Seguridad informática para community managers

Lesmes, Lorena Diana

2013

Cod. 1521/2013

Universidad de Buenos Aires
Facultad de Ciencias Económicas

UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS ECONÓMICAS

SECRETARÍA DE POSGRADO
CARRERA DE ESPECIALIZACIÓN EN DIRECCIÓN Y GESTIÓN DE MARKETING Y ESTRATEGIA COMPETITIVA

TRABAJO FINAL

"SEGURIDAD INFORMÁTICA PARA COMMUNITY MANAGERS"
GUÍA PARA LA PROTECCIÓN DE LA REPUTACIÓN EN REDES SOCIALES

Diana Lorena Lesmes
Cursante

Daniela Buján
Tutora de Trabajo Final

2013

DECLARACIÓN DE ORIGINALIDAD

"Declaro que el presente documento, así como el previo plan de trabajo son de mi exclusiva y original elaboración y no lo he presentado de manera total o parcial en ninguna otra ocasión. Este escrito contendrá citas y referencias de terceros que serán debidamente señaladas a lo largo del mismo."

Diana Lorena Lesmes Buitrago
DNI. 94074133

Junio de 2013

INDICE

INTRODUCCIÓN: ANTECEDENTES

INTERNET Y SOCIAL MEDIA MARKETING

Hace más de 40 años se dio el primer uso de Internet por medio de intercambios de mensajes entre personas. Luego aparecieron los grupos de noticias (foros online) y el correo electrónico que se consolidaron como las actividades principales de la década de los 90. Por esta época, en el Centro Europeo de Investigaciones Nucleares (CERN), Tim Berners Lee, quien se encontraba en la búsqueda de un sistema de almacenamiento y recuperación de datos, retomó la idea de Ted Nelson de usar hipervínculos. Este sistema fue llamado World Wide Web (WWW) o telaraña mundial[1].
De esta manera se logró vincular información en forma lógica a través de las redes, ésta era programada en un lenguaje de hipertexto con "etiquetas" que asignaban una función a cada parte del contenido que luego iban a ser interpretadas por un programa de computación, hoy conocido como "navegador". A partir de entonces, Internet comenzó a crecer más rápido que otro medio de comunicación y muchos usuarios empezaron a acceder a documentos (páginas web) que, en ese momento creaban pocas personas u organizaciones por su complejidad técnica. Sin embargo, esas empresas no eran conscientes de que las conversaciones -correos electrónicos, foros, chats- que se estaban generando en la web acerca de ellas.
En 1999, cuatro autores escribieron un manifiesto con 95 tesis, para intentar dar a entender este fenómeno a las empresas. El Cluetrain Manifesto[2] se convirtió en un documento de referencia acerca de lo que estaba por ocurrir una década después. A comienzos del siglo XXI empezaron a tomar fuerza las tesis del Cluetrain. Por un lado, nacieron los «blogs», basados en un software de gestión de contenidos que podía usar cualquier persona, éste permitía actualizar muy fácilmente una página web. Por otro lado, apareció el buscador Google que mostraba en los primeros puestos a aquellas webs que cumplieran los estándares fijados por la industria, que actualizaran frecuentemente y recibieran enlaces entrantes desde otras webs. De esta forma se iban haciendo visibles para todo el mundo las conversaciones humanas. Las empresas vieron la necesidad de tomarse en serio las tesis del Cluetrain en especial la número uno: "Los mercados son conversaciones".

Actualmente Internet sigue creciendo y no como un medio más, si no como una infraestructura sobre la que se construyen medios de comunicación (incluyendo chats, *messengers*, *skypes*, tv o radio). Hay mucha expectativa alrededor de los medios sociales -blogs, redes, *microblogging*, wikis y demás- ya que el marketing tiene un campo más amplio que la publicidad en ellos; ventas, atención al cliente, fidelización, comunicación corporativa, desarrollo de producto, investigación de mercados, etc. Los

---

[1] Wikipedia. Artículo: Historia de Internet, http://es.wikipedia.org/wiki/Historia_de_Internet
[2] LEVINE, Rick; LOCKE, Christopher; SEARLS Doc; WEINBERGER David. The Cluetrain Manifesto: The End of Business as Usual, Basic Books, 2001.

medios sociales permiten interactuar con un consumidor activo y productor de contenidos, generar lazos emocionales con él a través de conversaciones con las marcas y llevan los contenidos hacia donde está la gente con un efecto viral que crece exponencialmente.

LA FIGURA DEL COMMUNITY MANAGER

A lo largo de los últimos años se ha empezado a hablar de este nuevo perfil profesional: Según AERCO (Asociación Española de Responsables de Comunidad) "El responsable de comunidad sería "aquella persona encargada de sostener, acrecentar y, en cierta forma, defender las relaciones de la empresa con sus clientes en el ámbito digital, gracias al conocimiento de las necesidades y los planteamientos estratégicos de la organización y los intereses de los clientes. Una persona que conoce los objetivos y actúa en consecuencia para conseguirlos"[3]

El Community Manager combina habilidades en comunicación corporativa, relaciones públicas y marketing digital. Entre sus funciones principales se encuentran:

- La escucha activa, es decir, monitoreo de reputación de marca en la red.
- Circular esta información internamente.
- Liderar y gestionar la comunidad en torno a la marca
- Explicar la posición de la empresa a la comunidad.
- Encontrar vías de colaboración entre la comunidad y la empresa.

Según varias fuentes de información que intentan definir el perfil del community manager, éste debe contar con las siguientes habilidades:

Técnicas:
Conocimiento del sector en el que se va a desempeñar, conocimientos en marketing y publicidad, excelente redacción, dominio sobre nuevas tecnologías de internet y programación web, creatividad y cultura 2.0, que consiste en la interacción y el *multitasking.*

Sociales:
Capacidad de conversación, habilidad para solucionar problemas, dinamismo, empatía, asertividad, trabajo en equipo, liderazgo, mediación, accesibilidad, detección de oportunidades, evangelización de marca, valores de justicia y equidad, transparencia.

---

[3] AERCO y Territorio creativo. "La función del Community Manager", Documento distribuido por Puromarketing.com, edición digital. Noviembre 2009

El "hábitat" natural del community manager es el internet, allí deberá desempeñar todas sus funciones y llevar la gran responsabilidad de representar una marca y gestionar su reputación. En consecuencia, es importante tener en cuenta los peligros y las amenazas dentro del *social media* para evitar potenciales crisis que puedan afectar la imagen y generar consecuencias negativas para la rentabilidad de la empresa.

SEGURIDAD INFORMÁTICA

Esta rama se ocupa de mantener los sistemas seguros, compuestos por hardware y software, de proteger a los usuarios en un "nivel aceptable" y la información de los mismos. La seguridad informática intenta proteger los datos, ya que estos son buscados por los delincuentes informáticos por representar la base económica de muchas empresas en el mundo. Es de conocimiento público que las grandes empresas contratan hackers para espiar a la competencia y en muchos casos para robar su información.
Por estas razones la seguridad informática ayuda a trabajar de manera óptima con los recursos que ofrece la tecnología basándose en los siguientes principios[4]:

1. **Confidencialidad:** Asegurar que los datos no van a ser vistos por personas no autorizadas. Por ejemplo al realizar una transacción con una tarjeta de crédito por internet, se busca cifrar la información para que no pueda ser leída por otros.
2. **Integridad**: Se centra en que los datos y documentos no puedan ser manipulados, alterados o cambiados. Por ejemplo, en el envío de un correo electrónico es importante que la información enviada, llegué de manera fiel al destinatario.
3. **Disponibilidad**: Trata de que la información esté disponible para los usuarios autorizados. Por ejemplo, un ataque de denegación de servicio que comprometiera a un servidor web causaría el no funcionamiento de la página web y, por lo tanto, una falta de disponibilidad de los contenidos para clientes o visitantes.

También es importante el concepto de privacidad como el derecho de mantener en secreto las acciones, datos y comunicaciones personales.

Amenazas

Los ciberdelincuentes se valen de varias técnicas para la obtención de datos. Entre estas encontramos principalmente las infecciones de los sistemas mediante aplicaciones creadas con alguna intención dañina sobre el usuario o la información, estas son conocidas como "malware", acrónimo en inglés de las palabras "*malicious*" y

[4] ASENSIO, Gonzalo. "Seguridad en Internet: una guía práctica y eficaz para proteger su PC con software gratuito" , Ediciones Nowtilus S.L., 2006.

"*software*" que equivale a software malicioso. Dentro de este grupo se encuentran los virus, gusanos, troyanos, spyware, etc.

Ingeniería Social

Esta es una técnica ampliamente utilizada por los atacantes presentes en los medios online. La ingeniería social explota vulnerabilidades psicológicas de los seres humanos. Por lo general, este método de ataque busca canalizar la atención de los usuarios aprovechando elementos de su personalidad (como una excesiva curiosidad, excitada mediante la exhibición de noticias importantes), con el fin de que realicen actos involuntarios sin pensar que se está colaborando con el delincuente para que éste logre su objetivo, y sin sospechar que forma parte del engaño.

Este trabajo pretende realizar un aporte para la formación de este nuevo perfil que en los últimos cuatro años ha tomado mucha fuerza en la rama del Social Media Marketing, además de ser un requisito para obtener el título de Especialista en Dirección y Gestión de Marketing y Estrategia Competitiva de la Universidad de Buenos Aires.

1. PLANTEO DEL PROBLEMA

Con el boom de las redes sociales en internet y el apuro de las marcas por tener presencia en ellas, la información disponibles se ha centrado en acciones de marketing y posicionamiento en buscadores sin tener en cuenta aspectos como la seguridad de la información y las amenazas presentes en este medio. A partir de esto, se generan las siguientes inquietudes:

¿Están las marcas incursionando en el social media sin la conciencia de los riesgos en tema de seguridad que esto conlleva?

¿El relativamente nuevo perfil del community manager está debidamente preparado para afrontar esta realidad a la hora de gestionar la reputación de marca en redes sociales?

¿En los planes de gestión de crisis de las empresas se contemplan los ataques informáticos?

¿Cómo afrontar una crisis de reputación en el social media causado por un ataque informático?

¿Cuáles son las prácticas que debe tener en cuenta un community manager para prevenir un ataque informático?

2. HIPÓTESIS

La seguridad informática en un tema muy enfocado hacia rubros de ingeniería o administración de sistemas, programación, derecho y áreas relacionadas con el manejo de dinero como el *homebanking*. En segunda instancia, es dirigido a usuarios finales que consumen el servicio de internet o realizan actividades cotidianas en ese medio. La figura del community manager, al ser tan reciente, se encuentra mimetizada entre estos campos, ya que participa del lado de la empresa pero tiene comportamientos de usuario. Y ante la falta de conciencia de esta problemática es muy probable que las empresas no sientan la necesidad de tomar medidas preventivas para la protección de datos.

Entre las funciones del community manager que se han definido por las distintas instituciones, principalmente en Europa ya que en Latinoamérica se siguen los preceptos importados del primer mundo y se brindan cursos muy básicos, la parte tecnológica solamente contempla las configuraciones de las plataformas o el conocimiento básico de ciertos lenguajes de programación sin incluir el tema de seguridad ni resguardo de datos.

Por lo que se ha podido observar durante el año 2011, las grandes marcas han sido victimas de varios ataques a pesar de contar con amplios recursos. Esto demuestra varias vulnerabilidades y evidencia la necesidad de concientización de la problemática.

Los descuidos en protección de la información que incluyen pérdida de bases de datos, listas de clientes, números de tarjetas de crédito, etc., acarrean graves consecuencias en la reputación y la credibilidad de las marcas, lo que puede echar para atrás años de trabajo invertidos en posicionamiento.

Mediante diferentes estudios a través de encuestas a directivos de grandes, medianas y pequeñas compañías, realizados por empresas de seguridad informática, se ha notado un alto porcentaje de preocupación pero poco conocimiento de cómo protegerse y la mínima aplicación de buenas prácticas por parte de los usuarios.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Demostrar la importancia de la seguridad informática y las buenas prácticas en la protección de datos y gestión de la reputación para los responsables de comunidades en redes sociales

3.2 OBJETIVOS ESPECÍFICOS

1. Concientizar sobre la responsabilidad que tiene el community manager en la gestión de la reputación de marca y, por tanto, sobre la necesidad de educarlo en el campo de la seguridad informática.

2. Conocer el desempeño actual del puesto del community manager en varias empresas y de qué forma se gestiona y protege la información que se encuentra disponible en el ciberespacio.

3. Aportar una nueva área de investigación y conocimiento para tener en cuenta en la formación profesional de todos los involucrados en las estrategias de social media marketing.

4. Generar una guía que permita al community manager realizar sus tareas de forma segura sin arriesgar la información sensible de la empresa.

5. Obtener el título de Especialista en Dirección y Gestión de Marketing y Estrategia Competitiva de la Universidad de Buenos Aires.

4. JUSTIFICACIÓN

Como ha sido marcado anteriormente, el tema de seguridad informática no está contemplado en los actuales programas de educación dirigidos a los Community Managers o a las personas que serán responsables de gestionar la presencia online de las marcas. Estas personas pueden pertenecer tanto al área de comunicación como a la de marketing dependiendo del tamaño de la empresa y en otros casos, a agencias de publicidad o marketing que prestan este servicio de forma tercerizada.
Por tal razón, y la importancia de este cargo junto a la repercusión para la reputación de la marca, se encuentra la necesidad de sumar esta temática a la base de conocimiento para los responsables de comunidades online y también para los gerentes de marketing o directivos de las compañías, ya que deben conocer los riesgos y las alternativas para preservar la integridad de sus negocios en el social media.

Cabe resaltar que a lo largo de los últimos años, el tema de seguridad informática ha cobrado un protagonismo al darse a conocer varios ataques vía internet dirigidos hacia marcas tan prestigiosas como Sony, Adidas, Vodafone, TripAdvisor o la agencia de publicidad Epsilon que registró un robo masivo de información que contenía datos de clientes como Amazon, Hilton, JPMorgan Chase y City Group, entre otras. En otros casos se aprovecharon las plataformas para diferentes fines maliciosos, incluyendo, infección a equipos, daño a usuarios, publicidad engañosa y competencia desleal. Todo esto valiéndose de técnicas de ingeniería social, vulnerabilidades y malas prácticas por parte de los administradores de los recursos online.
También se vieron movimientos globales como el *hacktivismo*, liderados por el grupo Anonymous, en nombre de la defensa de los usuarios y las poblaciones en general. Este grupo realizó una serie de ataques que vulneraron servidores web de sitios gubernamentales latinoamericanos, perfiles de Facebook y Twitter de diferentes personajes.

5. MARCO TEÓRICO

Para sustentar varios conceptos a lo largo del trabajo, se tomarán como teoría los postulados del profesor Philip Kotler, distinguido por innumerables premios y galardones en los últimos 40 años, elegido Líder en Pensamiento de Marketing. Así mismo se tendrán en cuenta las obras de Michel Porter, economista estadounidense, profesor en la Escuela de Negocios de Harvard, especialista en gestión y administración de empresas, y director del Instituto para la estrategia y la competitividad. Se utilizarán los libros de ambos autores como referencia obligada.

KOTLER, Philip, "Marketing 3.0: From Products to Customers to the Human Spirit", John Wiley & Sons Ltd, 2010.

KOTLER, Philip, "Principios de marketing", Prentice Hall, Edición: 12, 2008.

KOTLER, Philip, "Marketing Insights from A to Z: 80 Concepts Every Manager Needs to Know ", John Wiley & Sons Ltd, 2003.

KOTLER, Philip, "Marketing 3.0", Lid Editorial Empresarial, 2010.

PORTER, Michael E, "Estrategia competitiva: Técnicas para el análisis de la empresa y sus competidores", Piramide Ediciones Sa, 2010.

PORTER, Michael E, "Ser competitivo (edición actualizada)", Deusto Ediciones SA, 2009.

Otros títulos complementarios serán:

RIES, Al y TROUT, Jack. "Posicionamiento", Mc Graw Hill, 2005.

RIES Laura Ries y RIES Al. "Las 22 leyes inmutables de la marca", Mc Graw-Hill, 2000.

5.1 COMPETITIVIDAD

La competitividad debe ser entendida como la capacidad que tiene una organización, pública o privada, lucrativa o no, de obtener y mantener ventajas comparativas que le permitan alcanzar, sostener y mejorar una determinada posición en el entorno socioeconómico. El término competitividad es muy utilizado en los medios empresariales, teniendo incidencia en la forma de plantear y desarrollar cualquier iniciativa de negocios, lo que provoca, obviamente una evolución en el modelo de empresa y empresario.

La competencia está integrada por las empresas que actúan en el mismo mercado y realizan la misma función dentro de un mismo grupo de clientes con independencia de la tecnología empleada para ello. Por lo tanto, un competidor no es el que fabrica el

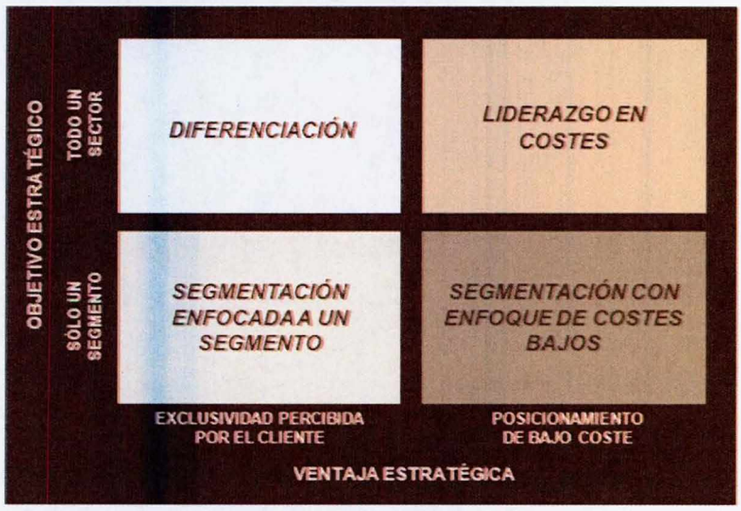
mismo producto genérico, sino aquel que satisface las mismas necesidades con respecto al mismo público objetivo o consumidor.

De acuerdo con el modelo de la ventaja competitiva de Porter, la estrategia competitiva toma acciones ofensivas o defensivas para crear una posición defendible en una industria,
con la finalidad de hacer frente, con éxito, a las fuerzas competitivas y generar un retorno sobre la inversión.

Los tipos básicos de ventaja competitiva son:

1. Liderazgo por costos (bajo costo)
2. Diferenciación

Por otro lado, también influye el enfoque de mercado, ya que un producto o servicio puede dirigirse hacia un sector o hacia un segmento. Algunos autores hablan del "enfoque" como si fuera otra estrategia en sí misma.
Del cruce de estas variables surgen los distintos cuadrantes de la matriz, que se explican por sí mismos. Para Porter es difícil ser simultáneamente líder en costes y en exclusividad, corriéndose el peligro de quedarse a medias en ambos objetivos. Existen algunas excepciones como Apple, capaz de luchar por diferenciación y a la vez disponer de un considerable volumen en algunos segmentos.



Estrategias genéricas de Porter
Fuente: http://managersmagazine.com

Toda empresa se debe relacionar con su con su entorno mediante un análisis competitivo que le ayudará a identificar las fortalezas y debilidades, así como las oportunidades y amenazas existentes en su mercado objetivo.

- Análisis externo. Supone el análisis del entorno, de la competencia, del mercado, de los intermediarios y de los suministradores.

- Análisis interno. Supone analizar la estructura organizativa de la propia empresa, y de los recursos y capacidades con las que cuenta.

Según Porter, ser competitivo es "*diferenciarnos por nuestra calidad, por nuestras habilidades, por nuestras cualidades, por la capacidad que tengamos de cautivar, de seducir, de atender y asombrar a nuestros clientes, sean internos o externos, con nuestros bienes y servicios, lo cual se traduciría en un generador de riquezas*".[5]

5.2 RENTABILIDAD

Siguiendo a Lawrence Gitman[6] desde el punto de vista de la Administración Financiera, "la rentabilidad es una medida que relaciona los rendimientos de la empresa con las ventas, los activos o el capital. Esta medida permite evaluar las ganancias de la empresa con respecto a un nivel dado de ventas, de activos o la inversión de los dueños. La importancia de ésta medida radica en que para que una empresa sobreviva es necesario producir utilidades. Por lo tanto, la rentabilidad esta directamente relacionada con el riesgo, si una empresa quiere aumentar su rentabilidad debe también aumentar el riesgo y al contrario, si quiere disminuir el riesgo, debe disminuir la rentabilidad..."

Por otra parte, Joseph Guiltinan[7] plantea desde el enfoque de Marketing, que "la rentabilidad mide la eficiencia general de la gerencia, demostrada a través de las utilidades obtenidas de las ventas y por el manejo adecuado de los recursos, es decir la inversión, de la empresa..."

Integrando las anteriores definiciones se puede afirmar que la rentabilidad es el porcentaje o tasa de ganancia obtenida por la inversión de un capital determinado. Sin embargo, para el problema específico del marketing, esta definición debe estar asociada con el producto, así las cosas, una definición aproximada del concepto de rentabilidad, desde el enfoque de Marketing podría ser: "es el porcentaje del margen de contribución variable que mide la capacidad que tiene un producto para generar utilidades a la empresa". En donde, el margen de contribución variable es la diferencia resultante entre las ventas del fabricante y la sumatoria de los costos variables de producción (mano de obra, materiales, empaques, etc.) y los costos variables de ventas (comisiones, descuentos, etc.) en el Estado de Pérdidas y Ganancias por producto.

---

[5] PORTER, Michael E. "Ventaja competitiva: Creación y sostenibilidad de un rendimiento superior", Piramide Ediciones Sa, 2010.

[6] GITMAN, Lawrence J. "Fundamentos de Administración Financiera", Editorial Harla S.A., México, 1992.

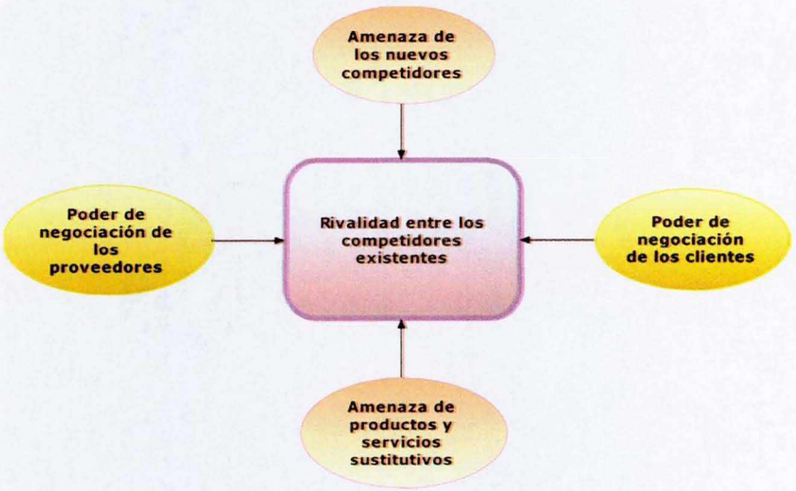
[7] GUILTINAN, Joseph P. y Gordon W, Paul. "Administración de Mercadeo. Estrategias y Programas", Editorial , McGraw-Hill, México, 1984.

Las cinco fuerzas de Porter

Las 5 Fuerzas de Porter es un modelo holístico que permite analizar cualquier industria en términos de rentabilidad. Fue desarrollado por Michael Porter en 1979 y, según éste, la rivalidad entre los competidores es el resultado de la combinación de cinco fuerzas o elementos.

Poder de negociación de los Compradores o Clientes
Poder de negociación de los Proveedores o Vendedores
Amenaza de nuevos entrantes
Amenaza de productos sustitutivos
Rivalidad entre los competidores

Este modelo de las Cinco Fuerzas de Porter propone un modelo de reflexión estratégica sistemática para determinar la rentabilidad de un sector con el fin de evaluar el valor y la proyección futura de empresas o unidades de negocio que operan en dicho sector.



Representación gráfica del modelo de Porter
Fuente: Wikipedia

5.3 GLOBALIZACIÓN

La globalización se trata de un proceso que se impone debido a la mayor comunicación entre las diversas partes del mundo, llevando prácticamente a la superación de las distancias, con efectos evidentes en campos muy diversos. La misma constituye la característica más típica del mundo de hoy.
La globalización es un proceso económico, político y social que si bien es cierto no es nuevo, ha sido retomado con mayor énfasis en los países en desarrollo como premisa especifica para lograr un crecimiento económico y erradicar la pobreza. Pero este

fenómeno en ningún momento fue concebido como modelo de desarrollo económico, sino más bien como un marco regulatorio de las relaciones económicas internacionales entre los países industrializados.

El término engloba la creciente internacionalización del capital financiero, industrial y comercial, nuevas relaciones políticas internacionales y el surgimiento de la empresa multinacional que a su vez produjo como respuesta a las constantes necesidades de reacomodo del sistema capitalista, nuevos procesos de producción, distribución y consumo, llevando a una expansión y uso intensivo de la tecnología.

Según Kotler[8], la globalización, la hipercompetencia e Internet están reestructurando los mercados y los negocios. Estas tres fuerzas actúan incrementando la presión bajista de los precios. La globalización empuja a las compañías a producir en los lugares más baratos y traer sus productos de países con precios inferiores a los de sus mercados domésticos. Internet facilita la comparación de precios y el movimiento hacia la mejor oferta. El reto del marketing es encontrar formas de mantener los precios y la rentabilidad, teniendo en cuenta estas macrotendencias.

5.4 POSICIONAMIENTO

El concepto de posicionamiento que se conoce actualmente es gracias a Al Ries y Jack Trout, cuando escribieron su libro "Posicionamiento" en 1982[9]. En realidad la palabra había sido usada anteriormente en relación con la colocación de los productos en las tiendas, con esperanza de que fuera a la altura de los ojos. Sin embargo, Ríes y Trout dieron un giro a este término: "Posicionamiento no es dónde posiciona un producto en el lineal. Posicionamiento es la actuación sobre la mente del consumidor". Ries y Trout veían el posicionamiento, principalmente, como un ejercicio de comunicación. A menos que el producto sea identificado como el mejor en algo que es significativo para un grupo de consumidores estará pobremente posicionado y lo recordarán con dificultad. Recordamos las marcas que sobresalen como las primeras o las mejores en algo.

5.5 BRANDING

El *Branding* es un anglicismo empleado en marketing que hace referencia al proceso de creación de valor de marca (*brand equity*) mediante la administración estratégica del conjunto total de activos y pasivos vinculados en forma directa o indirecta al nombre y/o símbolo (isotipo) que identifican a la marca influyendo en el valor suministrado;

---

[8] KOTLER, Philip, "Marketing Insights from A to Z: 80 Concepts Every Manager Needs to Know ", John Wiley & Sons Ltd, 2003.

[9] RIES, Al y TROUT, Jack. "Posicionamiento", Mc Graw Hill, 2005.

tanto al cliente como a la empresa oferente; por un producto o servicio, incrementándolo o reduciéndolo según el caso.
Debido a las condiciones turbulentas del mercado, la mayor dificultad para mantenerse en él, producto de las presiones de la globalización y de la agresiva competencia, ha conllevado que la gestión de marcas posea mayor importancia en la actualidad.
La marca nos ayuda a seleccionar un producto o servicio en un mundo complejo de crecientes opciones de elección, especialmente cuando la diferencia entre productos es escasa o difícil de evaluar.
Las marcas son algo más que un producto, servicio o identidad (el nombre, el logotipo, el diseño y la voz de marca). La marca es sinónimo del negocio y estilo que está tras el producto o servicio, que incluye al personal de la organización, una filosofía y un espíritu que lo sustenta. Las marcas ofrecen un conjunto de valores, una visión y una actitud. Las organizaciones establecen un posicionamiento de marca para proyectar una imagen pública e interna coherente; este posicionamiento delimita unos perímetros para responder a las oportunidades y retos, además de orientar a aquellos que trabajan para la organización.

Una vez que el producto se ha consolidado en el mercado, debe demostrar su continuidad en él a través de la actividad de la marca. El propósito de las campañas de publicidad no siempre es vender el producto o servicio, sino que también sirven para crea conciencia, mejorar el prestigio y afirmar o cambiar las percepciones. La identidad de la marca no necesariamente ha de ser visible, pues puede estar asociada con eventos o campañas, que son transmitidas más a través de personas que a través del logotipo o marca. Las empresas pueden invertir millones en crear una marca o producto y muchos millones más en mantenerlo vivo, pero el activo de marca puede perderse rápidamente si éste es incapaz de captar a su público o si su comportamiento está por debajo de las expectativas que anuncia.

6. METODOLOGÍA

Para completar este trabajo se han planteado tres fuentes de información principales: investigaciones mediante encuestas y análisis bibliográfico.

Sobre las encuestas se realizaron dos divisiones: la primera a Community Managers de diferentes categorías de producto y, la segunda, a usuarios seguidores de marcas en redes sociales. El objetivo es conocer si los responsables de comunidad tienen conocimientos en seguridad informática y si emplean practicas de protección de datos. Con las encuestas a usuarios se buscaría determinar la repercusión en la reputación y la confianza de una empresa en caso de sufrir alguna crisis generada por la mala gestión de la seguridad informática.

6.1 ENCUESTAS A COMMUNITY MANAGERS:

- **Población:** Community Managers de habla hispana (España y Latinoamérica) presentes en asociaciones y foros online.

- **Muestra:** El objetivo es encuestar a mínimo 15 responsables de comunidad de Latinoamérica y España.

- **Unidad de muestreo:** Community Managers que manejen cuentas de productos de diferentes categorías y de diferentes países de habla hispana.

- **Técnica:** Encuesta en Internet.

- **Instrumentos:** Plataforma Google Drive / Cuestionarios, publicada en Internet con un link de acceso a la encuesta.

- **Metodología de selección:** Voluntarios que quieran participar en la encuesta convocados a través de grupos y asociaciones de Community Managers en Facebook y LinkedIn.

6.2 ENCUESTAS A USUARIOS QUE SEAN SEGUIDORES DE MARCAS EN REDES SOCIALES COMO FACEBOOK Y TWITTER:

- **Población:** Internautas latinoamericanos.

- **Muestra:** Mínimo 30 usuarios con las características antes mencionadas.

- **Unidad de muestreo:** Hombres y mujeres que pueden ser diferentes nacionalidades latinoamericanas entre 24-35 años, que utilicen las redes sociales.

- **Técnica:** Encuesta en Internet.

- **Instrumentos:** Plataforma Google Drive / Cuestionarios, publicada en Internet con un link de acceso a la encuesta.

- **Metodología de selección:** Se contactarán por medios online a las que tengan los requerimientos mínimos para participar de forma voluntaria.

Con los cuestionarios descritos anteriormente, se ha planteado hacer una investigación cuantitativa, descriptiva y causal con preguntas estructuradas. Se ha elegido el método de encuesta en Internet, ya que este medio es el entorno en donde se desarrollan las principales actividades de los Community Managers y la interacción de los usuarios con las marcas.

La bibliografía que se tomará en cuenta, tal como se expuso anteriormente, se concentra en documentos sobre *branding*, posicionamiento, marketing *online*, *social media marketing* y seguridad informática. Con esta investigación, se espera generar herramientas que le den solución al problema principal y generar una guía que permita al Community Manager realizar sus tareas de forma segura y consciente sin arriesgar la información sensible de la empresa.

Por último, el método que se utilizará para analizar la información será estadístico, descriptivo. A partir de la hipótesis, se tratará de llegar a las conclusiones.

7. ANÁLISIS DE DATOS

7.1 ENCUESTAS A COMMUNITY MANAGERS

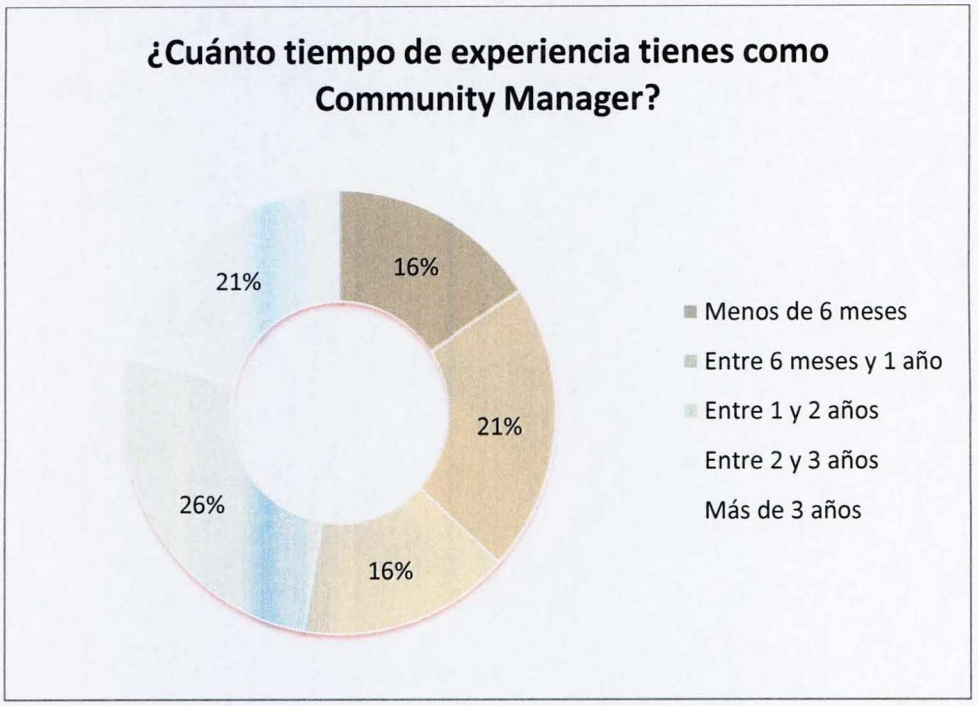
A través de un cuestionario estructurado (ver anexo) se ha publicado una encuesta online, la cual se ha difundido en diferentes plataformas sociales de Internet: Facebook, Twitter y LinkedIn. Cada una concentra diferentes tipos de públicos. En Facebook se encuentra la más amplia variedad de internautas, contando actualmente con más de 1000 millones de usuarios. Twitter, la red social también conocida como *"microblogs"*, cuenta con más de 200 millones de usuarios activos. El perfil de usuario de esta red, cuenta con conocimientos un poco más avanzados en tecnología. Por último, la red profesional LinkedIn, que concentra a miembros de entornos corporativos, empresas y grupos de debate alrededor de infinidad de temáticas
Dentro de estas Redes Sociales se encuentran varias asociaciones de Community Managers de España y Latinoamérica, así como grupos temáticos. Esto facilitó la búsqueda de estos nuevos profesionales, quienes contestaron el formulario de manera voluntaria, no probabilística. Aunque esta muestra no tenga una representatividad tan rigurosa y los resultados no sean extrapolables a la población general, se ha hecho de manera cuidadosa y controlada, eligiendo personas con características especificas previamente definidas.

7.1.1 Perfil de la muestra

Participaron 19 profesionales que afirmaron ser Community Managers. 47% hombres y 53% mujeres. El 58% reside en Argentina, el 27% en España y el restante 15% en Bolivia, México y Colombia.

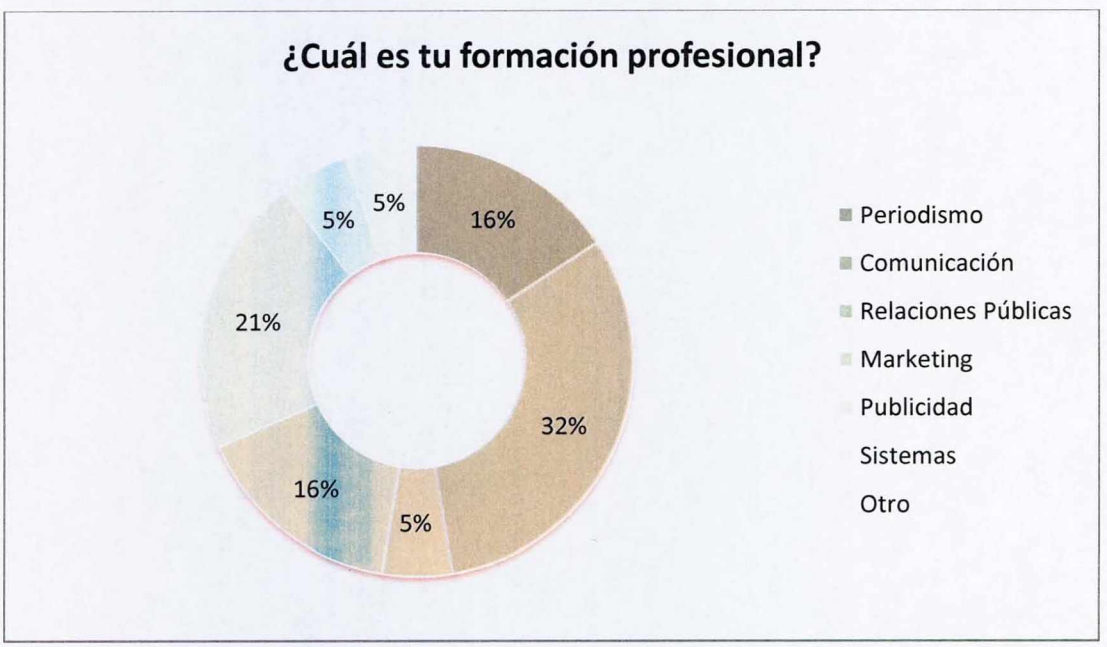
7.1.2 Experiencia y formación

El nivel de experiencia varia ya que ésta se considera aún una profesión nueva. Solamente el 16% declara tener más de 3 años en el oficio. El 37% tiene menos de un año y el restante 37% declara tener entre uno y dos años de experiencia.

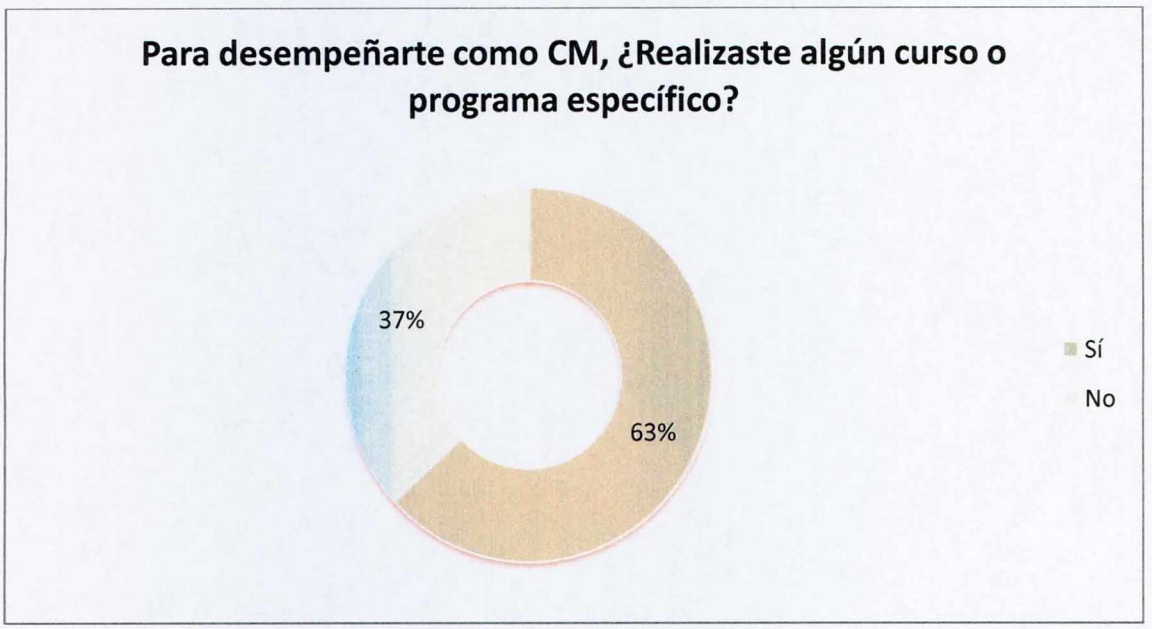


El 63% declaró trabajar en relación de dependencia con empresas o agencias prestadoras del servicio de gestión de Redes Sociales. El 21% afirmó ejercer de manera independiente y el restante 16% no contestó.

El 32% de los profesionales provienen de la rama de comunicación, 21% se formaron en el área de publicidad, un 16% en periodismo y otro 16% en marketing. El restante 15% pertenecen a relaciones públicas, sistemas y otras.

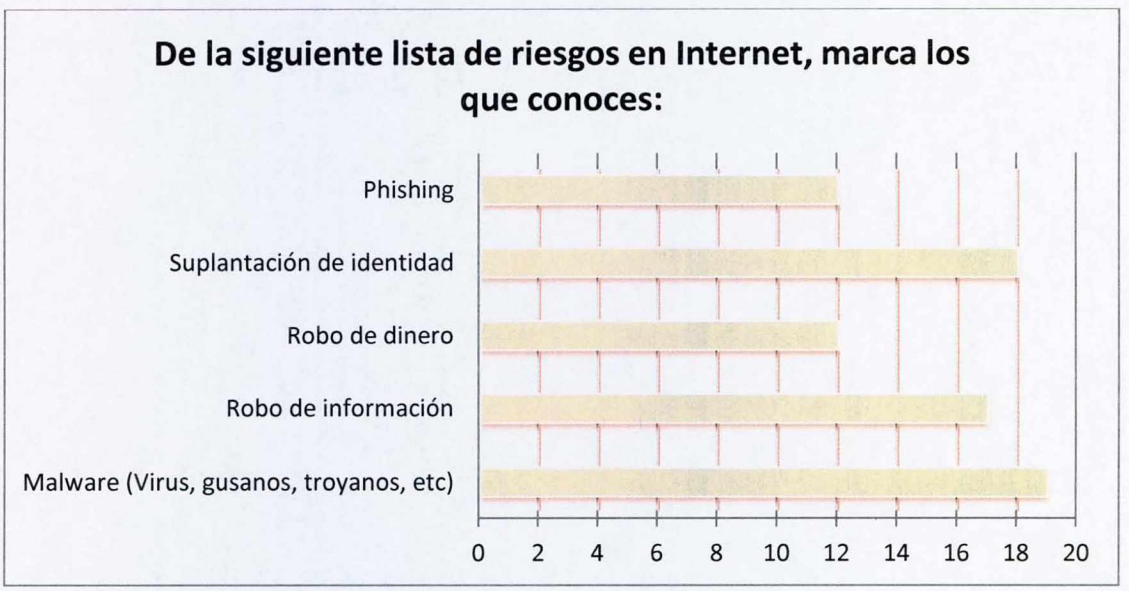


El 63% afirma haber realizado un curso o programa específico sobre gestión de Redes Sociales. El 37% incorporó el oficio a sus carreras de grado base.

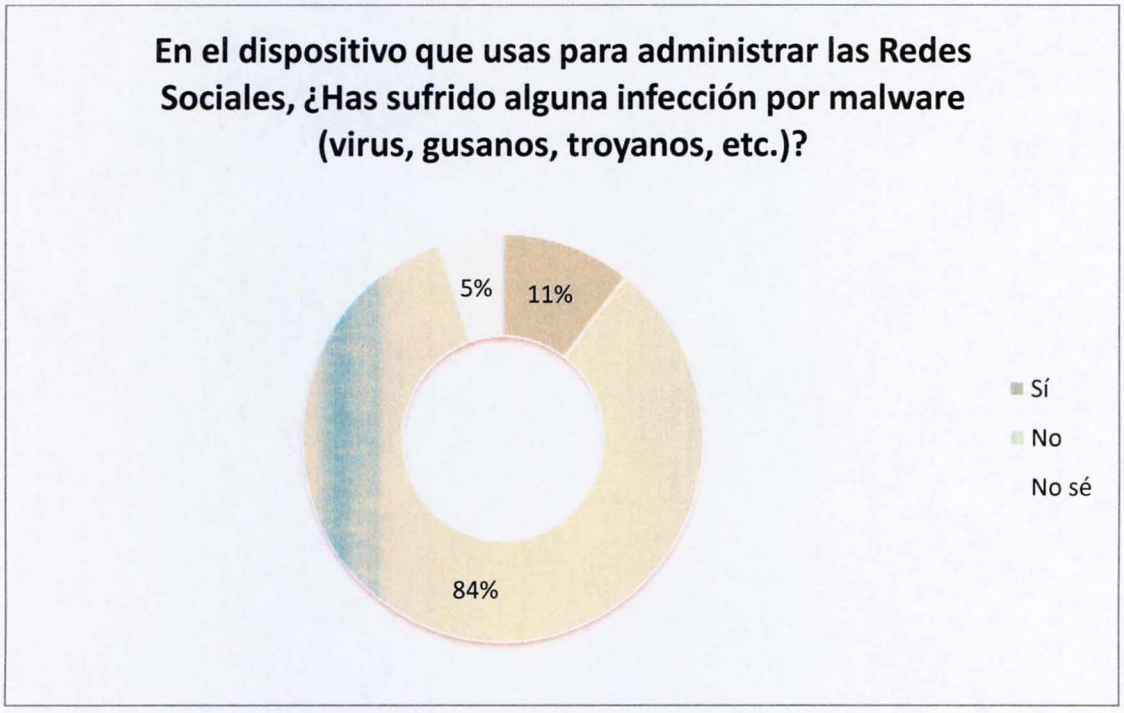


7.1.3 Riesgos y amenazas en Internet

Se le pidió a los encuestados que marcaran en la lista los riesgos en Internet que conocían. Todos afirmaron conocer el *Malware* (códigos maliciosos), que popularmente se conoce como virus, gusanos, troyanos, etc. En segundo lugar se encuentra la Suplantación de identidad, luego el Robo de información y por último el *Phishing* y el Robo de dinero.



El 84% asegura que nunca ha recibido una infección por Malware en los dispositivos que usan para gestionar las Redes Sociales. El 11% si ha resultado afectado y el 5% no lo sabe. Es común que muchos usuarios nunca se lleguen a enterar que han sido infectados por códigos maliciosos, ya que los ciberdelincuentes pueden utilizar de manera remota sus equipos sin que estos lo perciban o cuando no se encuentren haciendo uso de los dispositivos.



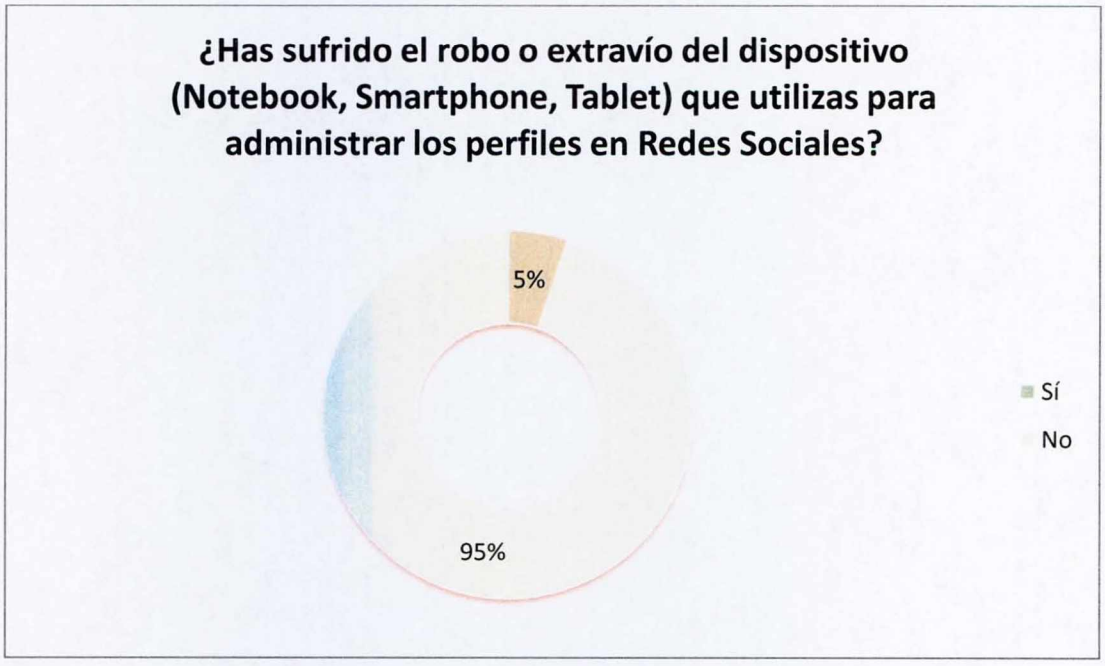
De la porción que afirmó haber recibido una infección, todos niegan que ésta se haya propagado por Redes Sociales. Sin embargo, en los últimos años estas plataformas se han convertido en los principales medios de infección, siendo principalmente difusoras de enlaces maliciosos a través de su servicio de mensajería instantánea, aplicaciones y los feeds de actualizaciones de los perfiles de usuario. Durante 2012 los servicios de Yahoo!, Twitter y LinkedIn fueron vulnerados por delincuentes informáticos, quienes obtuvieron los datos de más de 7.5 millones de usuarios de dichas plataformas.[10]

El 50% de los profesionales que fueron victimas de un ataque por Malware perdieron credenciales de correo electrónico y el otro 50% dice no haber perdido nada luego de la infección. Muchos de los usuarios piensan que si los archivos no se borran de sus

[10] http://blogs.eset-la.com/laboratorio/2012/07/12/yahoo-nueva-brecha-seguridad-red/ http://blogs.eset-la.com/laboratorio/2013/02/04/ataque-twitter-compromete-250000-usuarios/ http://blogs.eset-la.com/laboratorio/2012/06/06/cambie-contrasena-linkedin-posible-fuga-informacion-masiva/

equipos, no los han perdido. Los delincuentes suelen robar la información a través de copias de los archivos sin que el dueño lo note. Otra modalidad consiste en utilizar el espacio del disco duro de la victima para alojar material ilegal y distribuirlo a través de Internet. De esta forma, en caso de ser descubierto, las pruebas incriminatorias quedarán en el equipo del usuario infectado.

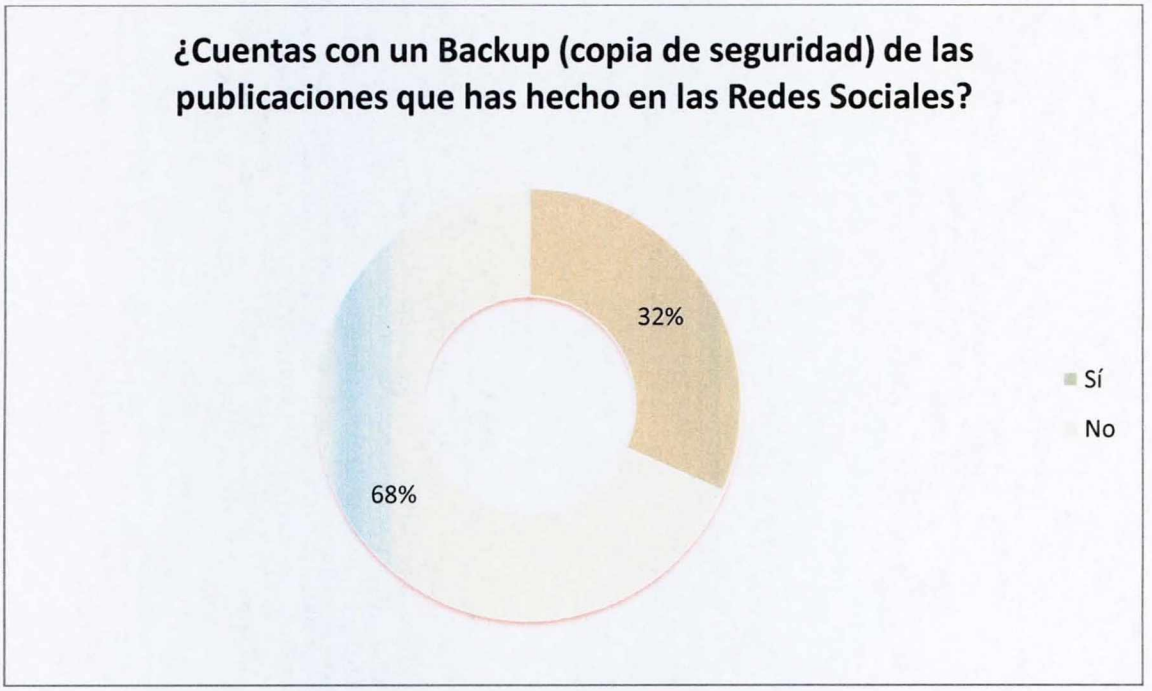
Otra forma de perder información es mediante la pérdida o robo del dispositivo que la aloja. Aunque el 95% de los profesionales declara no haber perdido el dispositivo con el que administra las cuentas en Redes Sociales, este riesgo es latente especialmente en los países de la región latinoamericana debido a sus altos niveles de inseguridad.
En los últimos tiempos, las personas, debido a la movilidad, la hiperconectividad y por los beneficios que trae la tecnología, han ido integrando sus dispositivos móviles (como *smartphones*, *notebooks* y *tablets*) a la vida laboral. Este fenómeno es más conocido como BYOD (por las palabras en inglés: *Bring Your Own Device*) y se refiere a que los empleados lleven sus dispositivos móviles su lugar de trabajo y allí utilicen libremente los recursos de la empresa como correo electrónico, servidores de archivos, de bases de datos, entre otros. De esta forma, si no se cuenta con una política de seguridad o buenos hábitos de navegación, se expone información sensible de la compañía.



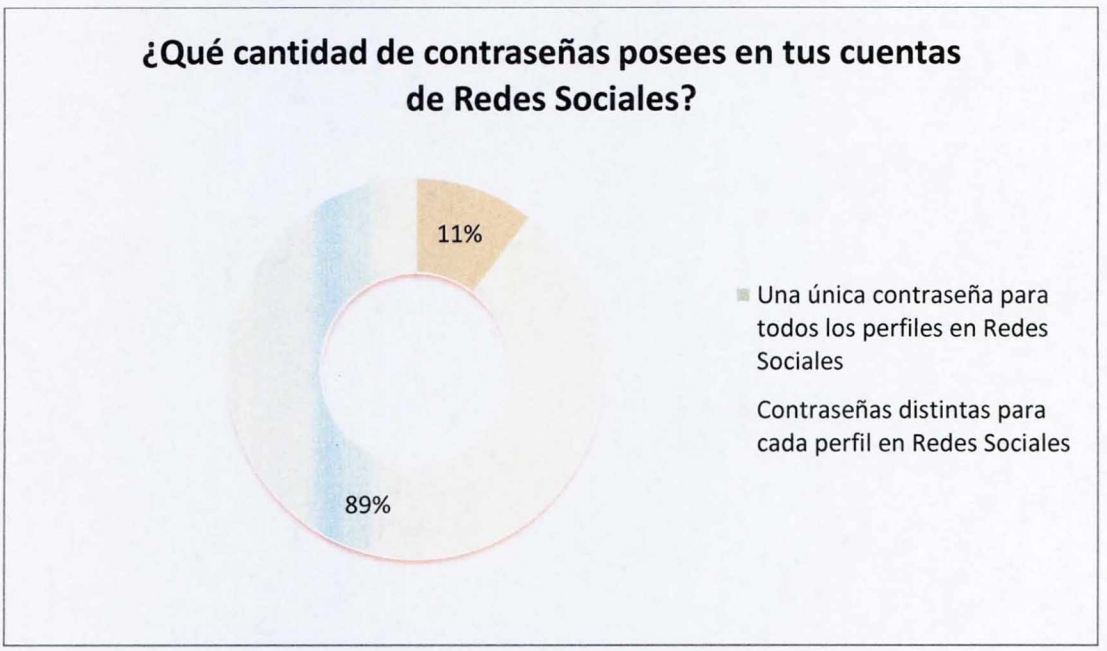
7.1.4 Hábitos y prácticas de protección de la información

El 68% de los Community Managers afirmó no contar con una copia de seguridad de sus publicaciones. Es decir, que en caso de perder el control de una o varias cuentas en Redes Sociales, debido a un ataque informático, podrían perder definitivamente la información depositada en dichas plataformas virtuales.

El respaldo de la información (o *backups*) ayuda a mitigar los efectos de una infección por malware, el robo o pérdida del dispositivo.

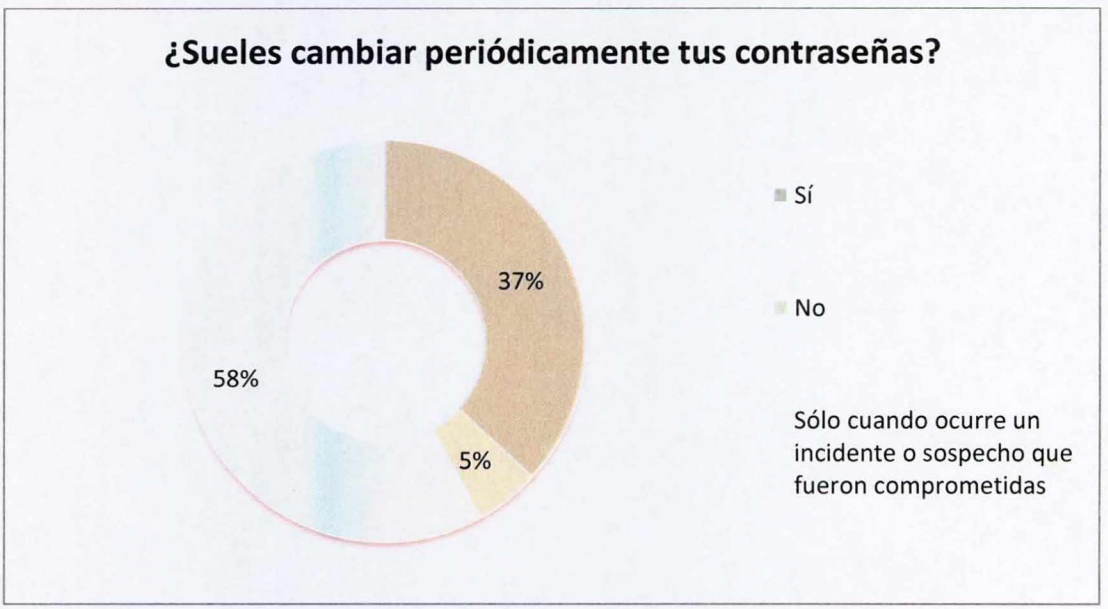


La contraseña o *password* es un sistema de autenticación simple mediante el cual, un usuario debe validar su identidad para poder acceder a un servicio como correo electrónico, Redes Sociales o recursos compartidos de red, etc. donde se tiene almacenada información relevante. Debido a esto, existen personas interesadas en vulnerar estos sistemas para obtener los datos y así, adquirir beneficios económicos.
Por esta razón es importante contar con diferentes contraseñas para cada servicio. DE esta forma, en caso de verse comprometido alguno de ellos, no pondrá en riesgo los demás.
Los profesionales encuestados afirmaron, en su mayoría, que utilizan distintas contraseñas para cada cuenta en Redes Sociales. Sin embargo, sigue habiendo un 11% de Community Managers que poseen la misma contraseña para todos los servicios. Como se explicó anteriormente, esta mala práctica aumenta el riesgo de perder el control de varios servicios a partir de un único ataque.



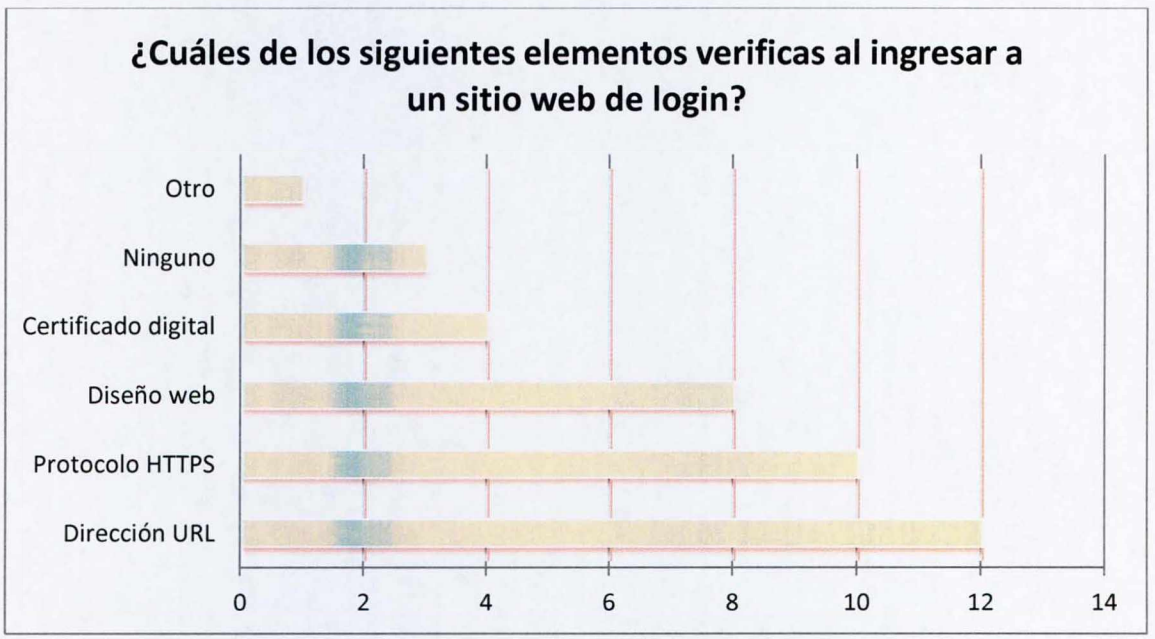
Tan importante como utilizar diferentes contraseñas para cada uno de los servicios, lo es cambiar las mismas de forma periódica. Esto ayuda a disminuir los posibles efectos de un robo de credenciales, tal como le sucedió a las empresas antes mencionadas; Yahoo!, Twitter y LinkedIn, donde quedaron expuestos los datos de los millones de usuarios que hacían uso de sus plataformas.

El 58% de los Community Managers cambia sus contraseñas cuando ocurre un incidente o sospechan que estas han sido comprometidas. A pesar de esto, lo más correcto sería renovarlas cada cierto periodo de tiempo, ya que muchas veces los usuarios infectados por malware no se enteran del hecho si no mucho tiempo después o, incluso, nunca lo llegan a advertir. El 5% no posee el hábito de cambiar sus contraseñas y el 37% dice que sí lo hace de manera periódica.



Uno de los métodos preferidos por los delincuentes informáticos es el *Phishing*. Este término hace referencia a la "pesca" de contraseñas y consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación del sitio web o un correo electrónico de un ente de confianza[11]. De esta forma, el usuario cree ingresar los datos en un sitio confiable cuando, en realidad, estos son enviados directamente al atacante. La observación de varios elementos como la dirección URL, el protocolo HTTPS, el diseño, el certificado digital, etc. Permite identificar si un sitio web es falso.

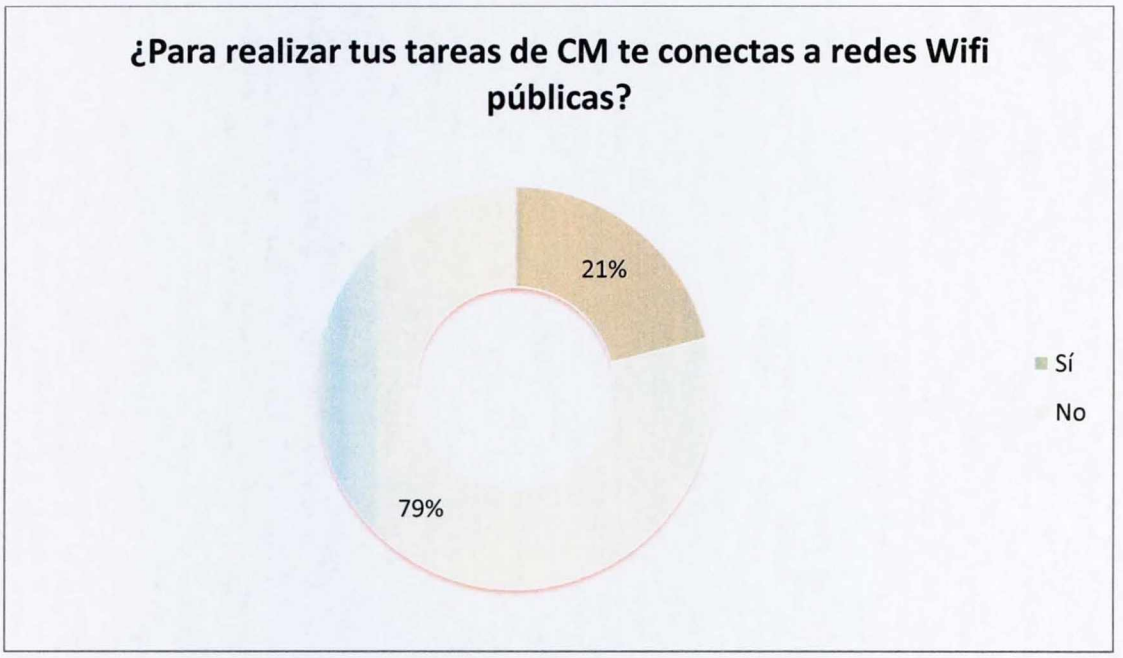
El 63% de los profesionales revisan la dirección URL del sitio antes de ingresar sus datos. En segundo lugar se encuentra el protocolo HTTPS con un 52%. El 42% se fija en los detalles del diseño, mientras que el 21% revisa que el certificado digital coincida con el nombre de la página. El 8% no verifica la originalidad del ente antes de proporcionar las credenciales de acceso.



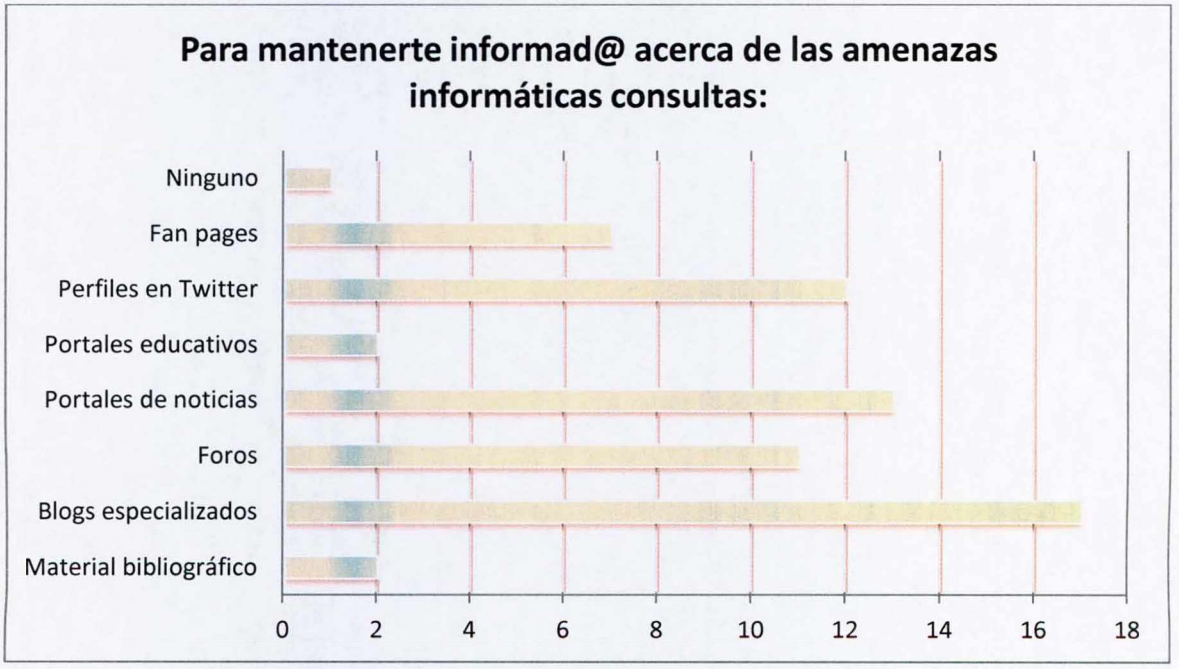
Las conexiones de Internet inalámbricas se han popularizado fuertemente los últimos años, tanto en el ámbito hogareño como en el corporativo y en los espacios públicos. La amplia utilización de *smartphones* y computadoras portátiles ha impulsado la difusión de esta tecnología en diferentes ámbitos. La falta de configuraciones de seguridad podría permitir que personas no autorizadas, con fines maliciosos, accedan a la información confidencial que circula por la red.

El 21% de los Community Managers afirma que se conecta a Internet a través de redes *Wifi* públicas para realizar sus tareas. Es decir, la información circula de manera no cifrada quedando expuesta y a disposición de otros usuarios ajenos a la empresa o marca.

[11] http://www.eset-la.com/centro-amenazas/amenazas/Phishing/2144

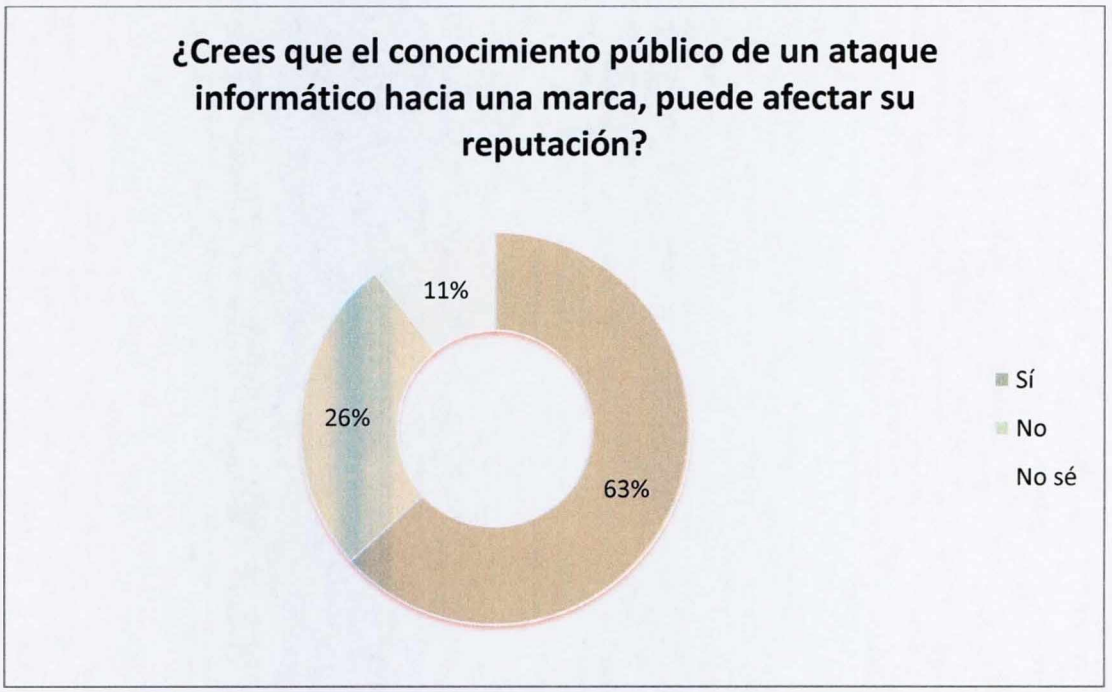


El 89.5% de los encuestados se mantienen informados acerca de las amenazas informáticas a través de blogs especializados. El 68,4% se actualiza a por medios de portales de noticias. El 63.2% sigue cuentas en Twitter para mantenerse al tanto. El 58% utiliza los foros como fuente de información. El 36,8 lo hace siguiendo páginas en Facebook. Es interesante que solamente el 10.5% recurre a material bibliográfico y portales educativos para obtener información certera acerca de los riesgos en Internet. El 5.3% no se informa por ningún medio sobre los peligros en la red.

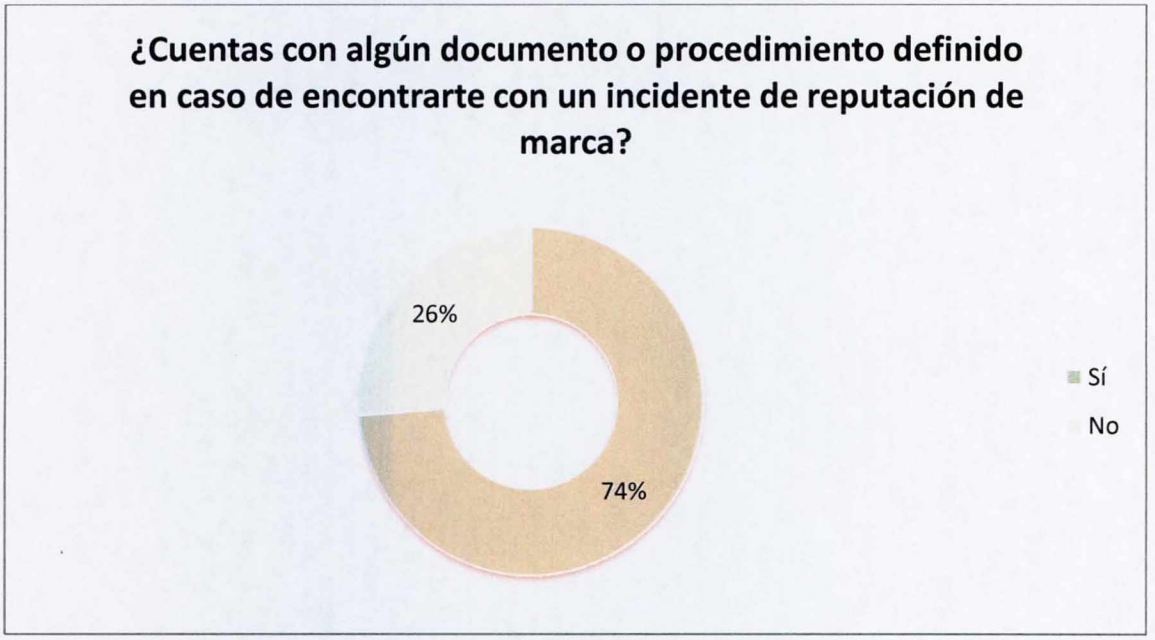


7.1.5 Reputación de marca

Se le preguntó a los Community Managers si consideraban que un incidente de seguridad, tal como un hackeo de cuentas, una infección o un ataque dirigido, podrían afectar la reputación de la marca. El 63% estuvo de acuerdo con esa afirmación, el 26% dijo que no y el 11% no lo sabe. Es de destacar que dentro del los que estuvieron respondieron positivamente, se encuentran los profesionales con menos experiencia, es decir, menor a 2 años.



Por último, se le preguntó a los encuestados si contaban con un procedimiento o manual de crisis en caso de contar con incidente de reputación de marca. El 74% afirmó poseerlo y el 26% no.



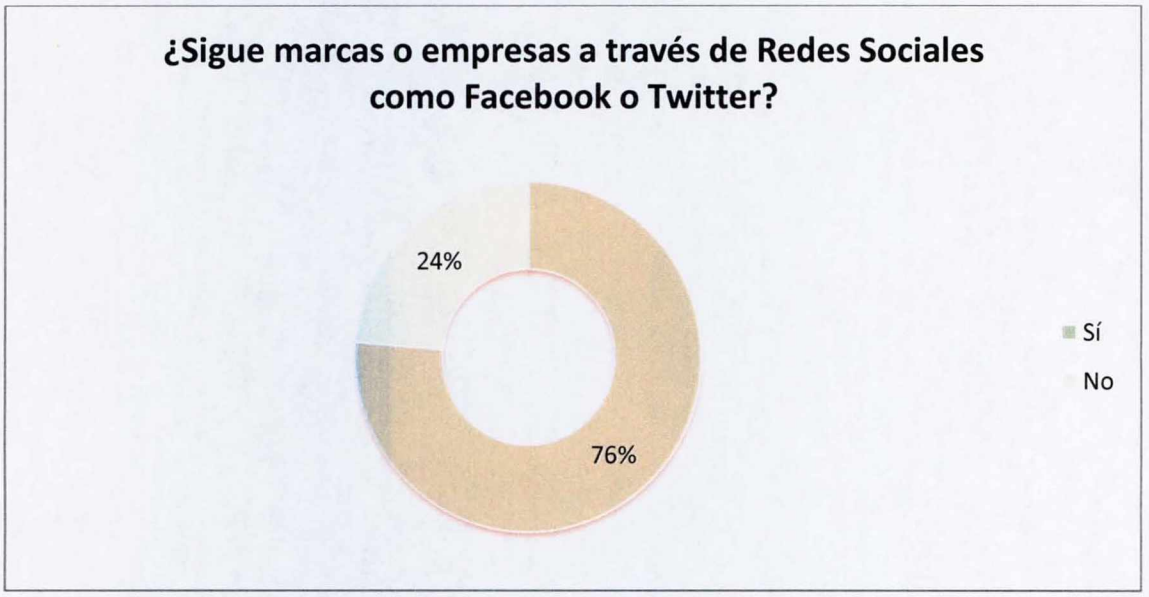
7.2 ENCUESTAS A USUARIOS SEGUIDORES DE MARCAS EN REDES SOCIALES

A través de un cuestionario estructurado (ver anexo) se ha publicado una encuesta online, la cual se ha difundido principalmente en la red social Facebook. Se eligió esta plataforma por ser la más utilizada por usuarios finales y la más popular en su categoría, donde la mayoría de las marcas tienen presencia para interactuar con sus adeptos.

7.2.1 Perfil de la muestra

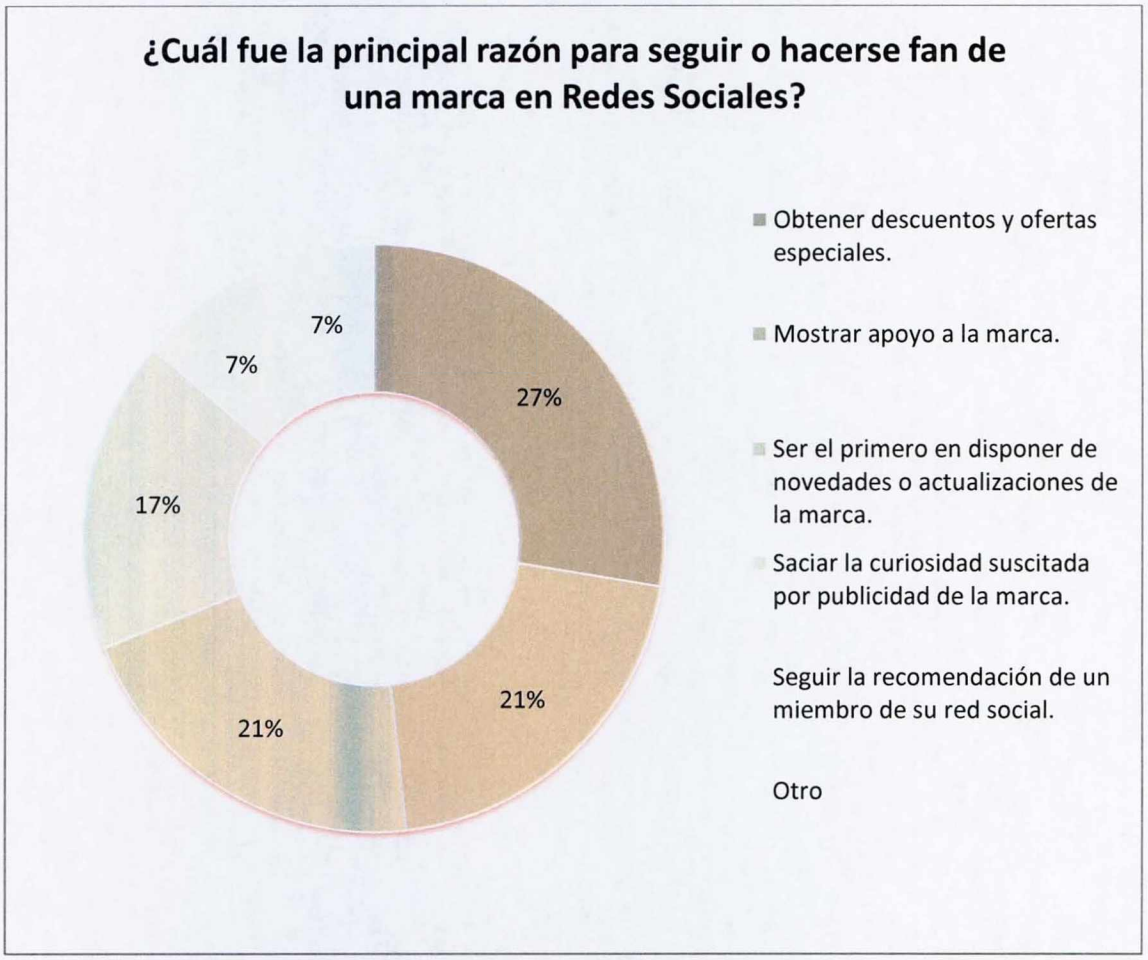
Participaron 37 usuarios de redes sociales, los cuales accedieron a la encuesta por medio de un enlace publicado en Facebook. 49% hombres y 51% mujeres. El 62% reside en Colombia, el 32% en Argentina y el restante 6% en México y Chile.

El 76% de los usuarios declaró que seguía a una o varias marcas o empresas en Redes Sociales. El 24% no lo hacía.

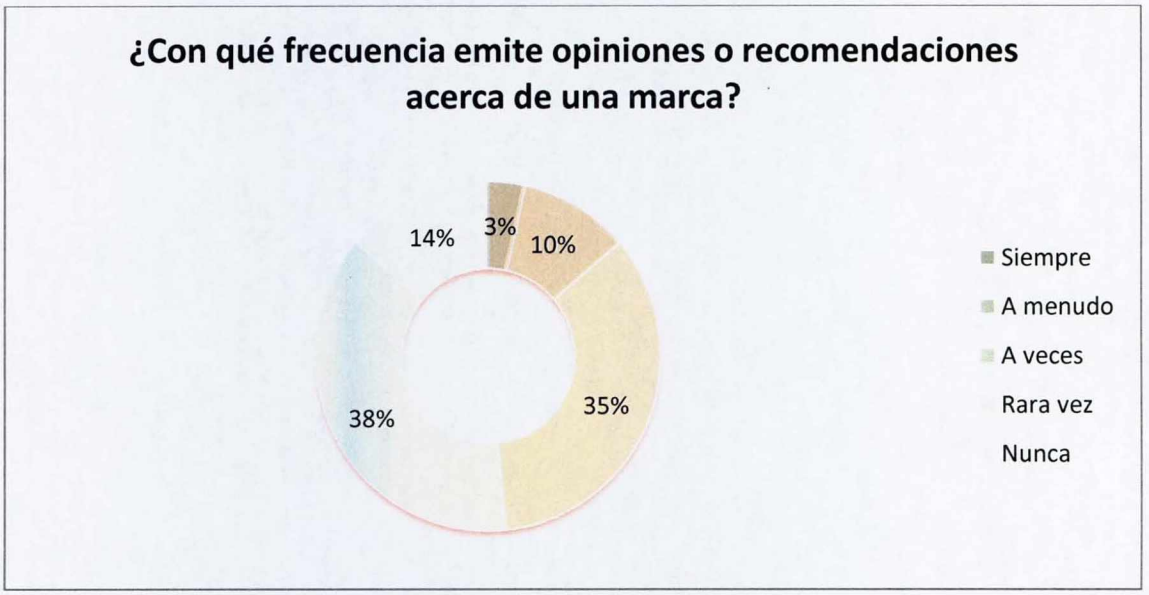


7.2.2 Relación con la marca

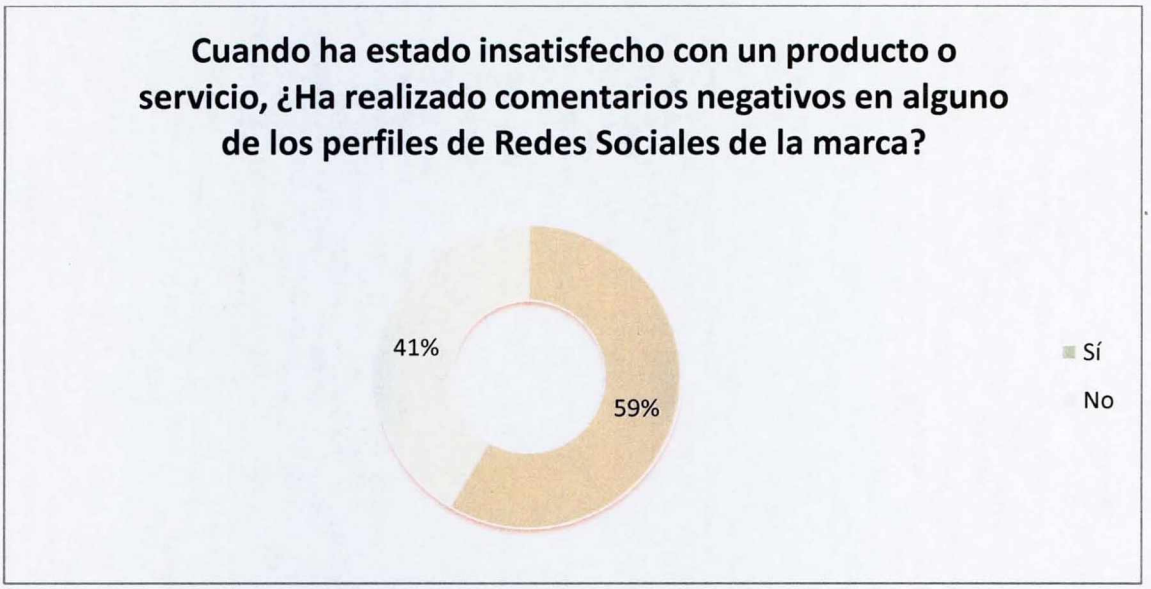
El 27% de los fans en Redes Sociales declararon que la principal razón para seguir una marca o empresa es obtener descuentos y ofertas especiales. El 21% lo hace para mostrar apoyo a la marca y otro 21% para ser el primero en obtener novedades acerca de la marca. Un 17% se hace fan gracias a la curiosidad generada por alguna publicidad. El 7% lo hace por recomendación y otro 7% lo hace por distintos motivos, como asistir a charlas o por simple gusto.



Aunque solamente el 3% emite siempre opiniones o recomendaciones, hay un 35% que declara hacerlo a veces y un 10% que lo hace a menudo. Las plataformas sociales están optimizadas y diseñadas para que los usuarios depositen allí sus experiencias y apreciaciones de los productos que consumen. De esta forma, una de las principales métricas para determinar el nivel de *engagement* de los fans es la cantidad de comentarios. Estos se dividen en positivos y negativos. A partir de esto se puede tener una idea del sentimiento hacia la marca, la principal métrica cualitativa en el monitoreo de reputación.



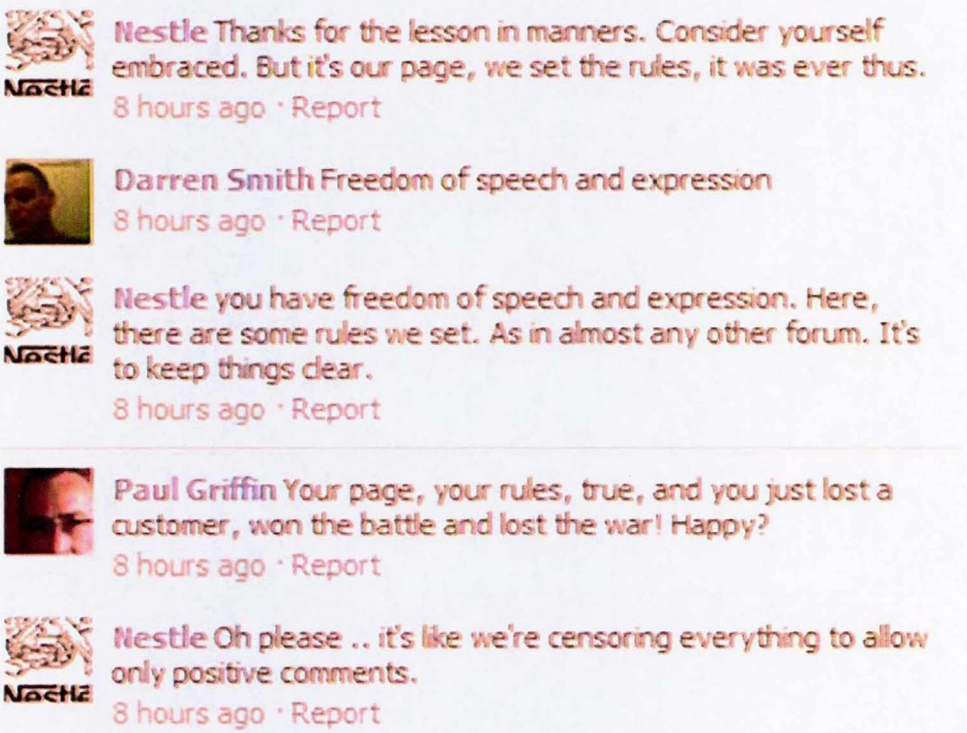
De la misma forma, el 59% de los encuestados declaró haber realizado comentarios negativos en algún perfil de Redes Sociales de una marca cuando ha estado insatisfecho con un producto o servicio. Los comentarios de estas características son públicos y los puede ver cualquier persona que ingrese a ese espacio virtual. Es posible borrarlos, aunque son bastantes los casos que han tenido efectos lamentables al realizar esa acción.



Uno de los casos más representativos de la mala gestión de comentarios fue el de Kit Kat de Nestlé[12]. En marzo del año 2010 el Community Manager intentó silenciar las

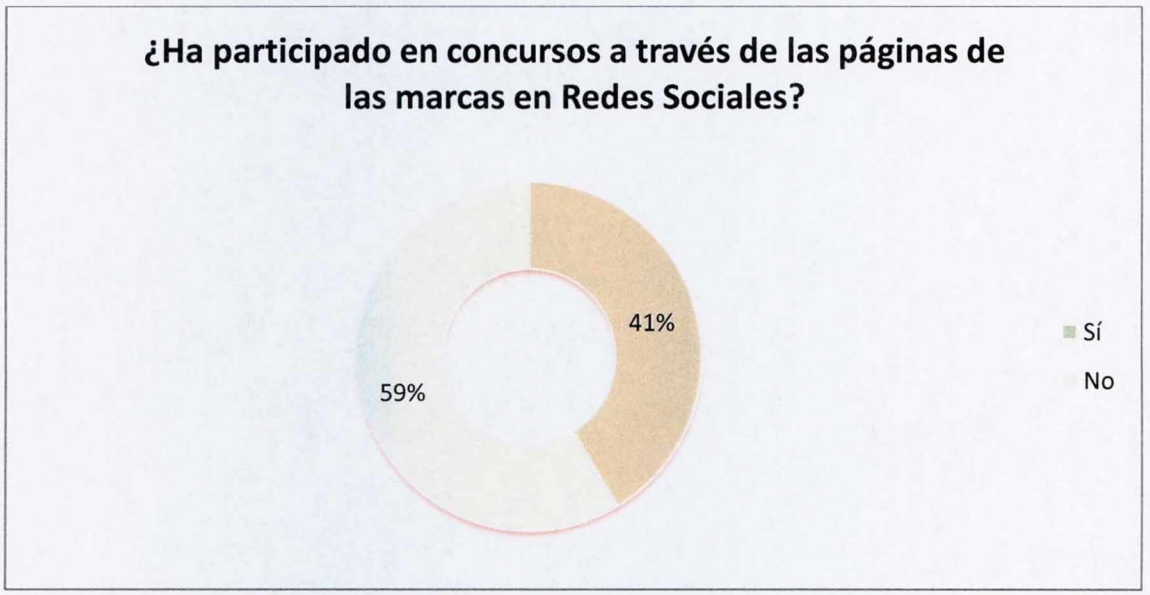
[12] http://www.internetadvantage.es/blog/marketing-social/el-caso-nestle-otro-fracaso-relaciones-publicas-en-redes-sociales/

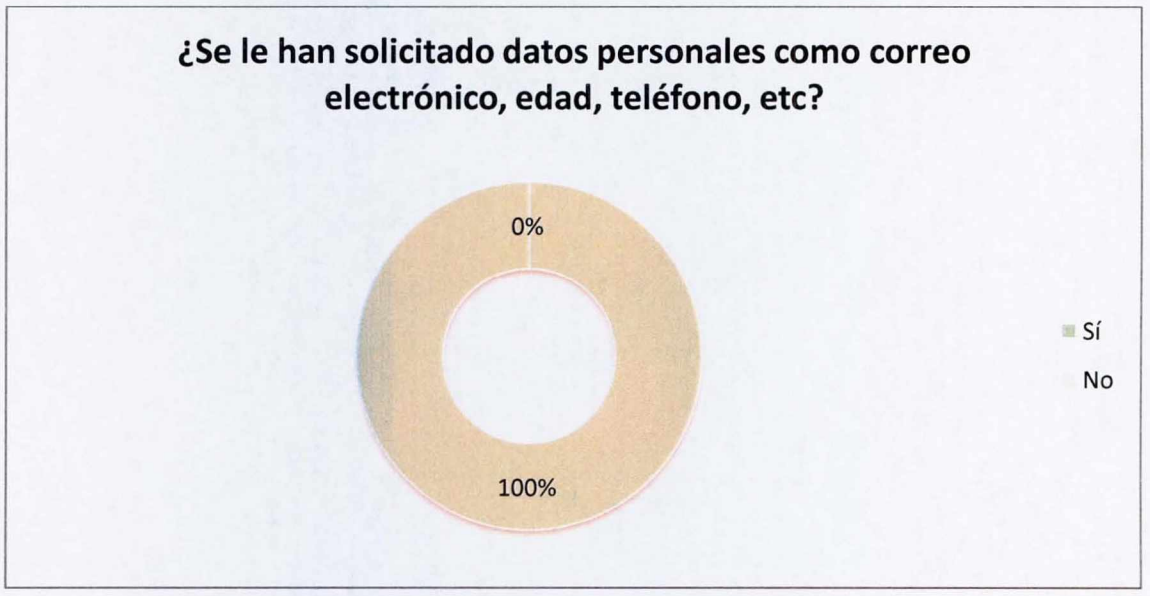
quejas de los fans ante una acción judicial de Nestlé contra Green Peace. El grupo activista alegaba la utilización de aceite de palma procedente de Indonesia para elaboración de los productos de dicho fabricante, destruyendo el habitat de una especie protegida como los orangutanes. La situación desató una gran cantidad de críticas dentro y fuera de los medios sociales hasta que un representante de la marca pidió disculpas por los errores cometidos y sus malas formas, anunciando que dejarían de eliminar los post de los fans.



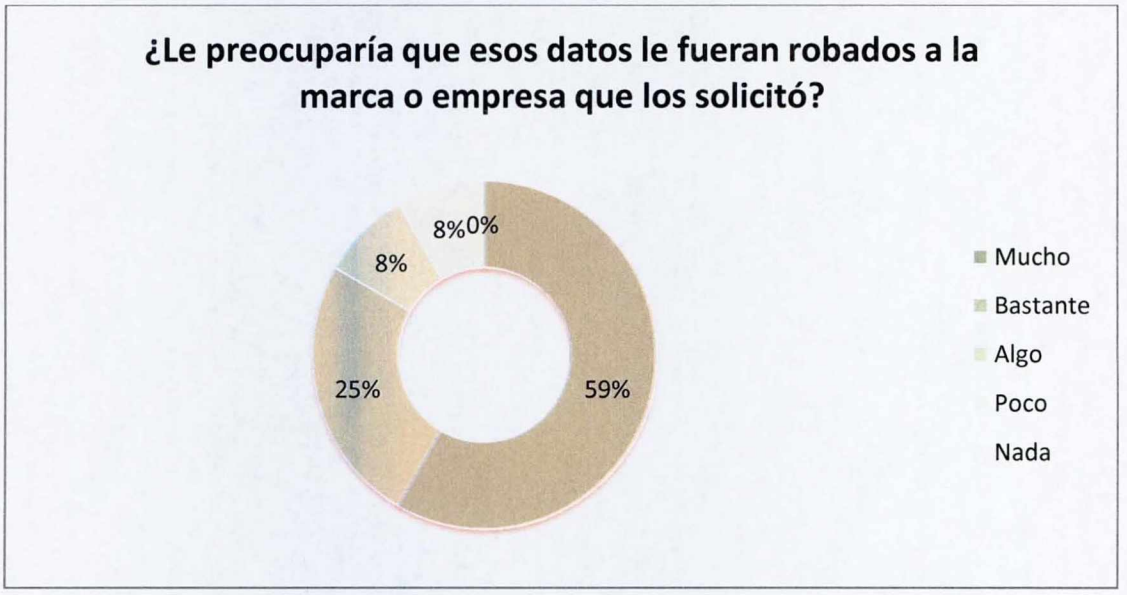
7.2.3 Privacidad y seguridad de los datos personales

El 41% de los seguidores de marcas en Redes Sociales ha participado en algún concurso realizado por las mismas. En todos los casos han tenido que proporcionar sus datos personales como nombre, dirección, e-mail, etc. Estos datos son sensibles teniendo en cuenta que la mayoría de las personas alojan información confidencial en sus cuentas de correo electrónico como contraseñas de otros servicios, documentos, fotografías y, en varios casos, datos bancarios. Las empresas deben contar con unas políticas de privacidad y confidencialidad en el manejo de esta información. A su vez, los atacantes informáticos buscan obtenerla para sacar rédito económico. Uno de los negocios más comunes es la venta de bases de datos para el envío de publicidad no deseada o *spam.*



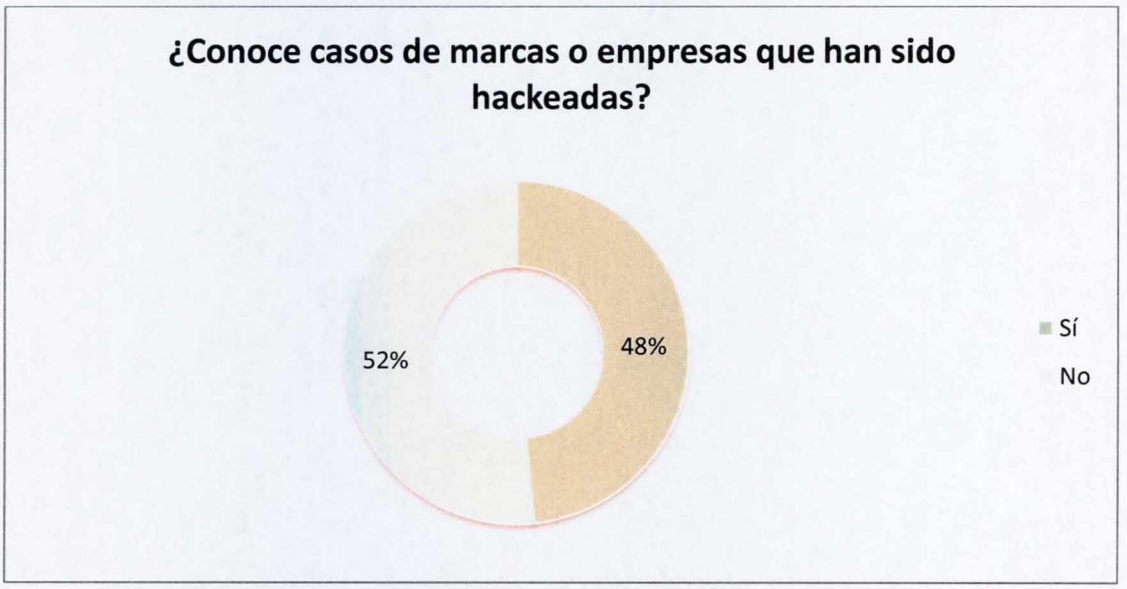


El 59% de los que han participado en concurso, en donde entregaron sus datos personales, manifestó que le preocuparía mucho si la empresa o marca perdiera sus datos en consecuencia de un ataque informático. Al 25% le preocuparía bastante y al restante 16% poco y nada.



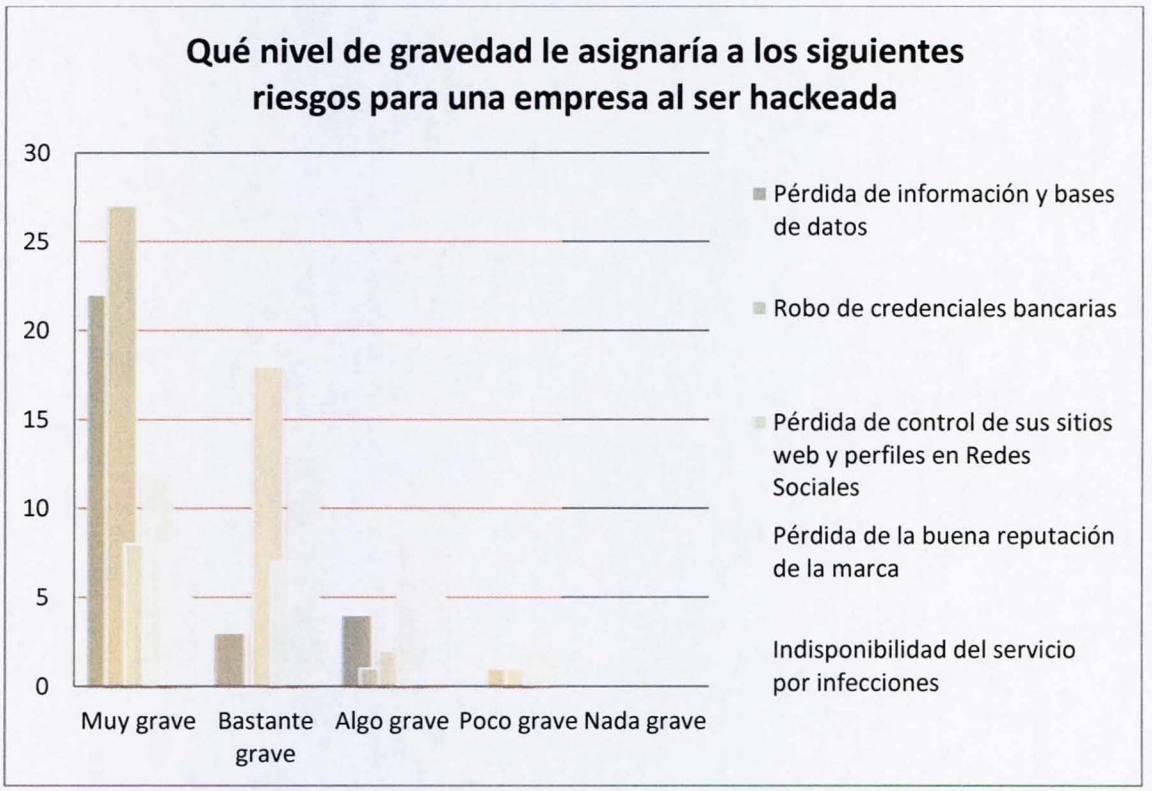
7.2.4 Ataques y amenazas en la red

El 48% de los usuarios de Redes Sociales afirmó conocer casos de empresas que fueron vulneradas a través de un ciber ataque. Gracias al poder que ahora tienen las personas para compartir contenidos en la red, es más fácil que este tipo de noticias se transmitan rápidamente. De esta manera el fenómeno "de boca en boca" se replica en este medio pero con más velocidad. El consumidor ha pasado a ser "prosumidor", un generador de contenidos y conversaciones alrededor de los productos. Ya no es la figura pasiva que recibe unidireccionalmente el mensaje de la marca.



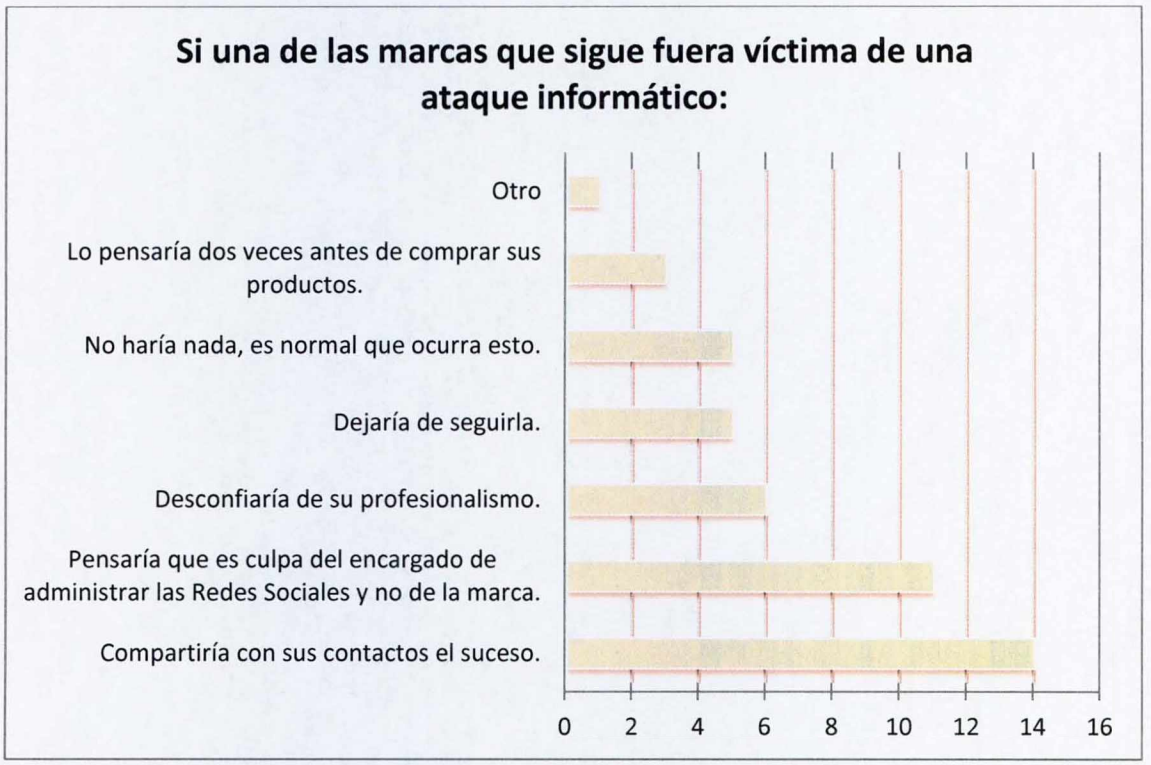
Se le pidió a los usuarios que le asignaran un nivel de gravedad a las diferentes consecuencias que sufriría una empresa al ser hackeada, es decir, al ser vulnerada por medios informáticos para obtener datos confidenciales de la misma.

El 93% consideró el robo de credenciales bancarias, muy grave, ya que esto implica directamente el robo de dinero. La siguiente consecuencia negativa considerada muy grave fue la pérdida de información y bases de datos con un 76%. La pérdida de control de sus sitios web y perfiles en Redes Sociales es bastante grave para el 62% de los encuestados, así como la Indisponibilidad del servicio por infecciones con un 45%. La pérdida de la buena reputación de la marca es bastante grave para el 24% y muy grave para el 41%. Ninguna de los efectos ante un ataque informático es catalogado como nada grave.



7.2.5 Reputación de marca

En el caso de que una empresa o marca fuera victima de un ataque informático, el 48,3% de los seguidores compartiría con sus contactos el suceso, lo cual, por la naturaleza de las redes sociales y el poder del fenómeno "boca en boca" podría desencadenar una cantidad exponencial de comentarios en torno a esa situación. Una de las principales funcionalidades de las Redes Sociales es la acción de "compartir". Se puede realizar con un solo clic y la información alcanza un nivel de exposición igual a la suma de los contactos de cada una de las personas que la comparta.



Un claro ejemplo fue lo que le sucedió en marzo de 2013 a la conocida cadena de comidas rápidas Burguer King. Como parte de una campaña hacktivista, el popular grupo *Anonymous* ingresó y tomó control de la cuenta oficial de Burger King aprovechando una contraseña débil utilizada por el Community Manager. Los atacantes modificaron toda la configuración de cuenta para hacer publicidad del principal competidor de la marca: McDonald's.

Transcurrida media hora, luego del ataque, la cuenta de Twitter sumó más de 9 mil nuevos followers[13] quienes, por supuesto, lo hicieron para hacer seguimiento al incidente y no por motivos de gusto hacia la marca.

El 38% de los usuarios pensaría que un incidente de este estilo es culpa del encargado de gestionar los perfiles sociales y no de la marca. EL 21% desconfiaría del profesionalismo y, consecuentemente, el 17% dejaría de seguir la marca después de que ésta fuera victima de un ataque informático. Esto refleja una pérdida de credibilidad en el liderazgo de la misma. Otro 17% de los encuestados considera que este tipo de sucesos son comunes y no reaccionarían de ninguna manera. El 10% aseguró que lo pensaría dos veces antes de comprar los productos pertenecientes a la marca. Y por último, un 2% esperaría una comunicado oficial por parte de la marca explicando las causas del acontecimiento.

[13] http://blogs.eset-la.com/laboratorio/2013/02/18/burger-king-o-mcdonalds-o-como-una-contrasena-debil-en-twitter-puede-danar-tu-imagen/

8. CONCLUSIONES

Las marcas tienen presencia en Redes Sociales sin tomar recaudos en temas de Seguridad de la Información.

El apuro por tener presencia en las Redes Sociales, sin una correcta planificación, hace que muchas marcas incursionen en este medio sin las debidas precauciones de seguridad. Como se pudo observar, los profesionales del Social Media, es decir, los Community Managers, no cuentan con una formación sólida en materia de seguridad de la información. Muchos de ellos aprendieron el oficio en base a su carrera de grado y la complementaron con algún curso básico, pero en ninguno de sus estudios vieron esta temática como contenido. Al desconocer el valor y riesgo de este oficio, muchas empresas contratan este servicio sin la conciencia de lo que este representa para la reputación de su marca.

El ataque informático a través de las Redes Sociales no es contemplado por las empresas ya que tradicionalmente se implementan las políticas de seguridad a los sitios web propios y a las redes internas. Por esta razón no se aplican estos criterios a la hora de elegir un gestor de perfiles en Redes Sociales ni a la configuración básica de sus cuentas en dichas interfaces.

Los ataques informático afectan la reputación de marca

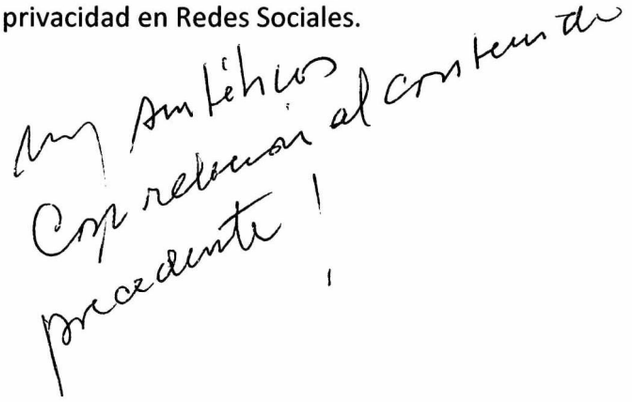
Los usuarios/consumidores presentes en Redes Sociales tienen ya implementadas las funcionalidades de compartir contenidos, presentes en estas plataformas. Estas se han convertido en arma de doble filo para las marcas ya que sirven para tanto para recomendar, como para desprestigiar. La primera acción ante un ataque informático que realizaría un usuario sería compartir la noticia con sus contactos. En consecuencia, se pierde la credibilidad en la marca, producto o empresa por parte de los consumidores.

Los programas académicos relacionados con el Community Management no incluyen la Seguridad Informática en sus temarios.

Por ser una profesión joven, el Community Management se encuentra en una etapa incipiente donde los contenidos se van desarrollando al ritmo de los avances tecnológicos y las necesidades que éstos planteen. Los cursos y diplomados en este oficio se centran en el conocimiento de las plataformas y conceptos de marketing en el social media y sus funcionalidades. Cuando se trata el tema de la reputación de marca, se abarca únicamente desde la opinión de los consumidores y la calidad de los productos pero no se contempla la opción de la seguridad y el manejo de los datos de los clientes.

Los Community Managers no están preparados para una crisis de reputación de marca por un ataque informático.

A pesar de contar con manuales de gestión de crisis, los profesionales del Community Management desconocen, en su mayoría, la repercusión de un ataque informático en la reputación de marca. Además, aunque conocen las amenazas presentes en Internet, no cuentan con buenas prácticas ni hábitos de navegación y configuración de la privacidad en Redes Sociales.



9. RECOMENDACIONES

Es necesario que las instituciones que ofrecen programas de formación afines con el oficio de Community Management, tales como Relaciones Públicas, Periodismo, Comunicación, Marketing, Publicidad, etc., implementen en sus programas la materia de Seguridad Informática, ya que aplica para cualquier uso que se le de a Internet. Ya sean como usuarios o administradores, los roles que desempeñen en este medio están en riesgo de ser victimas de cualquier amenaza cibernética.

Aunque los programas académicos aún no lo contemplen, los profesionales del Social Media deben instruirse a fondo en materia de Seguridad Informática para proteger su oficio y a las marcas que representan. De esta manera cubrirán, por ahora, los contenidos faltantes en su formación.

A continuación se pone a disposición una Guía Básica de Seguridad Informática para Community Managers, la cual servirá como base para la protección de la información y la que deberá actualizarse constantemente con el avance de las tecnologías y los cambios en las plataformas. Sin embargo, la precaución y los buenos hábitos de navegación son un punto de partida inmutable.

9.1 GUÍA PARA LA PROTECCIÓN DE LA REPUTACIÓN EN REDES SOCIALES

9.1.1 Glosario básico de Seguridad Informática

Definiciones tomadas del "Diccionario de Seguridad Informática. Edición 2012" editado por la firma de Antivirus ESET Latinoamérica.

Anonymous: seudónimo para referirse a distintos grupos hacktivistas que operan desde varios países a través de Internet. Debido a la reciente masificación de sus acciones, es difícil determinar si una amenaza específica será concretada o no. Ataques de estos grupos han sido dirigidos a sitios del gobierno peruano, del Senado Argentino, del Proyecto Hidroaysén de Chile y de la Ley Sinde de España, entre otros.

Antispam: herramienta que identifica y filtra correo no deseado con el objetivo de evitar que llegue al usuario. De esta forma, se evita la pérdida de productividad que estos correos producen y se minimizan los riesgos en cuanto a las amenazas que por estos circulan (como malware o *phishing*). Las técnicas de filtrado van desde detección de palabras comunes del *spam* hasta listas de correo basura definidas por el usuario o listas mayores ubicadas en servidores remotos.

Atacante: persona que atenta intencionalmente contra la seguridad y normal funcionamiento de un sistema informático. Suele tener como objetivo último la obtención de un beneficio económico o el robo de información confidencial.

Botnet: red de equipos infectados por códigos maliciosos que son controlados por un atacante de modo transparente al usuario, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cada sistema infectado, al que suele llamarse zombi, interpreta y ejecuta las órdenes emitidas. Ofrece a los delincuentes una fuente importante de recursos que pueden trabajar de manera conjunta y distribuida. Mayormente se utilizan para el envío de *spam*, el alojamiento de material ilegal o la realización ataques de denegación de servicio distribuido.

Certificado digital: archivo con carácter de documento emitido por una autoridad de certificación que asocia una entidad con una clave pública. Garantiza la confidencialidad de la comunicación llevada a cabo entre la misma y los usuarios. Es utilizado, entre otras cosas, en los sitios web que utilizan el protocolo https.

Código malicioso: conocido también como malware, programa o aplicación diseñado con algún f in dañino. Se consideran malware a distintos tipos de amenazas, cada una con características particulares.

DDoS: ataque distribuido de denegación de servicio, por sus siglas en inglés "*Distributed Denial of Service*". Ampliación del ataque DOS que se lleva a cabo generando un gran flujo de información desde varios puntos de conexión, por lo general a través de una *botnet*. El ataque se realiza a través del envío de determinados paquetes de datos al servidor, de forma tal de saturar su capacidad de trabajo y forzar que el servicio deje de funcionar.

Delito informático: crimen que utiliza medios electrónicos o comunicaciones basadas en Internet u otras tecnologías para llevarse a cabo. Los delitos informáticos son uno de los componentes que conforman el cibercrimen.

Exploit: aplicación o fragmento de código utilizado para aprovechar una vulnerabilidad o defecto del sistema. Al ejecutarse, altera el funcionamiento normal del sistema víctima, realizando acciones no previstas o inesperadas como, por ejemplo, desbordamiento de buffer o ejecución de código no autorizado.

Firewall: dispositivo de hardware, software o ambos diseñado para controlar el tráfico de una red en base a políticas predefinidas.

Fuga de información: incidente que se produce cuando datos relevantes para una organización son accedidos por personas no autorizadas. Generalmente se afecta la confidencialidad de la información.

Gusano: programa malicioso que cuenta con la capacidad de auto-reproducción, al igual que los virus, pero con la diferencia que no necesita de un archivo anfitrión -archivo que aloja una porción de código malicioso- para la infección. Generalmente modifica el registro del sistema para ser cargado cada vez que el mismo es iniciado. Suelen propagarse a través de dispositivos USB o vulnerabilidades en los sistemas.

Hacktivismo: acrónimo de "hacker" y "activismo". Es la utilización de técnicas de ataques informáticos por parte de personas o grupos con intenciones ideológicas. Por ejemplo, suelen realizarse modificaciones paródicas de contenido web o ataques de denegación de servicio (DoS) con el fin de realizar protestas en referencia a temas sensibles como la política, los derechos humanos o la libertad de expresión, entre otros.

Hoax: en español, "bulo". Correo electrónico o mensaje en redes sociales con contenido falso o engañoso que se distribuye en cadena debido a su temática impactante que parece provenir de una fuente fiable o porque el mismo mensaje pide ser reenviado. Es muy común que se anuncien potentes amenazas informáticas, la noticia del cierre de algún servicio web o se solicite ayuda para personas enfermas. El objetivo de este tipo de engaños suele ser recolectar direcciones para el envío de spam, generar incertidumbre entre los receptores o simplemente diversión.

Ingeniería social: conjunto de técnicas utilizadas para engañar a un usuario a través de una acción o conducta social. Consiste en la manipulación psicológica y persuasión para que voluntariamente la víctima brinde información o realice algún acto que ponga a su propio sistema en riesgo. Suele utilizarse este método para obtener contraseñas, números de tarjetas de crédito o pin, entre otros.

Keylogger: en español, "registrador de teclas". Tipo de software que registra las teclas pulsadas en un sistema para almacenarlas en un archivo o enviarlas a través de Internet. Suele guardar contraseñas, números de tarjeta de crédito u otros datos sensibles. En la actualidad se pueden encontrar versiones más nuevas de esta herramienta fraudulenta capaces de realizar capturas de pantalla cuando se registra un clic, haciendo que estrategias de seguridad como el uso del teclado virtual sean obsoletas.

Malvertising: acrónimo de las palabras "*malicious*" (del inglés, "malicioso") y "*advertising*" (del inglés, "publicidad"). Técnica utilizada para insertar publicidades con contenido malicioso en los anuncios que se muestran en sitios web legítimos.

Parche de seguridad: actualización que se aplica a un software para resolver vulnerabilidades. Por lo general, no modifica la funcionalidad sino que corrige problemas de seguridad.

Password stealer: tipo de troyano que tiene como objetivo robar la información introducida en los formularios web de autenticación, entre la que se encuentra nombre de usuario y contraseña.

Pharming: tipo de ataque que permite redireccionar un nombre de dominio a una dirección IP distinta de la original. El objetivo de este ataque consiste en dirigir al usuario a una página web falsa a pesar de que éste ingrese la dirección URL correcta. El

ataque suele realizarse sobre servidores DNS (en inglés, "*Domain Name System*") globales o en un archivo ubicado en el equipo víctima (*pharming* local).

Phishing: ataque que se comete mediante el uso de Ingeniería Social con el objetivo de adquirir fraudulentamente información personal y/o confidencial de la víctima, como contraseñas y/o detalles de la tarjeta de crédito. Para efectuar el engaño el estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza utilizando una aparente comunicación oficial electrónica como correos electrónicos, sistemas de mensajería instantánea o incluso llamadas telefónicas. Los casos de *phishing* más comunes toman como objetivo de ataque a clientes de grandes entidades financieras y suelen contener algún tipo de amenaza de interrupción del servicio u otras consecuencias indeseables, si las instrucciones que indican no se realizan.

Política de seguridad: conjunto de reglas y procedimientos para la regulación de las prácticas de los usuarios con el fin de evitar el uso indebido de los sistemas informáticos que pueda derivar en problemas en los mismos y en la seguridad de la información de la organización. El documento que plasma las políticas de seguridad de una empresa debe ser válido para cualquier integrante de la organización y debe describir los fundamentos de las medidas de seguridad: qué se desea proteger y cómo se lo desea proteger.

Protocolo: sistema de formato de mensajes que permite el intercambio de los mismos entre diferentes dispositivos informáticos y comunicacionales mediante una red, estableciendo distintas reglas que determinan la sintaxis, semántica y sincronización de la comunicación. Pueden ser implementados tanto a nivel de software como de hardware.

Ransomware: código malicioso que cifra la información del equipo infectado y solicita dinero para devolver al usuario el poder sobre los mismos. La contraseña para el descifrado es entregada luego de realizado el pago, según las instrucciones dadas por atacante. En la mayoría de los casos, el ataque afecta sólo a ciertos archivos, siendo los más comúnmente perjudicados los de ofimática- como procesadores de texto, hojas de cálculo o diapositivas, las imágenes y los correos electrónicos.

Robo de identidad: incidente que se produce cuando un atacante obtiene información privada de un usuario y la utiliza para suplantar la identidad de la víctima.

Rogue: programa que simula ser una solución antivirus o de seguridad, generalmente gratuita, pero que en realidad es un programa dañino. Este tipo de ataque comienza con la muestra de ventanas de advertencia, llamativas y exageradas, acerca de la existencia de software malicioso en el sistema. De esta manera se instiga al usuario a la descarga de una falsa aplicación de seguridad (con la finalidad de instalar malware en la computadora) o a su compra (obteniendo el correspondiente rédito económico).

Scam: estafa realizada a través de medios tecnológicos como el correo electrónico o sitios web falsos. Se trata de un delito que consistente en provocar un perjuicio patrimonial a alguien mediante el engaño y con ánimo de lucro, utilizando para ello la tecnología. Las técnicas utilizadas principalmente para engañar al usuario son el anuncio de una ganancia extraordinaria o las peticiones de ayuda caritativa. En el primer caso aparecen, por ejemplo, los anuncios de empleo con rentabilidades inesperadas o el premio de una lotería o juegos de azar por el cual se le solicita al usuario que haga una entrega de una pequeña suma de dinero para verificar datos o cubrir los costos de envío y administración del dinero obtenido. El segundo caso, y el más común, consiste en la solicitud de una donación al usuario para una obra caritativa. Los contenidos más generales hacen referencia a países de extrema pobreza (generalmente de África), a personas enfermas o a catástrofes internacionales. El correo invita a la víctima a hacer un depósito o envío de dinero a fin de colaborar.

Script: porción de código que se inserta en un sitio web para ejecutar instrucciones ante la ocurrencia de un evento, como hacer clic en un botón o durante la carga de la página web. Se dice también de un archivo formado por un conjunto de instrucciones que son ejecutadas línea por línea.

Seguridad de la información: disciplina que establece un conjunto de normas dentro de una organización para el resguardo de la información. Busca conservar la integridad, confidencialidad y disponibilidad de la misma.

Seguridad informática: disciplina dedicada al resguardo y protección de los sistemas informáticos, la información contenida en ellos y sus usuarios.

Spam: correo no deseado o correo basura envía do de forma masiva por un remitente desconocido, ya sea en formato de texto o con contenido html. Es utilizado, por lo general, para envío de publicidad, aunque también se lo emplea para la propagación de códigos maliciosos. Sirve también como puerta para cometer *scam* o *phishing*. Representa un riesgo para la seguridad y tiene efectos secundarios, como el impacto negativo en la productividad del personal por la lectura de los mismos y el aumento del consumo de recursos (ancho de banda, procesamiento, etc). A su vez, puede manifestarse en comentarios de foros, blogs o en mensajes de texto. Inicialmente, el *spam* fue utilizado para enviar mensajes en formato de texto. Sin embargo, con la creación de filtros *anti-spam* se comenzaron a identificar este tipo de mensajes, y posteriormente, el *spam* evolucionó a correos con imágenes o

Spyware: aplicación espía que recopila información sobre los hábitos de navegación, comportamiento en la web u otras cuestiones personales de utilización del sistema del usuario sin su consentimiento. Posteriormente, los datos son enviados al atacante. No se trata de un código malicioso que dañe al ordenador, sino que afecta el rendimiento de del equipo y la privacidad de los usuarios. Sin embargo, en algunos casos se producen pequeñas alteraciones en la configuración del sistema, es especialmente en las configuraciones de Internet o en la página de inicio. Puede instalarse combinado

con otras amenazas (gusanos, troyanos) o automáticamente. Esto ocurre mientras el usuario navega por ciertas páginas web que aprovechan vulnerabilidades del navegador o del sistema operativo, que permiten al spyware instalarse en el sistema subrepticiamente.

Troyano: programa malicioso que simula ser una aplicación indefensa. Se instala y ejecuta como un software legítimo pero realiza tareas maliciosas sin conocimiento del usuario. A diferencia de los gusanos y virus, no tiene capacidad de replicarse a sí mismo. Los troyanos pueden ser utilizados para muchos propósitos, entre los que se encuentran el acceso remoto al equipo que permite que el atacante pueda conectarse remotamente al mismo, el registro de todo lo tipeado y el robo de contraseñas e información del sistema. El nombre de esta amenaza proviene de la leyenda del caballo de troya, ya que logra su éxito al engañar al usuario.

Typosquatting: técnica que consiste en registrar nombres de dominios similares a otros populares. El atacante espera que un usuario cometa un error de tipeo e ingrese a estos sitios para cometer fraudes como *phishing*, propagación de malware o publicidad no deseada.

Virus: programa malicioso creado para producir algún daño en el ordenador, desde mensajes molestos en pantalla y la modificación o eliminación de archivos hasta la denegación completa de acceso al sistema. Tiene dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo. Requiere de un anfitrión -archivo que aloja una porción de código malicioso- para alojarse, tal como un archivo ejecutable, el sector de arranque o la memoria de la computadora. Al ser ejecutado, se produce el daño para el que fue concebido y luego se propaga para continuar la infección de otros archivos.

Vulnerabilidad: falla en el desarrollo de una aplicación que permite la realización de alguna acción indeseada o incorrecta. Es una característica de un sistema susceptible o expuesta a un ataque. Pone en riesgo la información de los usuarios.
Zombi: computadora infectada y controlada de manera remota por un atacante. Una red formada por zombis se conoce como *botnet*.

9.1.2 Consejos y buenas prácticas para Community Managers

Seguridad en Redes Sociales

Contraseñas:

- No compartir las contraseñas de accesos a las cuentas de Facebook, Twitter y demás plataformas sociales.
- Utilizar una contraseña diferente para cada servicio y cliente.
- Utilizar contraseñas fuertes para evitar que alguien pueda adivinarlas.

Al crear una cuenta en un sitio web, siempre se deben utilizar claves que sean una combinación de números, letras mayúsculas y minúsculas y de ser posible utilizar caracteres especiales. De esta manera, la posibilidad de que un atacante descubra la contraseña es mínima. Distintos estudios han demostrado que los usuarios no suelen utilizar contraseñas fuertes para acceder a sus cuentas en Internet, lo que presenta una puerta de entrada para los atacantes. Algunos ejemplos de claves fuertes son "Jos33ntr@", "C0ntr@z3n@#", "Jp3t?xi9-", "4ApEKzqK" o "L@#nt67nx".

- Evitar acceder a redes sociales y otros servicios donde se maneje información privada desde equipos desconocidos que no sean propios, ya que podrían tener alguna aplicación para capturar las contraseñas.

Confidencialidad:

- No compartir información confidencial en Internet que pueda ser utilizada por cibercriminales para conocer datos personales y tener acceso a los sistemas.
- Contar con soluciones de seguridad en el equipo, como un antivirus y un firewall, que protejan ante virus, gusanos y troyanos que pudieran robar archivos del sistema.
- Configurar las políticas de privacidad en las redes sociales. Al utilizar redes sociales como Facebook, Twitter o Google+, los usuarios suelen dejar de lado los parámetros de privacidad y compartir no solo su información, sino que también comparten los datos de sus contactos con cualquier persona que acceda a su perfil. La configuración de las políticas de privacidad es una de las barreras a implementar para evitar que un atacante recopile información confidencial.

Conectividad:

- Utilizar una conexión segura. Al entrar a un sitio web, asegurarse de que la conexión sea a través de HTTPS (*Hipertext Transfer Protocol Secure*). Al acceder a una página web a utilizando este protocolo, la comunicación entre el cliente y el servidor viaja cifrada, lo que aumenta la seguridad y minimiza la posibilidad del robo de contraseñas. Es posible configurar una conexión segura en las Redes Sociales, para que toda la comunicación con el sitio sea cifrada.
- Cuidar la información en sitios públicos
- Si se decide conectarse a una red inalámbrica pública, se debe prestar atención a la seguridad de la misma. Se recomienda no acceder a sitios como la banca electrónica, ya que un atacante podría estar analizando el tráfico de la red y robar su información.

Navegación:

- Cuando se reciben correos electrónicos de dudosa procedencia, como por ejemplo de un contacto que habla en español si se recibe un correo en portugués, un supuesto correo de una entidad bancaria para actualizar la información, cadenas de correo acerca del cambio de un servicio de correos gratuito a pago o un multimillonario que quiere regalar su dinero.

- Buscar información de forma segura. Al intentar acceder a información a través de buscadores como Google, Bing o Yahoo!, el Community Manager podría ser víctima del *BlackHat* SEO y enlazado a una página falsa desde donde podría descargar una falsa solución de seguridad u otros códigos maliciosos. Estas metodologías de propagación de malware, utilizan acontecimientos de repercusión mundial para atraer la atención de los usuarios al intentar informarse de las noticias de último momento.

Hábitos:

- Analizar los dispositivos extraíbles. Los medios de almacenamiento externo, en dónde se incluyen a las los dispositivos USB son uno de los canales de propagación de códigos maliciosos más comunes. Al conectar una memoria en una computadora desconocida, los usuarios suelen infectar sus dispositivos y luego utilizarlos para transportar información del trabajo. De esta manera un Community Manager que no analice su dispositivo USB podría infectar toda la red de la empresa.
- Analizar los archivos adjuntos que llegan por correo electrónico o a través de Redes Sociales y demás servicios de Internet.
- Actualizar los programas y el sistema operativo. Tanto los distintos sistemas operativos (Windows, Mac OS, o las distintas distribuciones de GNU Linux) como las aplicaciones que se pueden instalar en ellos (navegadores web, aplicaciones de oficina, reproductores de video, programas de diseño, etc.), cuentan con actualizaciones de seguridad que solucionan distintos inconvenientes que podrían llevar a la infección del equipo. Si el Community Manager no realiza la instalación de estas actualizaciones, deja su sistema vulnerable a una posible infección con un código malicioso que convierta su equipo en parte de una red de computadoras zombis, conocidas como *botnet*.
- Descargar aplicaciones desde sitios web oficiales: muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema.
- Evitar el ingreso de información personal en formularios dudosos: cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio. Una buena estrategia es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información.
- Evitar la ejecución de archivos sospechosos: la propagación de malware suele realizarse a través de archivos ejecutables Cuando se descargan archivos de redes P2P, se sugiere analizarlos de modo previo a su ejecución con una solución de seguridad.

Transacciones:

- Verificar que la dirección del sitio corresponda con la del sitio que se quiere utilizar, una letra de más, un número extraño, pueden indicar que es un sitio potencialmente peligroso. Lo mas indicado es escribir directamente la dirección y no seguir enlaces que lleguen por correo electrónico o que se encuentren en páginas poco confiables.
- Leer las políticas y normativas del sitio.
- Muchas transacciones en línea son respaldadas con tarjetas de crédito o débito, es recomendable revisar el movimiento de las mismas una vez finalice la transacción para comprobar que todo ha ocurrido según lo esperado.
- Cuando se acceda a sitios para hacer transacciones utilizar dispositivos de total confianza, nunca hacerlo desde dispositivos de uso público, ya que pueden tener software malicioso que capture la información personal.
- No escribir información personal indiscriminadamente, es necesario asegurarse en que sitios está dejando la información y si se cumple con las características de seguridad mencionadas.

Movilidad:

- Si se accede a Redes Sociales desde un dispositivo móvil, configurarlo el para que la opción de bloqueo de pantalla se active en el momento que no se esté utilizando para evitar accesos no autorizados a través de los cuales se ponga en riesgo la información contenida en el mismo.
- Si el dispositivo móvil puede conectarse a una red celular, debe activarse la opción de bloqueo de tarjeta SIM, de tal forma que en el momento de encender el dispositivo solicite el código PIN. Con esto se restringe el acceso al uso de estos recursos en caso de robo o pérdida del mismo.
- No instalar aplicaciones descargadas directamente de páginas que no estén avaladas por los fabricantes del dispositivo o por los desarrolladores del sistema operativo. Esto con el objetivo de no instalar aplicaciones desarrolladas con algún contenido malicioso.
- Antes de descargar una aplicación es buena idea leer las críticas y las reseñas que otros usuarios han hecho o lo que se publica en medios reconocidos. Esto puede ayudarle al usuario a saber cuáles son las principales características de la aplicación antes de descargarla e instalarla.
- Antes de instalar o actualizar alguna aplicación, es recomendable verificar que tipo de recursos o permisos requiere la aplicación. Es muy importante que el Community Manager sea cuidadoso con aplicaciones que piden permisos para hacer cosas más allá de las necesarias.
- Gestionar las aplicaciones que se utilizan en el dispositivo, para no llenarlo de programas que además de disminuir el rendimiento del dispositivo, pueden generar una vulnerabilidad de seguridad para el usuario.

10. BIBLIOGRAFÍA

AERCO y Territorio creativo. "La función del Community Manager", Documento distribuido por Puromarketing.com, edición digital. Noviembre 2009

ASENSIO, Gonzalo. "Seguridad en Internet: una guía práctica y eficaz para proteger su PC con software gratuito" , Ediciones Nowtilus S.L., 2006.

GITMAN, Lawrence J. "Fundamentos de Administración Financiera", Editorial Harla S.A., México, 1992.

GUILTINAN, Joseph P. y Gordon W, Paul. "Administración de Mercadeo. Estrategias y Programas", McGraw-Hill, México, 1984.

KOTLER, Philip, "Marketing 3.0", Lid Editorial Empresarial, 2010.

KOTLER, Philip, "Marketing Insights from A to Z: 80 Concepts Every Manager Needs to Know ", John Wiley & Sons Ltd, 2003.

KOTLER, Philip, "Marketing 3.0: From Products to Customers to the Human Spirit", John Wiley & Sons Ltd, 2010.

KOTLER, Philip, "Principios de marketing", Prentice Hall, Edición: 12, 2008.

LEVINE, Rick; LOCKE, Christopher; SEARLS Doc; WEINBERGER David. The Cluetrain Manifesto: The End of Business as Usual, Basic Books, 2001.

PORTER, Michael E, "Estrategia competitiva: Técnicas para el análisis de la empresa y sus competidores", Piramide Ediciones Sa, 2010.

PORTER, Michael E, "Ser competitivo (edición actualizada)", Deusto Ediciones SA, 2009.

PORTER, Michael E. "Ventaja competitiva: Creación y sostenibilidad de un rendimiento superior", Piramide Ediciones Sa, 2010.

RIES Laura Ries y RIES Al. "Las 22 leyes inmutables de la marca", Mc Graw-Hill, 2000.

RIES, Al y TROUT, Jack. "Posicionamiento", Mc Graw Hill, 2005.

Sitios web de consulta:

Las 5 fuerzas de Porter
http://managersmagazine.com/managersmagazine/articulos/2015/06/15-fuerzas-de-michael-porter

Libro online Marketing Siglo XXI
http://www.marketing-xxi.com/

Seguridad Informática
http://blogs.eset-la.com/
http://blogs.protegerse.com/
http://www.eset-la.com/
http://www.pandasecurity.com/
http://www.seguridad.unam.mx/
http://www.pcsecure.com.mx/
http://www.segu-info.com.ar/

Wikipedia. Artículo: Historia de Internet,
http://es.wikipedia.org/wiki/Historia_de_Internet

ANEXO 1

Junio de 2013

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Por este medio informo que he tenido revisiones puntuales y apruebo la entrega del trabajo final de la Licenciada Diana Lorena Lesmes Buitrago, inscripta en el Plan de Estudios de la Carrera de Especialización en Dirección y Gestión de Marketing y Estrategia Competitiva.

Saluda atentamente,

Daniela Buján
Marketing Services & Projects Manager
ESET Latinoamérica

Daniela Buján

Firma y aclaración

ANEXO 2

DANIELA BUJÁN - CURRICULUM VITAE
Marketing Services & Projects Manager at ESET Latinoamérica
daniela[illegible]@gmail.com
http://ar.linkedin.com/in/daniel[illegible]

EXPERIENCIA

Marketing Services & Projects Manager at ESET Latinoamérica
Como Mktg S&P Manager, estoy a cargo de dos subáreas del departamento, una relacionada a la organización de eventos y exposiciones, y la otra al desarrollo de proyectos y campañas de marketing que apuntan a alcanzar diferentes objetivos de marketing y comerciales de la compañía, como por ejemplo la generación de herramientas para el canal de distribución, campañas de *branding*, generación de leads, etc.

Coordinadora de Proyectos de Marketing at ESET
En este puesto, desarrollé e implementé diferentes proyectos de marketing de la empresa, muchos de ellos especialmente orientados a marketing de reclutamiento y fidelización de canales. También, trabajé en campañas de publicidad asociadas a la generación de leads, *awareness* de marca y de productos, lanzamientos de nuevos productos, entre otras. Colaboré con la organización de eventos internos de la empresa.

Analista de Marketing at ESET
Como Analista de Marketing de ESET Latinoamérica, contribuí con la organización de los eventos en donde participaba la empresa y los distribuidores de cada país. Trabajé en la creación de algunos anuncios gráficos y piezas online para diferentes campañas, así como también en la organización y el desarrollo de diferentes materiales para las acciones de marketing en Brasil.

Responsable de Marketing y Publicidad at ELSERVER.COM
Mi posición tuvo por objetivo dar a conocer la empresa, sus productos/servicios, promociones y comunicados institucionales al público objetivo y a la comunidad; ubicando a la marca bajo el posicionamiento deseado. Algunas de las actividades que desarrollé para alcanzar ese objetivo fueron: Desarrollo del plan de comunicación. Coordinación con diseñadores y redactores del armado de piezas para campañas publicitarias online. Desarrollo de nuevos canales de ventas. Creación de alianzas comerciales y gestión de las mismas. Manejo de la carera de clientes de alianzas comerciales, cortesías y cuentas especiales. Generación de acciones para unificar criterios de comunicación internos, gestionando junto con RRHH, la implementación

del estilo de comunicación. Armado de propuestas para fidelización y retención de clientes, y manejo de proveedores. Reporte de resultados a la Dirección Comercial.

Asistente de Marketing at ELSERVER.COM
Mi objetivo en este puesto estaba orientado a contribuir a la fidelización y retención de clientes existentes, captación de nuevos clientes y posicionamiento de la marca. Algunas de las tareas que realicé durante este período fueron: Atención y seguimiento de cartera de alianzas comerciales. Planificar, armar presentaciones y asistir en la implementación de campañas de comunicación que difundan la información sobre la empresa para alcanzar objetivos comerciales y comunicacionales. Difusión y ejecución de mecánicas promocionales. Redacción y difusión de comunicados de la empresa y gestión de publicaciones de prensa. Realización de campañas online a través de Google AdWords. Organización de eventos. Coordinación de armado y envío de *newslettter* a clientes.

Asistente de Cuentas BTL at Arthur Newton Comunicación
El objetivo de este puesto era atender las cuentas de la agencia y asistir en la planificación y desarrollo y ejecución de las propuesta a realizar según la necesidad de cada cliente. Las tareas comprendidas dentro de este puesto fueron: Atención de Cuentas de la agencia. Solicitudes de presupuestos, armado de mecánicas y ejecución de promociones Presentaciones a clientes. Difusión y *clipping* de prensa. Organización de eventos empresariales (lanzamientos de productos, acciones con públicos internos, jornadas empresariales, etc.). Negociación con proveedores.

EDUCACIÓN

Universidad de Ciencias Empresariales y Sociales
Licenciada, Publicidad, 2004 - 2007

ANEXO 3

Encuesta a Community Managers

Este cuestionario ha sido elaborado por Lorena Lesmes para la realización del Trabajo Final de la Especialización en Dirección de Marketing y Estrategia Competitiva de la Universidad de Buenos Aires. Los datos que se extraigan serán analizados para obtener conclusiones sobre los hábitos en materia de seguridad informática de los Community Managers.

Nombre:
Apellido:
País:
E-mail:

1. ¿Cuánto tiempo de experiencia tienes como Community Manager?

- o Menos de 6 meses
- o Entre 6 meses y 1 año
- o Entre 1 y 2 años
- o Entre 2 y 3 años
- o Más de 3 años

2. Empresa, medio u organismo para el cual trabajas:

_____

3. ¿Cuál es tu formación profesional?

- o Periodismo
- o Comunicación
- o Relaciones Públicas
- o Marketing
- o Publicidad
- o Sistemas
- o Ninguna
- o Otra, ¿Cuál?

4. Para desempeñarte como Community Manager, ¿Realizaste algún curso o programa específico?

- o Si
- o No

5. ¿En tu formación profesional, curso o programa recibiste contenidos sobre seguridad de la información?

- o Si
- o No

6. De la siguiente lista de riesgos en Internet, marca los que conoces:

- ☐ Malware (Virus, gusanos, troyanos, etc)
- ☐ Robo de información
- ☐ Robo de dinero
- ☐ Suplantación de identidad
- ☐ Phishing

7. En el dispositivo que usas para administrar las Redes Sociales, ¿Has sufrido alguna infección por malware (virus, gusanos, troyanos, etc.)?

- o Sí
- o No
- o No sé

8. En caso de haber sufrido la infección, ¿Esta fue propagada a través de las Redes Sociales?

- o Si
- o No

9. ¿Perdiste algo a partir de ese ataque informático?

- o SÍ, una o más cuentas de correo electrónico
- o Sí, una o más cuentas de Redes Sociales
- o Sí, perdí dinero
- o Si, perdí información como fotografías y documentos
- o No, no perdí nada
- o No lo sé
- o Otro:

10. ¿Has sufrido el robo o extravío del dispositivo (Notebook, Smartphone, Tablet) que utilizas para administrar los perfiles en Redes Sociales?

- o Si
- o No

11. ¿Cuentas con un Backup (copia de seguridad) de las publicaciones que has hecho en las Redes Sociales?

- o Si
- o No

12. ¿Qué cantidad de contraseñas posees en tus cuentas de Redes Sociales?

- o Una única contraseña para todos los perfiles en Redes Sociales.
- o Contraseñas distintas para cada perfil en Redes Sociales.

13. ¿Sueles cambiar periódicamente tus contraseñas?

- o Sí
- o No
- o Solo cuando ocurre un incidente o sospecho que fueron comprometidas.

14. ¿Cuál de los siguientes elementos verificas al ingresar a un sitio web de login?

- ☐ Dirección URL
- ☐ Protocolo HTTPS
- ☐ Diseño web
- ☐ Certificado digital

15. ¿Para realizar tus tareas de Community Management te conectas a redes Wifi públicas?

- o Si
- o No

16. ¿Crees que el conocimiento público de un ataque informático hacia una marca, puede afectar su reputación?

- o Sí
- o No

17. ¿Cuentas con algún documento o procedimiento definido en caso de encontrarte con un incidente de reputación de marca?

- o Si
- o No

¡Gracias por su colaboración!

ANEXO 4

Encuesta a seguidores y fans de marcas

Este cuestionario ha sido elaborado por Lorena Lesmes para la realización del Trabajo Final de la Especialización en Dirección de Marketing y Estrategia Competitiva de la Universidad de Buenos Aires. Los datos que se extraigan serán analizados para obtener conclusiones acerca de los usuarios de Redes Sociales y su interacción con las marcas que siguen.

Nombre:
Apellido:
País:
E-mail:

1. ¿Sigue marcas o empresas a través de Redes Sociales como Facebook o Twitter?

- o Sí
- o No

2. ¿Cuál fue la principal razón para seguir o hacerse fan de una marca en Redes Sociales?

- o Obtener descuentos y ofertas especiales.
- o Mostrar apoyo a la marca.
- o Ser el primero en disponer de novedades o actualizaciones de la marca.
- o Saciar la curiosidad suscitada por publicidad de la marca.
- o Seguir la recomendación de un miembro de su red social.
- o Imitar a un miembro de la red social que también sigue la marca.
- o Para reflejar estilo y personalidad
- o Otro

3. ¿Con qué frecuencia emite opiniones o recomendaciones acerca de una marca?

- o Siempre
- o A menudo
- o A veces
- o Rara vez
- o Nunca

5. Cuando ha estado insatisfecho con un producto o servicio, ¿Ha realizado comentarios negativos en alguno de los perfiles de Redes Sociales de la marca?

- o Sí
- o No

6. ¿Ha participado en concursos a través de las páginas de las marcas en Redes Sociales?

- o Sí
- o No

7. ¿Se le han solicitado datos personales como correo electrónico, edad, teléfono, etc.?

- o Sí
- o No

8. ¿Le preocuparía que esos datos le fueran robados a la marca o empresa que los solicitó?

- o Mucho
- o Bastante
- o Algo
- o Poco
- o Nada

9. ¿Conoce casos de marcas o empresas que han sido hackeadas?

- o Sí
- o No

10. Qué nivel de gravedad le asignaría a los siguientes riesgos para una empresa al ser hackeada: (Muy grave, Bastante grave, Algo grave, Poco grave, Nada grave)

Pérdida de información y bases de datos
Robo de credenciales bancarias
Pérdida de control de sus sitios web y perfiles en Redes Sociales
Pérdida de la buena reputación de la marca
Indisponibilidad del servicio por infecciones

11. Si una de las marcas que sigue fuera víctima de una ataque informático:

- ☐ Desconfiaría de su profesionalismo.
- ☐ Dejaría de seguirla.
- ☐ Le contaría a mis contactos el suceso.
- ☐ Lo pensaría dos veces antes de comprar sus productos.

- ☐ Pensaría que es culpa del encargado de administrar las Redes Sociales y no de la marca.
- ☐ No haría nada, es normal que ocurra esto.

¡Gracias por su colaboración!