riesgos informáticos ligados a la responsabilidad por los contenidos que se publican y la interacción con los grupos de interés. Incluye el panorama de las empresas colombianas con respecto al comercio electrónico y el *ranking* de las marcas con mayor posición en el mercado.

Las redes sociales apalancan las unidades de negocio de las empresas, ofreciendo productos y servicios por medio de tecnologías informáticas a fin de obtener ventajas competitivas; tales tecnologías generan como valor agregado la fidelización del cliente con las marcas por medio de la publicación de información pertinente y de interés, y abren espacios donde la opinión del cliente es de importancia para el negocio.

Se dan a conocer los riesgos informáticos asociados con las redes sociales, las tendencias criminales para vulnerar la seguridad de las plataformas tecnológicas de una organización, la responsabilidad social y algunas recomendaciones que se deben tener en cuenta en la adopción de estas redes. Se menciona, a manera de reflexión, la responsabilidad ética y legal que las organizaciones y las personas tienen en las redes sociales, en el conocimiento de toda la información sensible de cada persona y grupo de interés.

Palabras clave: Medios sociales, seguridad de la información, *software* malicioso, riesgos informáticos, amenazas.

ABSTRACT

This analysis is focused in determine the approach that firms have about social media, how these media have converted in an element for the strategy of marketing, and at the same time, they have generated information risks attached to the responsibility for the published contents and also the interaction with stakeholders. It includes the Colombian companies' panorama about the e-commerce, and the ranking of the brands better positioned in the market.

Social media empower business units of enterprises, offering products and services through informatics technologies, in order to obtain competitive advantages; those technologies generate, as added value, customer loyalty with the brands by meaning of information published, in terms of relevance and interest, opening spaces where the customer's opinion has importance for the business.

It shows the informatics risks associated to social media, the criminal trends for infringe the security of technological platforms within an organization, the social responsibility and some recommendations for networks adoption. It mentions as a consideration mode, the ethical and legal responsibility that organizations and the persons have in the social networks, knowing sensible information of every person and stakeholder.

Keywords: Social media, information security, malware, information risks, threats.

I. INTRODUCCIÓN

Las interacciones sociales han tenido un gran crecimiento e impacto en diversos ámbitos durante los últimos años, llegando cada vez a más personas por medio de las diferentes herramientas y dispositivos tecnológicos informáticos. Las empresas en búsqueda de nuevas estrategias de mercadeo encuentran en las redes sociales la oportunidad de obtener ventajas competitivas para ofrecer y comercializar productos y servicios enfocados en un concepto innovador: el cliente digital, el cual se inclina por aquellas empresas que tienen información disponible y actualizada en sitios web, las cuales generen mayor confianza. Las redes sociales pueden convertirse en aliadas que aprovechan la conexión masiva de usuarios, con la posibilidad de conocer sus preferencias de consumo y formas de adquisición.

Sin embargo, las redes sociales representan una amenaza potencial para las organizaciones, puesto que existe la probabilidad de fuga de información sensible o el ingreso de *software* malicioso (o *malware,* por sus siglas en inglés) a la red corporativa, que puede poner en riesgo no solo la seguridad de la información, sino, a la vez, generar implicaciones legales y pérdida de confianza por parte del cliente. Por tales razones, se deben evaluar las diferentes amenazas asociadas con las herramientas y los dispositivos tecnológicos informáticos e implementar los controles necesarios que ayuden a mitigar el impacto de tales amenazas.

Las empresas deben considerar una relación entre el mundo físico y el digital a fin de ofertar productos o servicios en instalaciones físicas y mantener una presencia activa en las redes sociales, pues es aquí donde se encuentran muchos de sus clientes potenciales. La estrategia básica en las redes sociales consiste en publicar anuncios que capten el interés o la curiosidad del público; pero, adicionalmente, las empresas impulsan nuevos productos o servicios, afianzan las relaciones con sus clientes, anuncian descuentos, promociones y posicionan sus marcas en la mente del consumidor. Facebook es una de estas redes sociales que en Bogotá cuenta con el mayor número de personas registradas en Colombia, como se observa en la tabla 1, en la se enumeran las principales ciudades y la cantidad de personas activas en el año 2015.

Tabla 1. Ciudades con más usuarios registrados en Facebook en Colombia

Bogotá	6.800.000
Medellín	2.500.000
Cali	1.600.000
Barranquilla	1.200.000
Bucaramanga	730.000

Fuente: Abad (2015).

En cuanto al uso de las redes sociales en el interior de las empresas, se evalúa el tiempo "muerto" de los empleados que las utilizan, lo cual impacta en la productividad y el rendimiento de la empresa. Algunos estudios indican que el 45 % del tiempo productivo de los empleados se desperdicia en redes sociales como Facebook y YouTube (SANS Institute, 2011a), razón por la cual en las empresas se restringe el uso e ingreso a estos y otros sitios.

El estilo de vida actual impone la necesidad de estar siempre conectados, gran parte del tiempo por medio de diferentes aplicaciones móviles que permiten comunicación e interacción *online*, con los riesgos inherentes de una red pública. La descarga e instalación de aplicaciones desde sitios web no confiables, la aceptación de perfiles llamativos de hombres o mujeres en redes sociales, la visita a enlaces que promueven un artículo o noticia que capte la atención, las cadenas de correos o mensajes que incentivan a compartirlos o a sumarles un *like* e incluso la descarga de fotos o la reproducción de videos que puedan parecer inofensivos forman parte de las fuentes de riesgos informáticos.

En este contexto surge la ingeniería social, definida por Romero y Sorzano (2016) como "un método de persuasión o de engaño para que las personas, sin darse cuenta, sean afectadas con el simple hecho de compartir datos vitales con un desconocido"; de esta forma, un atacante cibernético puede acceder a la información y dejarla expuesta para que sea alterada, eliminada, sustraída o secuestrada.

II. PANORAMA: MERCADEO DIGITAL EN LAS EMPRESAS COLOMBIANAS

En Colombia, muchas de las grandes empresas han apalancado sus unidades de negocio por medio de las redes sociales y han generado un factor diferenciador en el mercado. Según un estudio

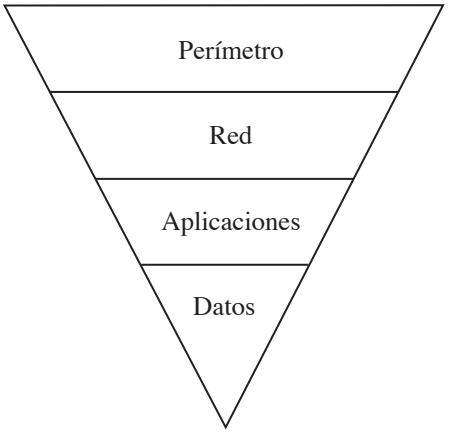
realizado en 2013, en Colombia, en los últimos doce meses, el 52 % de las personas encuestadas efectuó compras *online* (The Cocktail Analysis, 2013), lo que representa una participación considerable del comercio electrónico. Otro estudio realizado en 2013 indicó que el 27.1 % de las mipymes colombianas usa las redes sociales como apoyo para mantener contacto con los clientes y buscar nuevos (Corporación Colombia Digital, 2013). Esto resulta favorable al momento de incrementar las ventas y la satisfacción por parte del cliente, además, genera la capacidad de conocer patrones de consumo, gustos, preferencia de marcas e incluso la tendencia a referenciarlas con otros contactos.

El denominado *marketing* digital explota el conjunto de tecnologías de la información y las comunicaciones para posicionar una marca personal o empresarial en el mercado usando como canal de comunicación las diferentes redes sociales. Según una publicación de la revista *Dinero* (2015), en Colombia, "las primeras cinco marcas se ubican en un rango entre 55 % y 70 %: Movistar lidera el *ranking* con 68 %; Bancolombia, con 61 %; Avianca, 59 %; Claro, 55 % y cerveza Águila, 55 %". De lo anterior se deduce que cada vez más las empresas participan y compiten para llegar al cliente, de manera que su interacción y opinión son relevantes en pro del buen servicio y la mejora continua.

III. ENFOQUE DE INVERSIÓN EN SEGURIDAD INFORMÁTICA

De acuerdo con el estudio de Kuper (2005), las inversiones que las organizaciones ejecutan en seguridad de la información se focalizan en el perímetro, seguido de la red, las aplicaciones y, por último, los datos.

Figura 1. Inversión en seguridad de la información



Fuente: Kuper (2005).

Tomando como referencia la figura 1, las inversiones en seguridad informática en el contexto colombiano se concentran principalmente en el perímetro, donde se encuentran mecanismos de seguridad tales como antivirus, *firewalls*, *antispam*, IPS (*Intrusion Prevention System*), entre otros. Por lo general, la alta gerencia, al realizar dichas inversiones, asume que es suficiente con la protección de la red y los datos. Enseguida se encuentra la red, a la cual se presta poca atención, puesto que se trata de *software* especializado para el control de paquetes de datos en la red o la detección de intrusos, que generalmente son herramientas de alto costo. El siguiente componente se refiere a las aplicaciones, las cuales sí son desarrolladas *in house* o a la medida

del negocio por parte de un proveedor; no suelen considerar el esquema de seguridad como parte de los requisitos, aspecto transversal que debería estar presente en todo el ciclo de desarrollo de *software*. Por último, se encuentran los datos disponibles para el usuario final: estos son el objetivo de los ataques con los cuales se accede a la información al sobrepasar todos los mecanismos de seguridad antes mencionados.

Si bien es importante asegurar toda la infraestructura tecnológica, no se pueden dejar a un lado la sensibilización y el uso de buenas prácticas relacionadas con los diferentes riesgos informáticos a los cuales el usuario puede estar expuesto. Según Cano (2013):

> (…) será mejor que prevalezca la esencia del aseguramiento de la información y no las modas y procesos evolutivos de la tecnología, que, si bien son necesarios y claves para el desarrollo de las estrategias de protección, nunca reemplazarán al eslabón más débil de la cadena y el fin último de la seguridad: la gente.

IV. TÉCNICAS DE ATAQUE

Un delincuente cibernético puede usar diferentes técnicas para violar la seguridad de la empresa, entre las cuales se tienen las siguientes: *malware*, *phishing*, *ransomware*, *e-mail spoofing*, *baiting*, *dumpster diving*, entre otras. Su objetivo es tener acceso a la información privada y restringida de la organización o de los empleados, por lo que se requiere implementar políticas de uso y acceso, controles técnicos, talleres de sensibilización, métricas y seguimiento que permitan contribuir al control de los riesgos en redes sociales. Las técnicas mencionadas se definen a continuación en términos generales:

- *Malware*. Un atacante crea un código malicioso que es difundido por medio de un correo electrónico, una fotografía, un video, entre otros. Al momento en que la víctima lo descarga o lo abre, el equipo de cómputo o el dispositivo móvil se infecta.

- *Phishing*. Es una técnica utilizada por un atacante para suplantar la identidad, por lo general, de un sitio web. El atacante envía a la víctima un correo electrónico para que abra un enlace que lo lleva a un sitio web "conocido" para este. Una vez la víctima llega al sitio malicioso, encuentra una interfaz gráfica idéntica a la real y que a su vez lo lleva a diligenciar información sensible que el atacante obtiene de forma fraudulenta.

- *Ransomware*. Esta técnica permite a un delincuente cibernético secuestrar información de la víctima para luego solicitar dinero por su recuperación.

- *E-mail spoofing*. Es una técnica que consiste es suplantar la cuenta de correo electrónico de una persona. A la víctima que recibe el correo, este le parece un correo real, lo que puede conducirla a responderlo y enviar la información que se solicita en él.

- *Baiting*. El atacante deja una memoria USB o disco compacto "olvidado" al alcance de la víctima con el fin

de que ella lo pueda abrir y de esta manera se instale algún *malware* que comprometa la seguridad de la información.

– *Dumpster diving*. Esta técnica es utilizada para buscar entre la basura todo tipo de información física (en especial áreas de contabilidad, gestión humana, tesorería, facturación) que pueda servir al atacante para recolectar datos que le ayuden a cometer algún acto ilícito o fraudulento.

V. MEDIOS SOCIALES, UN RIESGO INHERENTE

Al identificar los riesgos informáticos en los medios sociales, se determinan también los activos de la organización que deben ser protegidos, con el fin de analizar las amenazas asociadas; estas pueden ser causadas por personas internas o externas a la compañía y pueden poner en riesgo la reputación y la pérdida de información. El impacto de un riesgo puede ser abordado con medidas para su mitigación, transferencia, aceptación o evitación, asimismo mediante su combinación. Al riesgo remanente después de ser mitigado o transferido se le conoce como "riesgo inherente", y es el que puede ser aceptado por la organización. Una encuesta realizada en 2013 indicó que en el 63 % de las empresas, el uso de redes sociales pone en riesgo la seguridad de la información, mientras que el 29 % dice tener controles para mitigar y reducir tal riesgo (SANS Institute, 2011b).

Sin embargo, el riesgo de una red social pública también puede afectar directamente al cliente o usuario que forme parte de esta, pues se están compartiendo datos e información sensible, de manera que la organización es la encargada de asegurar las diferentes restricciones de acceso a que haya lugar. Lo anterior lleva a concluir que los medios sociales no solo se pueden utilizar para desarrollar estrategias de *marketing*, sino que existe una responsabilidad ética y legal por parte de los administradores en medios sociales, conducente a proteger la invasión de la privacidad de cada persona.

Según Cano (2015), "las áreas de seguridad de la información no solamente deberán entender la dinámica de los negocios y condiciones geopolíticas emergentes, sino la evolución y monitoreo de las tendencias en las comunidades emergentes en Internet". Por tal razón, se requiere entender que los riesgos son evolutivos y cada vez más complejos y difíciles de comprender. Los atacantes cibernéticos saben y entienden que cualquier brecha de seguridad es la puerta para el acceso a la información de la organización, de los empleados o quizás de sus clientes.

Al diseñar una matriz de riesgos que considere los diferentes medios sociales, se pueden establecer los diversos escenarios de riesgos, teniendo como objeto diseñar medidas preventivas y de control que ayuden a disminuir el impacto de la materialización de un riesgo sin que se incurra en penalidades económicas, sanciones legales o daño de imagen corporativa por la no adopción, implementación y seguimiento.

VI. SEGURIDAD EN MEDIOS SOCIALES

Los medios sociales enfrentan nuevos retos y problemas relacionados con la protección de los datos de los usuarios y el manejo de sus servicios. Uno de los problemas es la suplantación de identidad, la cual tiene como finalidad propagar mensajes, imágenes o videos que incluyen enlaces a páginas maliciosas que descarguen algún tipo de virus. De igual forma, la suplantación de identidad en los medios sociales se puede utilizar para desprestigiar la imagen de una persona o empresa por medio del envío o la publicación de mensajes falsos. Por último, exigir dinero con la amenaza de publicar contenidos difamatorios o eliminar todos los contactos es una tendencia moderna conocida también como *ransomware*[1].

Otro problema lo constituyen los mensajes de *spam* (mensajes de publicidad no solicitada), los cuales son usados por atacantes cibernéticos para enviar contenidos de tipo comercial en los muros digitales y mensajería instantánea de los usuarios. Según Gómez y Otero (2011), "el *spam* está siendo perseguido en muchos países por los perjuicios que ocasiona tanto a los usuarios como a las empresas dentro de los distintos servicios de Internet…". Este tipo de amenaza es más difícil de controlar, pues en el momento en que se dispara un *spam*, este puede tener alcance a miles e incluso millones de usuarios, que se verán afectados por la instalación de aplicaciones dañinas en los dispositivos tecnológicos en los cuales se está ingresando.

En muchas organizaciones aún existe desconfianza en las redes sociales por el hecho de ser públicas e intercambiar datos sin mayores controles. Esto resulta preocupante, ya que puede ser la puerta para la fuga de información privada, sensible o confidencial del negocio o de los empleados, o también puede ser el medio por el cual se pueda propagar algún tipo de código malicioso que ponga en riesgo la seguridad de la información. Por lo anterior, las áreas de gestión de tecnología deben tomar medidas e instaurar controles de seguridad para evitar que cualquier acción vulnere la protección de la red y de los datos.

En consecuencia, las empresas que adopten el uso de algún medio social deben tener presentes medidas de control que permitan asegurar una protección adecuada contra actos delictivos. La independización de un conjunto de computadores que operan como servidores de redes sociales con respecto a los que procesan, almacenan y transfieren información del negocio es un blindaje ante un atacante informático. Las correctas configuraciones de seguridad y privacidad que tienen las plataformas de redes sociales es otra forma de salvaguardar datos personales que se comparten en los diferentes perfiles

1 https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

de los usuarios. Existen herramientas que ayudan a proteger el uso de redes sociales como Facebook, una de ellas es *Websense Defecio*, que se instala en el perfil del usuario con el objetivo de protegerlo de *spam*, contenidos maliciosos o intentos de secuestros de la cuenta.

Definir políticas en el uso y manejo en redes sociales[2] es otro control que debe estar en la agenda y en las competencias de los administradores de las plataformas de redes sociales, pues por medio de ellas se establecen los comportamientos que están permitidos y prohibidos. Por otra parte, la actuación improvisada, negligente e imprudente en el manejo de información que se comparte o difunde puede ocasionar sanciones a las organizaciones y a los profesionales responsables de la seguridad informática.

VII. RESPONSABILIDAD SOCIAL EN REDES SOCIALES

La naturaleza del hombre supone la habilidad de comunicarse con otros, y las redes sociales son un medio contemporáneo para esto. Como su nombre lo indica, mediante una red social se establecen y desarrollan relaciones con diferentes personas, así que es posible abordar temas varios, como amistad, política, comercio, religión y deportes, entre otros. Las redes sociales permiten que el usuario pueda ocultar su verdadera identidad, de manera que la persona puede expresar libremente emociones, sentimientos y pensamientos sin pudor ni temor a la censura o la crítica pública.

Este es un comportamiento muy usual en la sociedad, pues cada vez son más comunes el aislamiento, el individualismo y la soledad, y las redes sociales se convierten en el refugio para este fenómeno social, que satisface las necesidades de interactuar con otras personas de diferentes culturas, costumbres y maneras de pensar sin darse a conocer físicamente. También es usual que personas creen perfiles y hagan uso de fotografías falsas para obtener datos de otras personas, lo que representa un peligro, dado que es normal el compartir fotos, videos e información privada que luego pueden ser usados con fines ilícitos e incluso extorsivos.

El surgimiento de los medios sociales es reciente y su crecimiento ha sido gigantesco en los últimos años. Tal como indica Del Prado (2014), cerca del 90 % de la población conoce hasta cuatro redes sociales, 70 % participa al menos en una red social; de la población con acceso a Internet, 20 % es miembro de una red social y un usuario medio consulta su red social al menos dos veces al día. Dichas cifras resultan considerables para aquellos que se especializan en crear, divulgar o compartir contenidos que puedan captar el interés e incluso la curiosidad de las personas. Pero, más allá de todo lo anterior, surgen preguntas como estas: ¿qué responsabilidad social

2 http://socialmediagovernance.com/policies/

tienen las organizaciones con relación a los medios sociales?, ¿qué parte de esa responsabilidad se tiene como individuo?, ¿cuál es el papel de la ética en una red social? Estas y otras preguntas surgen y deben ser respondidas a la luz del conocimiento y la apropiación pertinente ante las implicaciones que estos medios tienen en la sociedad.

Los llamados *community managers* son las personas encargadas de administrar contenidos digitales en toda red social que las organizaciones utilicen para cumplir con el plan de *marketing online* y tener contacto con sus grupos de interés. Por otro lado, se encuentran los *social media strategists*, que, como los define Martínez (2012), "ponen en práctica metodologías de trabajo que facilitan la creación de planes estratégicos y tácticos en medios sociales". Estas personas no solo tienen una finalidad comercial, sino además una responsabilidad social respecto al manejo de la información y la influencia en el consumidor, la cual debe estar dentro de parámetros y directrices que respeten ideologías políticas, creencias religiosas, tendencias sociales, aspectos económicos, sociales y culturales.

Se podría pensar que el papel de un *community manager* es una tarea fácil, pues el estar conectado a Internet todo el tiempo pareciera algo sencillo, pero esto no es así, dado que una situación de crisis puede surgir en cualquier momento, teniendo en cuenta que en las redes sociales no existen horarios. En cuanto al perfil profesional, no siempre deben ser periodistas o comunicadores sociales, solo se requiere tener capacidad de gestionar contenidos y manejar una comunicación clara y objetiva. Otro aspecto que se debe tener en cuenta es el conocimiento de instrumentos para la creación de contenidos multimedia y el gusto por trabajar *online*, pues se requiere paciencia y tolerancia ante comentarios que causen algún tipo de malestar. Así mismo, todo lo anterior debe estar alineado con la misión y la visión de la empresa, puesto que no se pueden desviar del plan de *marketing*, la estrategia y los objetivos de negocio.

Parte de las respuestas a las preguntas antes mencionadas compromete la responsabilidad de las organizaciones en cuanto a la veracidad y el contenido de la información que publiquen, dado que, aparte de cumplir un objetivo comercial, también envían mensajes a las personas, mensajes que pueden ser favorables o desfavorables, e incluso se pueden herir susceptibilidades o generar controversia social. Del mismo modo, cada persona tiene una responsabilidad, pues en las redes sociales se debe mantener un lenguaje y comportamiento adecuados, ya que son espacios donde se encuentran muchas personas, y se debe tener un respeto a todas.

VIII. CONCLUSIONES

Los medios sociales pueden ayudar a crear ventajas competitivas en las organizaciones y generar valor agregado para sus clientes. Sin embargo, deben existir los mecanismos de seguridad necesarios para garantizar la integridad de la información como activo de la organización, de manera que se minimice su exposición a ataques cibernéticos y

se evite la fuga de información desde el interior de la empresa. Se deben implementar procesos integrales de gestión de los riesgos informáticos, que han de incluir actividades de monitoreo, identificación, valoración, definición de medidas preventivas y correctivas e incorporación de buenas prácticas de seguridad informática, considerando la oportunidad que las organizaciones tienen para utilizar las redes sociales, buscando un equilibrio entre el riesgo y el beneficio que representa el participar en dichas redes.

La responsabilidad de los administradores en redes sociales es muy amplia, puesto que estas personas conocen información sensible de cada uno de los contactos agregados, información que no puede ser utilizada para fines diferentes de los comerciales, pues esto traería implicaciones y sanciones tanto legales como éticas. Del mismo modo, la protección y la seguridad que se deben implementar en los equipos de cómputo dedicados a la administración y la gestión de medios sociales deben garantizar la privacidad de los datos de cada contacto, dado que, si un delincuente cibernético quiere atacar las redes sociales de una organización, podrá acceder a la información y utilizarla con fines delictivos e incluso criminales.

Para finalizar, se debe aprovechar la potencia de comunicación que ofrecen las redes sociales, ya que son medios de divulgación de información de manera casi instantánea (por medio de texto, fotos, imágenes, videos), que puede llegar a millones de personas en todo el planeta, sin olvidar que cada persona debe ser responsable de lo que publica y comparte con otras personas.

LISTA DE REFERENCIAS

Abad, D. (2015). *Estadísticas de Facebook y Twitter en Colombia (2015)*. Recuperado de goo.gl/ZD0iYS

Cano, J. (2013). *Inseguridad de la información: una visión estratégica*. Bogotá, Colombia: Editorial Alfaomega.

_____. (2015). *El CISO y sus competencias sociales*. Recuperado de https://www.linkedin.com/pulse/el-ciso-y-sus-competencias-sociales-jeimy-cano-ph-d-cfe

Corporación Colombia Digital. (2013). *Encuesta revela que 60.6 % de las mipymes colombianas están conectadas a Internet*. Recuperado de goo.gl/Mk0hgj

Del Prado, R. (Coord.). (2014). Ética y redes sociales. México: Editorial Tirant Humanidades México.

Gómez, A. y Otero, C. (2011). *Redes sociales en la empresa. La revolución e impacto a nivel empresarial y profesional*. Madrid: RA-MA. Recuperado de goo.gl/78kIMS

Kuper, P. (2005). The estate of security. *IEEE Security & Privacy, 3*(5). Recuperado de goo.gl/2H6VuK

Martínez, C. (Coord.). (2012). *Quiero ser community manager: 10 profesionales y 5 compañías analizan una nueva realidad*. Madrid, España: Editorial ESIC.

Revista Dinero. (2015). Las empresas estrella de las redes sociales en Colombia. *Dinero*. Recuperado de Recuperado de goo.gl/rah8KL

Romero, J. y Sorzano, M. (2016). El arte de la ingeniería social. *Aplicatec, 6*(1), Recuperado de goo.gl/Ydb3n0

SANS Institute. (2011a). *Risk assessment of Social Media*. Recuperado de goo.gl/DNnuzI

SANS Institute. (2011b). *Reducing the risks of Social Media to your organization*. Recuperado de goo.gl/eJOVHS

The Cocktail Analysis. (2013). *Las compras online en Colombia*. Recuperado de goo.gl/yaFllv