

UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE HUMANIDADES
LICENCIATURA EN CIENCIAS DE LA COMUNICACIÓN

**"ANÁLISIS SOBRE EL USO DE PERFILES FALSOS DE FIGURAS POLÍTICAS EN GUATEMALA
A TRAVÉS DE LA RED SOCIAL TWITTER DURANTE LOS AÑOS 2015 - 2017."**

TESIS DE GRADO

MÓNICA DEL CARMEN RODAS SANDOVAL
CARNET 11470-13

GUATEMALA DE LA ASUNCIÓN, FEBRERO DE 2018
CAMPUS CENTRAL

UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE HUMANIDADES
LICENCIATURA EN CIENCIAS DE LA COMUNICACIÓN

**"ANÁLISIS SOBRE EL USO DE PERFILES FALSOS DE FIGURAS POLÍTICAS EN GUATEMALA
A TRAVÉS DE LA RED SOCIAL TWITTER DURANTE LOS AÑOS 2015 - 2017."**

TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE
HUMANIDADES

POR

MÓNICA DEL CARMEN RODAS SANDOVAL

PREVIO A CONFERÍRSELE

EL TÍTULO Y GRADO ACADÉMICO DE LICENCIADA EN CIENCIAS DE LA COMUNICACIÓN

GUATEMALA DE LA ASUNCIÓN, FEBRERO DE 2018
CAMPUS CENTRAL

AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR

RECTOR: P. MARCO TULIO MARTINEZ SALAZAR, S. J.
VICERRECTORA ACADÉMICA: DRA. MARTA LUCRECIA MÉNDEZ GONZÁLEZ DE PENEDO
VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN: ING. JOSÉ JUVENTINO GÁLVEZ RUANO
VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA: P. JULIO ENRIQUE MOREIRA CHAVARRÍA, S. J.
VICERRECTOR ADMINISTRATIVO: LIC. ARIEL RIVERA IRÍAS
SECRETARIA GENERAL: LIC. FABIOLA DE LA LUZ PADILLA BELTRANENA DE LORENZANA

AUTORIDADES DE LA FACULTAD DE HUMANIDADES

DECANO: MGTR. HÉCTOR ANTONIO ESTRELLA LÓPEZ, S. J.
VICEDECANO: DR. JUAN PABLO ESCOBAR GALO
SECRETARIA: MGTR. ROMELIA IRENE RUIZ GODOY
DIRECTORA DE CARRERA: LIC. MIRIAM AMARILIS MADRID ESTRADA DE VALDEZ

NOMBRE DEL ASESOR DE TRABAJO DE GRADUACIÓN

MGTR. MICHAEL ERIC FINKEL STERN

REVISOR QUE PRACTICÓ LA EVALUACIÓN

MGTR. IGNACIO LACLERIGA GIMENEZ

Guatemala, 20 de noviembre de 2017

Señores

Miembros del Consejo

Facultad de Humanidades

Universidad Rafael Landívar

Presente

Estimados Señores del Consejo

Atentamente me dirijo a ustedes, para someter a su consideración el trabajo de tesis de la estudiante MÓNICA DEL CARMEN RODAS SANDOVAL, Carné No. 11470-13 de la carrera de Licenciatura en Ciencias de la Comunicación, cuyo título es: **“Análisis sobre el uso de perfiles falsos de figuras políticas en Guatemala a través de la red social Twitter durante los años 2015-2017”**. He revisado el trabajo de investigación y considero que llena satisfactoriamente los requisitos necesarios de una investigación, por lo que solicito le nombren revisor final de tesis.

En espera de una resolución favorable, me es grato suscribirme con muestras de consideración y respeto.



Mgtr. Michael Eric Finkel Stern

Asesor



Universidad
Rafael Landívar

Tradición Jesuita en Guatemala

FACULTAD DE HUMANIDADES

No. 052499-2018

Orden de Impresión

De acuerdo a la aprobación de la Evaluación del Trabajo de Graduación en la variante Tesis de Grado de la estudiante: MÓNICA DEL CARMEN RODAS SANDOVAL, Carnet 11470-13 en la carrera LICENCIATURA EN CIENCIAS DE LA COMUNICACIÓN, del Campus Central, que consta en el Acta No. 051658-2018 de fecha 24 de enero de 2018, se autoriza la impresión digital del trabajo titulado:

"ANÁLISIS SOBRE EL USO DE PERFILES FALSOS DE FIGURAS POLÍTICAS EN GUATEMALA A TRAVÉS DE LA RED SOCIAL TWITTER DURANTE LOS AÑOS 2015 - 2017."

Previo a conferírsele el título y grado académico de LICENCIADA EN CIENCIAS DE LA COMUNICACIÓN.

Dado en la ciudad de Guatemala de la Asunción, a los 2 días del mes de febrero del año 2018.

Irene Ruiz Godoy

**MGTR. ROMELIA IRENE RUIZ GODOY, SECRETARIA
HUMANIDADES**

Universidad Rafael Landívar



AGRADECIMIENTOS

A Dios por darme la sabiduría necesaria para realizar esta investigación y por ser luz en mi vida y en toda mi carrera universitaria.

A mis padres por ser base fundamental en mis valores, principios y creencias, estar siempre al pendiente de mis logros y derrotas, así como ser mi sostén en cada paso que doy.

A mis hermanos Alejandra y Javier por darle alegría a mi vida. Sin ellos no podría desenvolverme en la vida, son mis principales audiencias.

Al resto de mi familia por ser y estar en mi vida.

A mi asesor Michael Finkel por ser la lupa a cualquier detalle de este estudio, a Luis Assardo por ser inspiración y gran aportador de información a este trabajo. Por último a Karina García por ser la primera en confiar en mí y en esta investigación.

A la Universidad Rafael Landívar por abrirme las puertas y permitir que explorara mi creatividad durante el tiempo de estudios. Así como darme la oportunidad de vivir la experiencia en la Universidad Iberoamericana, Ciudad de México en el año 2015, al participar como estudiante de intercambio por un semestre.

A mis amigos del “MC” por ser mi familia escogida con la que puedo escapar de la presión y tensión. A Karlamaría por convertirse en la cómplice, amiga, consejera y alegría de esta aventura universitaria, la que siempre estuvo y estará.

DEDICATORIA

A Guatemala, mi país y tierra que me vio nacer, en la que confío plenamente para poder desarrollarme como profesional y poder dejar huella en ella.

Índice

I. Introducción	3
1.2. Antecedentes	4
1.3. Marco Teórico	10
1.3.1. Network Society.....	10
1.3.2. Redes Sociales como espacio de comunicación, información y opinión.....	15
1.3.2.1. Redes Sociales y medios de comunicación.....	17
1.3.2.2. Redes Sociales y cultura.....	20
1.3.2.3. Redes Sociales y política.....	21
1.3.2.4. Redes Sociales y movimientos sociales/políticos.....	22
1.3.2.5. Redes Sociales y políticas públicas de Estados.....	24
1.3.3. El lado oculto del ciberespacio.....	26
1.3.3.1. Identidad digital.....	30
1.3.3.2. Privacidad.....	31
1.3.3.3. Cibercrimen.....	35
a) El cibercrimen en medios de comunicación.....	40
b) El cibercrimen en la ciberpolítica.....	41
c) Delitos en el ciberespacio.....	45
1.3.3.4. Anonimato en el ciberespacio.....	49
1.3.3.5. Censura en Internet.....	51
1.3.3.6. Contenidos virales.....	52
1.3.4. Plataformas de Redes Sociales amenazadas por el cibercrimen.....	53
a) Facebook.....	58
b) Twitter.....	61
II. Planteamiento	65
2.1. Objetivo	66
Objetivo General.....	66
Objetivos Específicos.....	66
2.2. Variables o Unidades de análisis	67
a) Perfiles Falsos.....	67
Definición Conceptual.....	67
Definición Operacional.....	67
b) Figuras Políticas.....	67
Definición Conceptual.....	67
Definición Operacional.....	68
2.3. Alcances y Límites	68
2.4. Aporte	69
III. Método	70
3.1. Sujetos de estudio	70
3.2. Técnicas e instrumentos	72
3.3. Procedimiento	74
3.4. Tipo de Investigación	75
IV. Presentación y análisis de resultados	76
V. Discusión de resultados	121
VI. Conclusiones	127
VII. Recomendaciones	129

Bibliografía.....	130
Anexos	139
Anexo I	139
Anexo II	140
Anexo III.....	143

Resumen

La reputación o imagen de una figura política puede ser afectada o alterada por medio de diferentes métodos. Sin embargo, en la actualidad esta puede llegar a ser vulnerada dentro de la red digital a través del uso de distintas plataformas o sitios web. Castells (2014) describe al mundo digital como un espacio abierto, variado y flexible, donde la jerarquía de poder se ausenta y se tiene la posibilidad de establecer mensajes de contenido libre y diverso. La presente investigación tiene como objetivo analizar el uso de perfiles falsos de figuras políticas en Guatemala a través de la red social Twitter durante los años 2015 - 2017.

Para poder identificar cada perfil falso se realizó un análisis de contenido sobre las características de estos (comportamiento, interacción, fin y dinámicas de comunicación) referentes a las figuras más relevantes de los años 2015 - 2017. Asimismo la verificación de veracidad y efectividad del perfil analizado por medio de la aplicación TwitterAudit. A través de las tablas de cotejo se categorizaron los mensajes, métodos de comunicación y observaciones específicas de cada perfil según la información recopilada durante el monitoreo.

Posteriormente se realizaron entrevistas semiestructuradas a cuatro expertos representando cada área que abarca el estudio (seguridad web, cibercrimen, *netcenters*, campaña política en redes sociales). Por medio del análisis de los perfiles falsos identificados y la elaboración de las entrevistas, se logró determinar que estas cuentas con estos fines logran crear percepciones falsas acerca de la imagen de una figura política. Introducen la duda hacia las acciones realizadas por los cargos de gobierno u otros referentes a la política en Guatemala. También se detectaron los tipos de mensajes que manejan en su mayoría y el efecto de esta tarea.

El presente estudio muestra cómo en la actualidad se lucha por intentar obtener poder por medio del dominio de las plataformas de redes sociales. Sin embargo, muchas veces utilizan mecánicas convencionales de manipulación, persuasión, duda, censura y suplantación de identidad pero estructuradas en el ciberespacio codificándolo a actos definidos como criminales y delincuenciales.

I. Introducción

En la actualidad el mundo se mueve a través de la tecnología, movimientos interconectados que son capaces de impactar en la sociedad grandemente. Gracias al uso de aparatos electrónicos la interacción de un punto a otro es interminable, sin embargo, la era digital conlleva a que la sociedad se convierta en una sociedad red. Pequeños nodos conectados que pueden lograr transformaciones y generaciones de nuevas dinámicas económicas, políticas, sociales y sobre todo comunicacionales.

En cuanto la transformación de la comunicación en la era digital, se dice actualmente que la persona que no está "en línea" dentro de la red o la web, no existe en realidad. Ciertamente es posible, pues su identidad digital no está a la vista del mundo. La comunicación pues, se trata de estar conectado con el mundo e interactuar en tiempo real en distintos puntos. La inmediatez, es característica principal en estos tiempos.

Las redes sociales forman parte de esa inmediatez, la información o contenidos que se difunden a través de estas garantiza un alcance global en cuestión de segundos. Dichas características las han aprovechado sectores tanto de poder como activistas sociales, pues se han dado la tarea de trasladar los discursos de presión o movimientos sociales a las redes sociales para obtener mayores resultados y un alto número de simpatizantes.

Así también, el mundo del ciberespacio puede ser positivo en cierta forma, sin embargo, para este estudio se presentará al ciberespacio y redes sociales como un reto que afronta la sociedad hoy en día. El crimen ha llegado a las redes sociales y este ha sido poco estudiado y nada controlado. En Guatemala no existe mayor regulación sobre el contenido que se almacena en la web y mucho menos en las redes sociales.

El fin de este estudio es analizar la creación y uso de perfiles falsos en las redes sociales como Twitter que han logrado la desviación, presión y manipulación de contenido sobre un personaje. En este caso el uso de perfiles falsos que utilizan la imagen o identidad de entes políticos, vigentes o no vigentes en la actualidad guatemalteca y que han sido relevantes en los años 2015 al 2017.

1.2. Antecedentes

El uso de redes sociales para asuntos políticos ha ido aumentando, siendo un factor importante para generar grandes efectos en la comunicación política. En cuanto a la elaboración de una campaña política por medio de las redes sociales, Carías (2015) investigó sobre el uso de Facebook como red social de los partidos políticos en la campaña electoral 2015, enfocándose en las páginas oficiales de Facebook de los partidos políticos Partido Patriota (PP), Libertad Democrática Renovada (LIDER), y Unidad Nacional de la Esperanza (UNE). Por medio de una tabla de recolección de datos de cada partido y con una muestra basada en las páginas oficiales de los partidos ya mencionados, durante el período de elecciones 2015, obtuvo como resultado que UNE tenía mayor orden y fortaleza con sus publicaciones, mientras que LIDER saturaba la página de publicaciones y PP casi no divulgaba información de su campaña. Así también, concluye que los partidos políticos monitoreados, utilizaron Facebook durante su campaña para informar sobre sus visitas al interior del país a través de fotografías y vídeos. El tema de campaña negra también fue uno de los más mencionados, utilizado para lanzar comentarios que aludían a otros partidos pero no de forma directa.

En relación a esto, Montoya (2013) de la Pontificia Universidad Javeriana en Bogotá, Colombia, analizó y respondió a la pregunta: ¿cómo la incorporación de redes sociales generó determinados efectos en la campaña política presidencial para el período 2012?, en este caso planteó una hipótesis en la cual dicta que las redes sociales virtuales demuestran una expansión y una incidencia progresivamente mayor en la participación ciudadana respecto de las nuevas estrategias de marketing político y de campañas electorales, pero aún no son definitivas en transformar esa virtualidad en comportamientos políticos reales, así como en actitudes electorales que decidan comicios. Al identificar los efectos y el impacto de las redes sociales en la campaña política antes mencionada resalta que en los diferentes grupos demográficos mencionados existe una alta utilidad al internet, por encima del 90%. Expresa también que en Colombia existe una alta conectividad y por esta razón la incidencia que se manifiesta con el uso de las nuevas tecnologías es relativamente alta y por lógica generó un impacto importante, al menos en la campaña del Partido Verde.

Sin embargo, según los encuestados su voto no se vio afectado por la información proporcionada en las redes sociales.

Ahí mismo en Colombia, respecto al uso de las Nuevas Tecnologías de la Información y Comunicación (TIC's), Vega (2010) investigó el uso y el impacto de las TIC's en la campaña presidencial de 2010 en Colombia. Con esto expresa que una de las ventajas que percibe con el uso de Internet en las campañas políticas es el posicionamiento en el mundo como una herramienta de acceso a información ilimitada, acercando mucho más al electorado. Al igual que en el estudio de Montoya, el Partido Verde aprovechó los beneficios de las TIC's para que le permitiera identificar audiencias, integrar y organizar a los fans en objetos propuestos por la campaña. Concluye que motivar el voto es un aspecto clave para que exista conexión entre el candidato y el elector.

Mientras que en Ecuador, Toral (2013) investigó las Redes Sociales como un complemento en campañas electorales, como objetivo de estudio presenta el análisis del posible reemplazo de la política tradicional por la política 2.0 o bien es una estrategia complementaria. Para esto se enfocó en los perfiles de los políticos actuales de Ecuador y entrevistas de profundidad a aquellos actores políticos nacionales e internacionales, activos e inactivos, así como a dos comunicadores políticos. Gracias a estas entrevistas y el análisis de contenido por medio de la tabla de cotejo, obtuvo como resultado que la política 2.0 es el manejo de las nuevas tecnologías en campañas electorales, esto da pauta a afirmar que el uso de redes sociales es una herramienta extra dentro de la estrategia de campaña, las cuales permiten un acercamiento a la ciudadanía. Observó que las redes sociales más utilizadas para campañas electorales en ese país son Facebook y Twitter, mientras que Instagram no ha tenido mayor relevancia, ya que solo uno de los entrevistados ha utilizado dicha plataforma. Así también, la mayoría de los actores políticos manejan cuentas personales en Twitter: Rafael Correa (@MashiRafael), Cristina Fernández de Kirchner (@CFKArgentina). Pudo constatar que la Administración Presidencial de Venezuela es la que más tuits publica (41 tuits por día). Por esta razón, la autora concluye que una campaña política exitosa es aquella que concibe una estrategia muy bien dirigida y tiene las

herramientas precisas para difundirla, teniendo en cuenta que las redes sociales son una herramienta más del gran abanico de medios de difusión disponibles, las cuales se puede intermediario en las cuales los medios se puede dar a conocer hacia una gran cantidad de personas por medio de un plan publicitario. Concluye que las redes sociales sí influyen en la agenda mediática, a pesar que los medios no las utilicen de buena manera y con esto obtienen un impacto dentro de la sociedad por medio de la saturación de publicaciones.

En cuanto el impacto o uso de redes sociales para generar participación política o en movimientos sociales, Reyes (2017) investigó sobre movilización ciudadana y redes sociales: descripción de la emergencia de nuevos líderes de opinión en 2015. Esta investigación tuvo como propósito analizar el proceso de emergencia de nuevos líderes de opinión a partir de la percepción que columnistas, medios de comunicación digital, expertos en redes sociales y nuevos liderazgos de opinión pública tienen en torno al proceso de comunicación digital en las movilizaciones ciudadanas suscitadas en la crisis política de abril a agosto de 2015 en Guatemala. En la cual concluye que el Internet, como medio, realizó la labor de permear a la ciudadanía con información preferentemente a través de Facebook, Twitter y WhatsApp y así generar un movimiento ciudadano para reclamar un cambio en el sistema político actual, así como la construcción de la opinión pública digital no se hubiese concretado de no ser por la aplicación adecuada de herramientas comunicacionales durante los mensajes emitidos por liderazgos de opinión en sus plataformas digitales.

Respecto a la utilización de hashtags (#) para expresar las consignas de los movimientos ciudadanos y políticos, Magariño (2015) analizó la opinión política de los jóvenes en Facebook en la Ciudad de Guatemala en el movimiento #RenunciaYa. Esta investigación tuvo como sujetos de estudio a los jóvenes de 18 a 24 años, usuarios de Facebook y seguidores de las páginas Cartelera Política, Soy 502 y Líderes Políticos GT, que comentaban y opinaban sobre el acontecer político en ese período. Como instrumento utilizó la guía de análisis en base al esquema de Van Dijk y un cuaderno de notas. Como conclusión emite que Facebook funge como instrumento de participación y movilización política, ya que por su espacio virtual posibilita el debate e interacción sobre los acontecimientos y figuras políticas de Guatemala. Este movimiento virtual fue causado por

la falta de credibilidad de la juventud hacia el sistema político de Guatemala, siendo ellos mismos los promotores de dicho acontecer.

En el entorno internacional, siempre en el ámbito de la participación política y ciudadana, Ayala (2013) realizó un análisis comparativo sobre el caso del partido pirata alemán y la política mexicana (Internet y participación), como resultado plantea que la aportación del Partido Alemán va hacia el sentido de establecer herramientas que acercan a la gente con el quehacer político. Por el uso del Internet el ciudadano no tiene que decidirse por un programa o agenda establecido por un partido político, sino que tiene la posibilidad de intervenir en cada una de las iniciativas si así lo desea. En dicho escenario, los ciudadanos podrán intervenir el programa de su gobierno directamente a través de una plataforma electrónica, sin necesidad de pertenecer a ningún partido político.

En cuanto a la seguridad en redes sociales, los autores González - Manzano, González - Tablas, Fuentes y Ribagorda (2013) pertenecientes a las Universidad Carlos III de Madrid participaron en el VII Congreso Iberoamericano en Seguridad Informática (CIBSI) en Panamá. En su artículo de Seguridad en Redes Sociales: problemas, tendencias y retos futuros enuncian diez problemas asociados con la privacidad en las redes sociales y cada problema es acompañado de directrices que pretenden ser la base de futuras investigaciones y desarrollos. En este sentido, analizan de forma global la dificultad técnica de abordar estos problemas, así como el alcance que tienen en las redes sociales. En cuanto a los problemas encontrados se pueden mencionar la creación de nodos falsos (Sybil nodes), Copropiedad (usos de multitud de datos), transacción de datos, privacidad en la localización, control de los datos almacenados, control de accesos, anonimato de usuarios, manipulación tras el acceso, entre otros. Bajo esta idea, los autores discuten que a pesar de que ya se sabe de los problemas no se ha investigado a profundidad, peor aún, no se ha movilizad para mejorar la seguridad e integridad de la identidad virtual de los usuarios. Concluyen que es necesario realizar más estudios y sobre todo tratar de abordar los temas de Derecho al olvido, Manipulación tras el acceso, así como la regulación del cumplimiento al Derecho de privacidad.

En cuanto a la regulación de los delitos informáticos presentes en las redes sociales, Rodríguez (2011) plantea en su análisis descriptivo sobre las leyes existentes en Colombia y su regulación de los actos ilícitos reflejados en las redes sociales en el año 2011. Teniendo como sujetos de estudio las leyes informáticas y redes sociales utilizadas en ese país. Obteniendo como resultado que el uso de internet se ha extendido, ha aumentado el riesgo de su uso inadecuado. Los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático, pornografía infantil, entre otros. Está claro que la constitución política de Colombia sí otorga a través de su principalística y de normas que consagran derechos fundamentales, un respaldo suficiente como para que el legislador consagre normas tendientes a desarrollar lo que se conoce mundialmente como delitos informáticos. Esta ley y marco jurídico se ha convertido en una importante contribución y en un instrumento muy efectivo para que las entidades públicas y privadas puedan enfrentar los delitos informáticos, por lo tanto la ley colombiana no define el delito informático como tal, y menos, define las conductas delictivas presentes en las redes sociales, pues lo que se ha hecho es regular ciertos casos relativos a fraudes y accesos no permitidos a sistemas de información. Es importante tener en cuenta que a pesar de que no exista una clara definición de qué es o no es un delito informático, se puede tomar del código penal y el código de procedimiento penal para el manejo de dichos delitos. Como conclusión Rodríguez expresa que en Colombia no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa.

Por último, otro problema que se refleja en las redes sociales es la creación de perfiles falsos, para esto Temperini y Macedo (2015) investigaron sobre la problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen en Argentina. Teniendo como objetivo la determinación, categorización y análisis de distintas clases de perfiles falsos existentes en la red social Facebook. Entre los resultados encontrados se pueden mencionar la creación y utilización de un perfil falso no contradice ninguna normativa vigente, sino

que podría ser considerado como una manifestación de la libertad de expresión y a modo general, representando una de las libertades más importantes que se pueden encontrar en Internet. Se considera delito a la creación del perfil falso, si es con fines de usurpación de la identidad de una persona real, configurándose así un caso de usurpación o suplantación de identidad. Algunos países, como EE.UU y Canadá, poseen regulaciones generales para la suplantación de identidad, adaptadas de tal manera que el mismo tipo penal es aplicable tanto para el robo de identidad clásico, así como para el robo de identidad digital. Por ende, los autores concluyen que es necesario considerar el desarrollo de herramientas que permitan la detección y eliminación de los perfiles falsos, así como la adaptación o mejoramiento de políticas de acreditación de identidad ante Facebook a fin de evitar la proliferación de esta problemática.

En este sentido, se refleja que las redes sociales sí tienen impacto en la mayoría de estudios en cuanto a la política y cómo son utilizadas como herramienta para la comunicación política. Sin embargo, en la recolección de estudios se determina que no existe una regulación y control sobre la utilidad con malas intenciones así como la manipulación de datos, la creación de perfiles falsos para usurpar identidades reales. Por otro lado, se determina que este tipo de estudios no han tenido mayor movimiento en Guatemala, pues la recolección obtenida se destaca en investigaciones internacionales, ya que son estos los que se han interesado en abordar el tema de seguridad de la web 2.0 y los abusos que no se han regulado a nivel mundial. Estos últimos problemas mencionados pueden causar desviaciones en cuanto a la opinión pública de algún personaje político así como el sabotaje de estrategias electorales manejadas dentro de las redes sociales.

1.3. Marco Teórico

En base a esta investigación es necesario tener fundamentos teóricos que puedan respaldar y explicar a profundidad el fenómeno que se está dando a conocer. Como primer capítulo se expone cómo la teoría de la Network Society (Sociedad Red) se manifiesta en el tema principal de este estudio, así como los procesos de construcción de red, las dinámicas de comunicación que se efectúan dentro de la red y cómo se empodera la red a través de la comunicación. En el segundo capítulo se traspasa el ciberespacio, características y elementos estructurales que hacen de la actualidad una sociedad interconectada.

Asimismo, cómo el ciberespacio funciona para diferentes ámbitos, en este caso se enfoca en la ciberpolítica y cómo puede llegar a existir el cibercrimen, y este, afectar el contenido político virtual. Por último, aborda en dos capítulos las redes sociales más utilizadas a nivel mundial y la funcionalidad de cada una, así como las herramientas de reacción que contienen para la construcción de espacios de interacción o socialización dentro de la red.

1.3.1. Network Society

Para obtener una idea clara sobre este concepto es necesario explicar que las redes sociales o sociedad red se refiere a la interacción de individuos que tienen entre sí y a través de esa interacción logran la construcción o formación de grupos sociales por afinidad o intereses en común. "Las redes sociales son parte de nuestra vida, son la forma en la que se estructuran las relaciones personales, estamos conectados mucho antes de tener conexión a Internet", explica Ponce (2012, p. 2).

Una red se interconecta por medio de nodos y la función o significado depende de la interacción o codificación entre otros nodos. Algunos nodos desaparecen o son reconfigurados según las modificaciones que se manifiesten en las redes provocados por los cambios de códigos o programas (Castells, 2014, p.45).

Mientras Lozares (1996) define: "Por forma de la red se entiende la expresión abstracta de la relación y las propiedades de la configuración global o de algunas de las partes, es decir, lo que se suele describir como pautas, modelo o estructura de la red" (P. 110). En cuanto a

las redes dentro de la sociedad se refiere sobre las relaciones que vinculan a los individuos entre grupos sociales estructurados por su manera de comunicarse e interactuar. Siendo contruidos por actores sociales que se originan en la red.

Esta cierta vinculación con los actores sociales pueden ser manifestados como: empresas, personas individuales, agencias de servicio, estados, entre otros. En sí, la sociedad está formada por grupos sociales vinculados entre sí por medio de lazos relacionales: amistades, familiares, laborales, cívicos, religiosos (Wasserman y Faust, 1994, p. 17-20), (Lozares, 1996).

Esto indica que el comportamiento humano se ve desarrollado por los vínculos que se lleguen a formar dentro del entorno personal, sin embargo siempre es visto de manera grupal pues de esto se estructuran la relaciones interpersonales y culturas. Respecto a esto Lozares (1996) cita al teórico Kurt Lewin donde explica que tanto el comportamiento humano dentro de una red como la estructura de la misma se concentran en un espacio social siendo contruido por varias redes más. En base a esto se entablan las relaciones sociales.

El Análisis de las Redes Sociales <<ARS>> refleja que no solo existe una interacción entre individuos o grupos en la red social que expone conocimientos en base a la comunicación, sino que puede llegar a causar un gran impacto en el comportamiento de los actores, llegando a las estructuras de poder y en los procesos de aprendizaje (Sanz, 2003, p. 22).

En actualidad no se habla solamente de una red social y su comportamiento, sino de la interconectividad a la que se ve expuesta por medio de la tecnología. Ante esto se dice que una red social está vinculada por medio de actividades tecnológicas digitales de la comunicación y la información por medio de la microelectrónica. Esta estructura social es aquella que está organizada por un grupo de humanos mediante una comunicación codificada por la cultura (Castells, 2014, p. 51).

Siendo redes globales tienen la capacidad de trascender límites territoriales, ya que llegan a tener actividades virtuales en distintos puntos del mundo. Es decir, todo grupo social que interactúe dentro de la red digital pase a ser de una sociedad red a una sociedad global. Esto provoca que las actividades humanas, en la actualidad, se enfoquen en el mundo digital.

Para Igor Sádaba y Ángel Gordo (2008), el discurso que se ha manejado en las últimas tres décadas es sobre cómo la tecnología reivindica en la política y en la organización de las redes sociales. Así como en el marco empresarial la tecnología ha sido parte de los movimientos políticos y ciudadanos, pues estos han utilizado elementos técnicos como herramientas de poder. Poder luchar para posicionarse.

Castells (2014), determina que el control y actividades humanas se han transportado al ciberespacio pues cualquier movimiento social para valer los derechos, grupos financieros, educaciones universitarias, el arte, el cine, los medios de comunicación se han enfocado en crear contenido de interactividad para que la misma sociedad esté expuesta a las tecnologías de comunicación e información.

Por otro lado la sociedad red se ve expuesta en diferentes ámbitos. Al enfocarse en las grandes masas se refiere cómo la sociedad está vinculada con la información y comunicación de los medios masivos. Se sabe que las corporaciones de medios primero son empresas y toda empresa necesita ingresos, esta idea hace que los medios sean definidos como: "captadores de audiencia". En este sentido, las capacidades de un medio de comunicación para influenciar en la sociedad son altas, sin embargo mientras exista contacto con el Internet esto se vuelve limitante para estos grupos mediáticos.

En el artículo publicado en la Revista Telos (2008), Castells comparte que la comunicación en la red es la web global, "redes de comunicación horizontal que incluyen el intercambio multimodal de mensajes interactivos de muchos a muchos, tanto sincrónicos como asincrónicos" (p. 45).

La sociedad red en las grandes masas no se limita a lo que dicen los medios de comunicación, sino que buscan por otras vías la información. Los avances tecnológicos de la información y comunicación provocan una reconfiguración en el espacio mediático, pues se tiene mayor facilidad de acceso a herramientas virtuales para que la fluidez comunicacional e interactiva sea cada vez más inmediata (Campos, 2008).

En cuanto a la política y los medios de comunicación existe una íntima relación, siendo capaces de crear corporaciones de medios de comunicación por medio de una figura política.

Esto provoca que la política tenga cierta dependencia de los medios masivos pues necesita ser escuchada, estructurada y conocida por la sociedad, por lo que Castells añade:

La política se basa en la comunicación socializada, en la capacidad para influir en la opinión de las personas. El canal de comunicación más importante entre el sistema político y los ciudadanos es el sistema de los medios de comunicación de masas, siendo el primero de ellos la televisión. Publicación en la Revista Telos (2008, p.3).

Sin embargo, esta relación mediática y política puede llegar a modificarse pues la introducción de las tecnologías globales provoca que la comunicación esté al alcance de muchos y el poder pase a ser parte del espacio digital. Por lo que Castells (2014) expresa:

El sistema de comunicación digital global, si bien refleja las relaciones de poder, no se basa en la difusión jerarquizada de una cultura dominante. Es un sistema variado y flexible, abierto en el contenido de sus mensajes dependiendo de las configuraciones concretas de empresas, poder y cultura (p. 189).

En la actualidad el desarrollo de un territorio se basa en la cantidad de la conectividad de computadores al Internet y el grado de inteligencia de estos aparatos. Siendo parte del discurso de muchos políticos como parte de sus propuestas de políticas públicas a realizar durante su mandato. También es lo que proyectan los grupos mediáticos y las grandes élites, la comunicación e información difundida a través de las nuevas tecnologías (Burch, León, Tamayo, 2001).

Gracias al Internet la difusión de la comunicación puede llegar a viralizarse a gran escala en distintos "nodos" sociales que están contruidos en la red. La socialización en la red es un fenómeno netamente de interactividad dentro de la Web 2.0 y hace que la comunicación sea amplia y enriquecedora en algunos casos (Castells, 2008).

Por otro lado gracias a la construcción de redes virtuales, la sociedad está sumergida en información. El establecimiento de la era digital en el manejo de la información las dinámicas del poder se centran en controlar contenidos y mensajes.

Según Ramonet (1998), la clasificación del poder se constituye en el económico, mediático y político. Sin embargo, con el avance tecnológico y las nuevas propuestas de comunicación digital se dice que los new media han ido posicionándose como grandes influenciadores dentro de los poderes formales que pueden llegar a existir en una determinada sociedad.

Para Castells la comunicación es poder. Se sabe que el Estado se centraliza en el poder, sin embargo este ha sido desafiado por la utilidad de herramientas digitales bajo una globalización sin límites, las presiones del mercado hacia la desregulación que disminuye su capacidad de intervención y la crisis de legitimidad política que debilita su influencia sobre los ciudadanos (Castells, 2008).

La emergencia de la autocomunicación de masa desintermedia a los medios y abre el abanico de influencias en el campo de la comunicación, permitiendo una mayor intervención de los ciudadanos, lo cual ayuda a los movimientos sociales y a las políticas alternativas. Pero al mismo tiempo también las empresas, los gobiernos, los políticos intervienen en el espacio de internet (p. 1).

Ramonet (1998), indica que se está originando la era de la sospecha, pues así como pasó en la televisión está sucediendo con los nuevos media. Han dado pauta a ejercer poder sobre los ciudadanos para manipularlos con el contenido difundido y así beneficiar al partido dominante en las épocas electorales. Esta exposición de contenido llega a mayor escala a las personas por las características que ya se conocen del Internet. Además el autor explica:

Nadie niega la indispensable función de las comunicaciones de masas en una democracia. La información es esencial para la buena marcha de la sociedad. No hay democracia posible sin una buena red de comunicaciones y sin el máximo de informaciones. Gracias a la información el hombre vive como un hombre libre. Todo el mundo está convencido de esto. Y, sin embargo, los media han entrado en una era sospechosa (p. 191).

Entonces, las dinámicas del poder no han cambiado, siguen siendo las misma solo que se han formado en base a una articulación entre lo global y lo local, estableciendo su debida organización en redes. Sin embargo, todo movimiento o idea se forma desde la base individual, se buscan redes afines a los valores e intenciones que se tengan para obtener el poder en conjunto dentro de la sociedad red. Como anteriormente se menciona, esto se logra a través del contacto y accesibilidad de la comunicación e información por medio del Internet.

1.3.2. Redes Sociales como espacio de comunicación, información y opinión

En el siglo XXI las redes sociales no solo son sociales sino que son virtuales, en donde generan comunidades ya no territoriales sino que digitales. En este apartado se plantea las teorías de sociedad red en el mundo digital y cómo esta se desarrolla en distintos puntos a través de plataformas tecnológicas que facilitan y transforman la comunicación vertical a una comunicación global, a una comunicación de todos a todos.

Entre los cambios que se pueden mencionar están los medios tradicionales "transformados" al mundo digital, estos siguen siendo utilizados por la mayoría de personas a pesar de que algunos han sido desplazados. Aun así, no se puede afirmar la erradicación de su uso. Sin embargo, ya existen nuevas modalidades que han sido poco estudiadas pero se han ido detectando poco a poco, como nuevas expresiones comunicativas que no solo informan sino que también entretienen, accionan e interactúan en base a múltiples finalidades (Zallo, 2011, p. 59).

Para Nicolás y Grandío (2012) la aparición de estas nuevas modalidades comunicativas establecidas dentro de la era del Internet, hace que la sociedad esté expuesta a cambios de

comportamientos, pues ahora deja de ser un individuo como tal y pasa a ser un "usuario" dentro del mundo digital, así también aparecen gestiones y relaciones más sociales, más colaborativas, más comunitarias y más comprometidas.

En cuanto a la postura de Zallo (2011; 59) el acceso al Internet hace que sea un campo de comunicación y cultura, por medio de las telecomunicaciones los usuarios pueden obtener infinidad de base de datos, los automatismos, el comercio electrónico, el pago, la publicidad o las relaciones sociales.

Luego de esta breve introducción al mundo digital y cómo se ha transformado la comunicación, para fines de este estudio el enfoque sobre las plataformas de Internet como las redes sociales, será desarrollado a profundidad para poder entender y comprender teóricamente las dinámicas a estudiar.

En cuanto a las relaciones sociales se han generado plataformas dentro del Internet para establecer nuevas culturas, nuevas formas de comunicación y nuevas políticas sociales, y económicas. En este caso se refiere al mundo de las redes sociales virtuales.

"Las social media son antes que nada sociales" (Nicolás y Grandío, 2012, p. 23). Las redes sociales principalmente son un espacio de entretenimiento y donde se puede entablar una relación con otros usuarios de manera virtual y tiempo real. Consideran las redes sociales como un medio de comunicación y expresión capaces de crear comunidades virtuales a fines de un interés en común. Así mismo como la generación y creación de una difusión multidireccional de contenido digital ya sea de propia autoría o que pertenece a otros usuarios.

Así también el juego de las redes sociales en la actualidad ha sido modificado partiendo desde su principal objetivo de entretenimiento, pues ahora abarca distintas dinámicas de comunicación, educación y política.

Para el aspecto comercial, empresarial e institucional, las redes sociales han sido de gran importancia en cuanto a su implementación para manejos comunicacionales como una campaña publicitaria, política o social. Las funciones que cumplen con las características

descritas en este texto son las plataformas de Twitter y Facebook (Nicolás y Grandío, 2012, p. 23).

En este sentido las redes sociales culturalmente hablando se tornan como la infraestructura para las nuevas políticas culturales, pues según Zallo (2011): "La aparición de... nuevos servicios, actores y prácticas sociales en un marco relacional global, obliga a repensar las políticas nacionales o regionales de comunicación" (p. 386).

1.3.2.1. Redes Sociales y medios de comunicación

Las redes sociales han hecho que la sociedad esté sumergida en información creando una cultura global y esto hace que grandes corporaciones de comunicación, información o telefonía establezcan servicios en los cuales puedan enganchar a la sociedad que de forma especial estimulan la imbricación de los tres sectores de la tecnología (informática, telefonía y televisión) que se convergen por medio del Internet y plataformas multimedia. (Ramonet, 2003; 209).

En cuanto a la postura de Jarvis (2015) por medio de computadores y teléfonos móviles las personas tiene acceso instantáneo a plataformas digitales que permiten el flujo de comunicación e información masivo, capacidad de relacionarse con todo el mundo sin necesidad de guardianes o mediadores como lo son los medios de comunicación.

Para Ramonet (2003) esta convergencia de tecnologías y servicios informáticos y comunicacionales es el simple hecho de negociaciones codiciosas a través de la era digital. Suministrar entretenimiento, información, cultura, noticias por medio de interconexiones con todos los medios de comunicación disponibles hoy en día.

Es tanta la capacidad de la información global, aún más con las conexiones a las redes sociales. En cuanto a esto Jarvis (2015) expresa:

No olvidemos a los miles y miles de ciudadanos... que intercambian información en Twitter, Facebook, Pinterest, Tumblr, foros en NI.com y otras redes sociales y a

través de sus propios blogs. Cuando utilizo las palabras (medio informativo) puedo hacer referencia a cualquiera de ellos, no solo al periódico tradicional (p. 40).

En referencia a la difusión de información por medio de redes sociales ya sea por parte de los medios de comunicación o la misma sociedad, provoca que existan espacios interrelacionados a través de la conexión a distintos entornos, espacios de expresión, y más que entretenimiento se convierten en espacios de construcción de opiniones, juicios o críticas.

Las personas en las redes sociales no solo se limitan a relacionarse con otras personas o sociedades sino que se tiene la oportunidad de crear valores, análisis, críticas que vayan construyendo su propio mundo virtual. Así es como se deja la idea que las redes sociales principalmente son con un enfoque de entretenimiento, pues ahora tiene varios enfoques como el empresarial y comercial (Nicolás, Grandío, 2012).

En lo que respecta a Caldevilla (2010) las redes sociales virtuales y las páginas web 2.0 se alimentan del contenido que se almacena en ellas, partiendo de una idea, concepto o planteamiento y esto se refuerza por la interacción entre grandes cantidades de usuarios formando una opinión, un debate, una referencia. Todas estas dinámicas hacen que el flujo de la comunicación se fusione y se vaya expandiendo de manera global.

La relevancia de las redes sociales en la actualidad no es por cómo surgen sino que de su origen nace un impacto que dará de qué hablar por mucho tiempo. La magnitud de las redes sociales es impresionante e infinita de entenderla. Hoy en día no se ha estudiado lo suficiente para entender el impacto de las redes sociales que han generado en el mundo. Así como también, es imposible imaginar el futuro de esto, pero se puede mantener la sospecha que se lograrán diversos cambios mundiales como los pequeños cambios que se han visto en estos últimos años.

Ahora los medios de comunicación tuvieron que adaptarse a las dinámicas del mundo digital. El surgimiento de los new media se dio de la necesidad de seguir siendo generadores de información hacia la sociedad, sin embargo es un acto desafiante pues están

en constantes cambios porque dependen del gusto y la elección del usuario hacia el contenido.

La postura de Jarvis (2015) dice que la hegemonía de las televisiones y los monopolios de medios de comunicación fue herida por la introducción del Internet a partir de 1990. No se destruyeron los medios, sino que erradicó el concepto de masas. El trabajo de plataformas como Google, Facebook o Amazon plantea una línea de conectividad con el usuario o comunidad en la red. En la actualidad tanto el medio como el periodista no solo deben generar el contenido, sino que se deben acercar mucho más al usuario, conocer sus intereses, gustos y desafíos. En esa línea se generan modelos de negocios para la supervivencia y éxito del medio.

En el estudio realizado por Elogia Ipsofacto en el 2009 en España, citado por los autores Nicolás y Grandío (2012; 69) presenta resultados significantes que dan una pequeña explicación de las acciones de los usuarios en las redes sociales. Entre los más relevantes están:

- Los servicios de internet más utilizados por los usuarios de redes sociales son los buscadores, los periódicos digitales y los foros.
- El usuario de redes sociales dedican más tiempo en este servicio que a otros servicios de internet o incluso que a los medios convencionales, ya que es el medio que más les gusta, principalmente por considerarlo el más divertido y uno de los más actuales y dinámicos.
- Las actividades que realizan los usuarios pueden segmentarse en dos grupos diferenciados, el segmento relacionado con el intercambio de información y experiencias y el relacionado con las aplicaciones disponibles en la red social.
- Facebook es la red más conocida de forma espontánea y sugerida, y es la preferida por la mitad de la muestra analizada.

Por lo tanto la interactividad en las redes sociales no solo se trata de intercambiar información o entablar una conversación con una persona de otro país, sino que va más allá

de eso. La dinámica de la interactividad en las redes sociales parte de la publicación de un artículo en un blog, este se viraliza por razones afines con otros usuarios y estos la comparten en su red o en otros sitios en internet.

Así como la interactividad del medio tiene la ventaja o desventaja de poder cambiar conductas, generar movimientos de opinión como se mencionó anteriormente. Establecimiento de una comunicación horizontal, ya que con estas acciones tanto el medio como el usuario son constructores de información (Caldevilla, 2010).

1.3.2.2. Redes Sociales y cultura

Respecto a la cultura hace que la hibridación aumente conforme la conectividad con varios espacios virtuales. También la creación instantánea de otras culturas, esto desde el punto de vista del comportamiento del usuario de redes sociales con otras comunidades virtuales.

En la misma línea de la cultura no solo puede llegar a existir una cierta hibridación cultural, sino una interculturalidad y/o una contracultura pues el espacio de la redes sociales es demasiado grande que no se limita al establecimiento de nuevas culturas, sino a una transformación constante que sucede según las dinámicas o prácticas de la sociedad en el mundo virtual.

"La comunicación y los sistemas de comunicación son herramientas decisivas sin las que no sería posible la globalización económica y del poder (Jorge A. y García M, 2009)", (Zallo, 2011; 55).

A partir de esto el mismo autor afirma que la cultura dentro de la globalización se denomina tecno-cultural y esto se ha expandido a tal magnitud que adquiere la capacidad de no solo cambiar la calidad y condiciones de vida sino que se enfrenta a un poderoso sector económico.

Respecto a las condiciones de vida ahora las actividades humanas tienen relación a la tecnología. Las plataformas de internet y las redes sociales pasan a ser parte del entretenimiento y ocio de la humanidad. La utilización de tres pantallas al mismo tiempo

(televisión, móvil, computadoras/tabletas) es una actitud común de las personas conectadas a internet. Durante el día están expuestos a espacios tecnológicos que en determinado momento de su rutina diaria se introducen a la utilización de estos aparatos llevándolos al viaje virtual. Cada aparato está a la mano del usuario de internet y es cuestión de si desea estar conectado o no (Igarza, 2010).

Zallo (2010) remarca que la tecno-cultura se basa en las competencias tecnológicas. Oleadas de aplicaciones reemplazadas o modificadas cada mes, lo mismo con las actualizaciones de aparatos tecnológicos (móviles, tabletas, computadoras, entre otras). Como la convergencia de herramientas en un solo aparato: una cámara fotográfica con grandes capacidades en un teléfono móvil.

La tecno-cultura predispone a la sociedad a enfatizar la necesidad en la conectividad y la innovación cada vez más inmediata de la tecnología. Nuevos modelos de estratificación social como nuevos poderes políticos y de telecomunicación que provoca una legitimización y condiciones de vida en base a la tecnología.

1.3.2.3. Redes Sociales y política

En el ámbito de la política tanto los actores políticos como los ciudadanos expanden su pensamiento, ideología a través de las redes sociales. Se han visto campañas políticas o actores políticos que han generado gran impacto en la sociedad.

No solo rompe barreras de comunicación sino que abre espacios donde pueden conversar ciudadano y político y de esta forma generar una opinión sobre un determinado tema o acción de la política de un Estado.

En el año 2008 según Túñez y Sixto las redes sociales fortalecieron la comunicación política durante la campaña electoral que llevó a Barack Obama a la presidencia. Esto fue una realidad gracias al volumen de participantes en las redes, significa entonces una herramienta estratégica para un candidato o político particular. Se crea una relación interpersonal de todos a todos, del candidato a los ciudadanos y viceversa.

Los nuevos modelos de comunicación entre los partidos políticos y los ciudadanos se han dejado ver en estos últimos tiempos. Las oportunidades son enormes para sacar provecho y poder entablar una conversación directa con los ciudadanos. Estos ciudadanos no solo son activos en política sino que son participantes en ellas (ciberactivistas). Un ciudadano que participa activamente valiéndose de las herramientas tecnológicas que tiene a su alcance (Caldevilla, 2009).

Redes sociales, política y Compromiso 2.0: La comunicación de los diputados españoles en Facebook, estudio realizado por Túñez y Sixto (2011, p. 92) presentan como resultados la falta de participación o usos de redes sociales por parte de los políticos en España. A pesar de que existen millones de usuarios ciudadanos, la mayoría de los partidos políticos no aprovechan las herramientas tecnológicas y los grandes beneficios que esto puede provocarles en su carrera política.

1.3.2.4. Redes Sociales y movimientos sociales/políticos

La indignación, libertad de expresión, activismo, participación en luz verde en las redes sociales. Es un espacio que han aprovechado muchos actores para construir movimientos de gran impacto. Movimientos capaces de paralizar o despertar al mundo. Es cuestión de emitir un pensamiento, opinión de un suceso o acción por medio de las plataformas y esto se convierte en poco tiempo en algo global.

Ahora es muy fácil enterarse qué movimientos activos hay en cualquier parte del mundo. En ocasiones se han manifestado movimientos en un país específico pero al ser manejado por con las redes sociales digitales conecta a otros usuarios de otras partes del mundo, estos deciden unirse a la voz si es de su afinidad discursiva. Por mencionar algunos que han surgido en lo que va de la era digital pueden ser: #NosFaltan43, #YoSoy132 (México), 15M (España), #YoSoyLucía (Argentina), #RenunciaYa, #25A (Guatemala), entre otros.

Para Castells (2012) los movimientos sociales en Internet no necesitan un liderazgo como tal, un centro de mando o un control, así como no necesita una organización vertical y esto facilita mayor participación pues estas redes son abiertas sin límites de espacio.

En cuanto a la postura de la psicología social dice que la polarización en grupos en Internet hace que la discusión discursiva sea interminable por la ausencia de voces moderadoras. Un usuario puede expresar su opinión moderada sobre un tema pero al compartirla en la red puede que otro no esté de acuerdo y se genere una discusión desequilibrada y esto hace el abandono de la postura inicial. En ese caso solo se habla y no se comunica por la falta de un moderador (Wallace, 2001).

Sin embargo Castells (2012) defiende su postura proponiendo a una sociedad en un espacio de autonomía pues dentro de un movimiento existen otros movimientos y de esta manera se van configurando continuamente, esto permite no tener un centro identificable pero capaces de llevar a cabo indispensables funciones de coordinación deliberada a través de la interacción con el resto de redes interconectados por nodos.

El auge de las redes sociales vino a facilitar el proceso de la movilidad social, ya que según McAdam, McCarthy y Zald (1996) los movimientos sociales no disponen de herramientas fuertes para influir en la sociedad y las decisiones políticas, por esa razón se abocan a terceros para poder empoderarse y llegar hasta el último eslabón del marco político. Los mismos citan a Lipsky donde este explica que estos terceros pueden ser actores de las élites o los mismos medios de comunicación.

Sin embargo, en la actualidad no es necesario abocarse a terceros cuando la sociedad tiene en sus manos plataformas digitales que son más emergentes y poderosas que las grandes élites y medios de comunicación tradicionales en la política. Ahora los movimientos ya no son tan vulnerables como antes, ni manipulados o paralizados por intentos de burocratización, por lo que Castells (2012) expresa:

Los movimientos suelen comenzar en las redes sociales de Internet, se convierten en movimiento al ocupar el espacio urbano, ya sea mediante la ocupación permanente de plazas públicas o por las manifestaciones continuadas. El espacio del movimiento se hace siempre mediante interacciones entre el espacio de los flujos de Internet y las redes de comunicación inalámbricas, y el espacio de los lugares ocupados y de los edificios simbólicos objetivo de las acciones de protesta (p. 213).

La política no convencional es protagonista en los movimientos sociales conectados por las tecnologías. Esto ayuda también para que en los momentos de la protesta estén en constante interacción y en caso que los medios de comunicación tradicionales no brindan cobertura a la opinión, idea o movilidad de activismo social (Lasén, Martínez, 2008).

1.3.2.5. Redes Sociales y políticas públicas de Estados

Por razones comunicacionales, políticas, culturales, empresariales, sociales y otras más, es importante que las instituciones estatales de cada Estado del mundo tomen en cuenta las políticas públicas necesarias para que el mundo digital y de redes sociales sean espacios de derechos constitucionales, ciudadanos y políticos siguiendo la línea democrática.

Las redes sociales son parte de las nuevas Tecnologías de la Información y Comunicación (TIC's) esto significa que el acceso hacia ellas debe ser indispensable para que se lleve a cabo el derecho de comunicación. Según Cristancho y Barreda (2015) en su texto El derecho a la comunicación en el entorno digital: Implicaciones para el ejercicio ciudadano, explican que es necesario que las TIC's estén al alcance de toda la población posible pues esto abre espacios donde se pueda actuar como ciudadano democrático y ser capaz de expresar su opinión, pensamiento o ideas sobre políticas públicas.

No hablar solo de una democracia como tal sino de una democracia 2.0 o ciberdemocracia. Crean una comunicación horizontal con los actores políticos y los ciudadanos (Caldevilla, 2009). Estar conscientes que algunos ciudadanos son potenciales agentes activos en la producción de contenidos web que están esperando una aparición política organizada e innovadora que establezca una interacción entre ambos sectores desintermediada. Esto crea un espacio colaborativo, transparente, participativo y un mejoramiento de la rendición de cuentas por parte del Estado (Criado y Rojas, 2013).

La necesidad de generar cambios a las políticas públicas sobre el internet es evidente, pues ahora hay que basarse en normativas tecno-culturales por el simple hecho que existe una proliferación de cadenas digitalizadas, el uso exitoso del teléfono móvil, la convergencia de medios, los nuevos usos de la comunicación, así como las redes sociales, los intercambios

de contenido y el uso de plataformas multi-usos que requieren un respaldo democrático (Zallo, 2011).

Este mismo autor plantea las posibles nuevas políticas culturales que se deben de considerar para aplicarlas en un territorio:

a) apoyo a la universalización de las redes para todos los ciudadanos en claves de accesibilidad y asequibilidad; **b)** fomento de la educación en los usos tecnológicos; **c)** fomento de producción de contenidos culturales y comunicativos digitales; **d)** impulso de acceso a los contenidos culturales en claves de integración social y participación ciudadana, incluyendo el reforzamiento del servicio público (E. Bustamante y R. Zallo, 2009, p. 263), (p. 386).

Un principio que busca la implementación de políticas públicas y regulaciones en TIC es el de generar las condiciones para que el acceso, uso y apropiación de las TIC sea equitativo e incluyente, particularmente para aquellos sectores de la población que por diferentes circunstancias se han visto excluidos de la estructura de oferta y demanda de actividades de las TIC, lo cual ha limitado su capacidad de participación social y política (Beckers & van den Besselaar, 2014), citado por Cistancho y Barreda (2015; 20).

En el caso de Guatemala, Gómez y Sandoval (2015), se encargaron en desarrollar el tema: El derecho a la comunicación en el entorno digital, una tarea pendiente en Guatemala, esta publicación se encuentra en el texto: Centroamérica, democracia desconectada. En el abordaje de la problemática sobre la infraestructura, servicio y usuario, el país se encuentra atrapado en las élites mediáticas y empresariales encargadas de brindar servicios de navegación, telefonía móvil, televisión digital entre otros.

Los datos brindados reflejan que no existen políticas públicas adecuadas o prácticas irregulares pasando por encima de las normativas de Ley y dando entrada al empoderamiento mediático y al monopolio. Así también se detecta que no hay una regulación fuerte por parte del Estado y se entiende que puede estar involucrado en este

tipo de negociaciones por intereses económicos y políticos, sin importar el beneficio de la sociedad.

El uso de las TIC en este caso de la redes sociales por parte de la sociedad es de gran beneficio, ya que son alternativas tecnológicas que facilitan en todo sentido el acceso a la información y la práctica del derecho de comunicación, estipulado por la Corte Interamericana de los Derechos Humanos (CIDH), la cual expresa: "Garantizar, proteger y promover el derecho a la libertad de expresión en condiciones de igualdad y sin discriminación, así como garantizar el derecho de la sociedad a conocer todo tipo de informaciones e ideas", (CIDH, 2014, numeral 14).

1.3.3. El lado oculto del ciberespacio

"Internet es el primer sistema creado por el ser humano que la humanidad no entiende, el mayor experimento en anarquía que jamás hemos tenido (Eric Schmidt, s.f)" (Chatfield, 2001).

El ciberespacio está construido con la misma complejidad social, pues entenderlo no es del todo fácil. El acceso a este espacio virtual conlleva muchos trasfondos interminables de explicar. Al hablar sobre lo que no se ve del Ciberespacio se refiere a los actores que obtienen la información y es utilizada para realizar malversación o manipulación de datos obtenidos por medio de plataformas o sitios digitales.

Chatfield (2011) dice que el Internet es una herramienta potente pero, cuando este está en manos de regímenes represivos y censuradores del mundo, puede tornarse peligrosa para todos aquellos que utilizan las herramientas para ejercer sus derechos como ciudadanos, así como la libertad, la mejora y el crecimiento del conocimiento.

"El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes", afirma Ribas (1998; 55).

Así como existe ingenio para crear espacios virtuales es el mismo ingenio para destruirlos o mal-emplos. La creciente utilidad de la información y del mismo Internet provocan que el robo de datos, virus, la ecología software malicioso se proliferen en la red (Chatfield, 2011, p. 84).

Las ventajas del Internet pueden llegar a ser sus mismas desventajas. Se obtiene información pero en un sentido macabro esto puede ser utilizado con fines destructivos, distorsionadores. Centrar esta idea en que el mal no está en las herramientas sino en la persona o usuario que las utiliza (Ribas, 1998).

Edwards y Edwards (2001) describen al Ciberespacio como un espacio personal enfatizando que es el usuario quién decide qué información tener o dar en la red, construye su propia red de amigos, páginas o sitios de navegación. Estas acciones hacen del Internet un espacio donde los cibernautas se desenvuelven personalmente. Aunque en la lógica general la relación se tenga con la pantalla, la conexión a la red hace que la proximidad sea íntima.

Asimismo plantea que las acciones spamming provocan una ruptura en el espacio personal y este se ve vulnerable ante ataques de contenido en correos electrónicos no deseados y recibidos repetidas veces. Es decir, el efecto de la práctica del spam es el rechazo total a su contenido, porque viola el espacio personal del usuario, se entromete agresivamente que no existe una respuesta a dicho correo.

"El correo no deseado" como mayormente se le conoce ha existido la misma cantidad de años que la creación del correo electrónico. Una actividad que contamina el mundo digital. Los spam son prácticamente basura y esta está formada por enlaces hacia otros sitios web, blogs y buscadores (maniobras basuras). La saturación de este tipo de información basura será una amenaza cada vez más importante para la vida del Internet (Chatfield, 2011).

Los spam han sido administrados por grandes corporaciones que se han enfrentado a grandes problemas legales con costos millonarios. *Cyberpromotions* fue obligada a retirarse de todos los servicios *on-line*. Otra empresa a mencionar es *Apex Global Internet Services*,

el director de esta, Phillip Lawlor recibió amenazas de muerte por la operación de correos no deseados. Esta acción describe el rechazo total de los usuarios, pues la explicación más valedera en este asunto es que las empresas de spamming violan el espacio personal de los internautas que estos se ven amenazados y deciden demandar (Edwards y Edwards, 2001).

Las redes de las telecomunicaciones han construido un mundo mucho más difícil de controlar que el propio mundo territorial. La naturaleza del Internet hace que sea complicada la persecución de delitos o acciones que tientan en contra de la humanidad, así como la no implementación de medios con una codificación segura provoca esta limitante y problemática en el ciberespacio (Ribas, 1998).

Chatfield (2011), explica dos tipos de acciones maliciosas, las más comunes hasta ahora:

El *scamming*, es el proceso más general por el que los *spammers* intentan sacar dinero de sus víctimas -una práctica asociada con los típicos trucos de *scamming* son los emails pidiendo al receptor que ayude a una supuesta tercera persona a sacar una gran suma de dinero de un país extranjero a cambio de una comisión-.

Mientras que el *phiship* es una técnica frecuente por la que los correos de spam y las páginas maliciosas intentan obtener detalles personales de usuarios incautos, que pueden ir desde los datos de conexión a la cuenta de e-mail y de la web, hasta los de la cuenta corriente o tarjeta de crédito (p.89).

Algunos críticos ven un final tenebroso para la sociedad, pues plantean que la sociedad se ve beneficiada al utilizar el Internet como medio de información y comunicación, pero lo que esto puede provocar es crear espacios de control y vigilancia por los mismos centros de poder. Expresan que cada vez existe mucha más oportunidad a que esto suceda por la creación de tantas plataformas (Kollock y Smith, 2003, p. 21).

Por la sofisticación de los usuarios hacia el internet o la fuerte labor que han hecho muchos informáticos para contraatacar a los *spammers*, estos últimos se han vuelto también expertos en la materia, con las técnicas actuales un spam ya no es solo por correo electrónico si no que se ve expuesto en virus creados por medio de dispositivos pirateados

obteniéndolos de los mismos usuarios. La persecución hacia los actores ha sido un fracaso, viajar de país en país ha hecho que la ilegalidad al spam sea inalcanzable para algunos estados interesados en establecer sanciones judiciales ante estas acciones (Chatfield, 2011).

Estas acciones son una pequeña parte del crimen que se almacena en el ciberespacio, sin embargo esto es la punta del iceberg. No solo del crimen se trata el ciberespacio, sino como mencionan Kollock y Smith sobre los espacios de control y vigilancia por parte de centros de poder o la existencia de la censura en la información como en los mensajes emitidos por los usuarios hace que la oscuridad del ciberespacio sea más grande, poco entendida y poco conocida.

A pesar que las plataformas, sitios web, espacios virtuales en la red se establezcan o se crean bajo términos y condiciones de uso o principios a cumplir, es difícil cumplir esta parte, porque no es fácil regular el mundo en sí, cómo se alcanzará controlar lo que se ha creado en el ciberespacio. Sin embargo, pretender regularlo es el reto que se tiene en la actualidad.

Otros actores que vale la pena hablar son los hackers, antes de ahondar más de ellos es importante aclarar que en general la actividad de hacking se orienta en distintos fines que definen que tipo de personas lo realizan. El hacking en general es una práctica para obtener información con tácticas y acciones informáticas de expertos.

Para Chatfield (2011) la cultura hacking actúa bajo una clandestinidad digital innovadora que puede llegar a tener varios logros tanto para fines benévolos como fines malévolos. Para esto el autor relata que a los inicios de la era del internet ser un hacker era un halago, porque se idealizaba como el experto en informática y habilidoso en usar herramientas o sistemas no convencionales para cualquier tipo de cosas. Sin embargo, conforme fueron avanzando los conocimientos del ciberespacio, algunos expertos se dedicaban a realizar estas mismas acciones pero con un fin mal intencionado y por esta razón en la actualidad al hacker se le refiere a toda aquella persona que es capaz de sabotear la seguridad, integridad y privacidad de los usuarios en Internet.

1.3.3.1. Identidad digital

Tanto para generar como para acceder a la información en el ciberespacio e independientemente si es a través de buenas o malas prácticas, se debe de tener una identidad en el mundo digital. Esta identidad actúa de forma similar a la identidad que cada individuo tiene en la sociedad territorial, pues en la global se proporciona el nombre, lugar de origen, edad, ocupación, intereses personales, entre otros elementos que van construyendo a la persona en usuario virtual.

"El mero hecho de que algo sea públicamente accesible no significa que la gente quiera verlo hecho público, D., Boyd", (Chatfield, 2011, p. 92).

Con la creación del internet la identidad se configuró para que sea utilizada con un lenguaje virtual y así tener la posibilidad de interactuar con los demás usuarios y sobre todo poder dejar huella para que sea parte de la realidad digital. Al reunir esto se incorporan nuevas características de la identidad digital, pues hay que tomar en cuenta que no se queda en un pequeño círculo de personas sino que se convierte en una identidad global (Fundación Telefónica, 2013).

En el espacio territorial se tiene un número de identificación como registro para cada persona en el país de origen, pues en el espacio virtual se tiene una serial en internet. El Protocolo de Internet o la dirección IP es el código de cada usuario, página o perfil social en la web. Este número está compuesto por una cifra de cuatro bloques separados por puntos y ofrece una dirección numérica específica. Ej.: 000.000.000.000 (Chatfield, 2011, p. 92).

La identidad digital entonces es la recolección de información publicada en el ciberespacio sobre un individuo (Oficina de Seguridad del Internauta, s.f). Así como la actividad que se genera en la red forma parte de la identidad y esto está ligado con el aprendizaje y experiencias que cada usuario obtiene al interactuar en Internet (Giones y Serrat, 2010).

En el texto Identidad Digital: El nuevo usuario en el mundo digital, publicación de Fundación Telefónica (2013; 9) explica: "la huella que las personas dejamos en la Red es

potencialmente permanente, puede ser enlazada, sigue un orden cronológico y en muchas ocasiones, no puede ser borrada porque es información que ha sido compartida con otros".

El abordaje de la información que se comparte es debate actual sobre la privacidad y seguridad que se obtiene al interactuar en la red, asimismo la reputación que se va construyendo en ella.

Para esto las autoras Giones y Serrat (2010, p. 6), explican que es importante tener presente "quién habla de quién, en qué sitios y de qué manera. No es lo mismo la opinión de una persona poco visible, que la opinión de una persona muy visible, que difundirá sus juicios de manera más rápida y probablemente a su vez a personas también más visibles".

1.3.3.2. Privacidad

En los casos antes mencionados es necesario preguntarse, ¿qué pasa con la información que se almacena en la red?, ¿qué sucede con las fotografías que se suben a una red social o se envían por un chat "privado"?, ¿cuáles son los riesgos que se corren al dar los datos personales a un sitio web?. Esta y otras preguntas hay que resolverlas para poder entender y conocer a profundidad las dinámicas existentes del Internet y qué tanta seguridad hay para proporcionar la información del usuario.

Para Chatfield (2011, p. 92), la privacidad se divide en dos grandes trazos: el primero son todos aquellos datos que se suponen que son absolutamente privados y protegidos de cualquier amenaza virtual, y el segundo las zonas de una privacidad relativa en la cual puede ser compartida por terceros a través de condiciones de seguridad básicas para establecer quienes tendrán accesibilidad a esta información.

La información que se puede encontrar en internet sobre una persona determinada es porque fue proporcionada por esa misma persona o por alguien más (institución, medios de comunicación, empresa, etc.). Esto debilita la privacidad personal, pues entre más información exista sobre el individuo mayor será el riesgo de que sea utilizada de manera indebida por todos esos actores mal intencionados en la red (Oficina de Seguridad del Internauta, s.f.).

El acceso de la información que se almacena en la "nube" o red es infinita y esta puede ser compartida por medio de las redes sociales, páginas de compra y foros donde las personas publican datos personales que dejan registrada su actividad virtual, preferencias y gustos, siendo capaces de definir comportamientos virtuales de cada usuario según sus movimientos en la red (Fundación Telefónica, 2013).

La proporción de datos como el número de identidad personal, correo electrónico, datos bancarios, ubicación geográfica, pueden ser alterados y vulnerables ante actos como el *phishing*, fraudes y usurpación de personalidad. Así como el aumento de spam en los servicios de información que se utiliza. Así también las solicitudes de amistad en las redes sociales que se tiene alguna actividad virtual (Oficina de Seguridad del Internauta, s.f.).

El mayor problema de la privacidad en el Ciberespacio es la falta de conciencia por parte de los usuarios sobre la información que se está compartiendo; este es el segundo problema después de las prácticas de hacking. Compartir información en varios sitios web sin revisar detenidamente qué se está dando a conocer puede llegar a causar daños a la identidad que se tiene en el espacio virtual (Chatfield, 2011).

El mismo autor narra en su texto 50 cosas que hay que saber sobre el mundo digital (2011, p.95) cómo la revista Wired en su portada publicada en el año 2011 mostraba como parte de su diseño la información que se sabe de una persona en Internet, desde la fecha de cumpleaños, hasta las últimas compras realizadas. Todo está registrado, todo lo que se hace en Internet se sabe.

El contenido que se comparte es parte de la visibilidad de la persona en la red. " Esta visibilidad puede ser autoconstruida a partir de los posts de un blog, los mensajes de Twitter, los comentarios a vídeos, fotos ..., pero también puede ser fruto de referencias o comentarios de terceros", explican Giones y Serrat (2010).

Por otra parte, las fotografías y videos subidos a la nube de Facebook, Gmail, Twitter o cualquier plataforma utilizada para compartir este tipo de información hace que no sean

privadas en un 100%, pues basta con escribir el nombre de la persona en algún buscador de cualquier navegador y aparecerán fotografías o vídeos de la persona.

La página oficial de la Oficina de Seguridad del Internauta (OSI) del Gobierno de España y del Instituto Nacional de Ciberseguridad (s.f.), determina que las actividades virtuales también son registradas por medio de los navegadores que se utilizan. El historial, contraseñas, cookies de navegación son elementos que quedan registrados en la nube.

La vulnerabilidad de los servicios online está a la orden del día por la configuración del sistema virtual en el que fue construido el sitio. En el año 2010 la red de blogs Gawker reveló que fue víctima de filtración de datos de sus usuarios por ataques de hackers, alterando a 1,3 millones de usuarios por medio de sus contraseñas que no tenía una codificación fuerte. En este sentido Gawker, dio a conocer la importancia de manejar distintas contraseñas para todos los sitios web en los que se navega, esto para que no se tenga fácil acceso a otras posibles cuentas que posean una misma contraseña (Chatfield, 2012, p. 93).

Según la página de Google (2017) www.google.com en la sección de privacidad describe:

Información que proporciona el usuario: En ese caso, te pediremos información personal, como tu nombre, tu dirección de correo electrónico, tu número de teléfono o tu tarjeta de crédito que almacenaremos con tu cuenta. Si quieres aprovechar al máximo las funciones para compartir que ofrecemos, también podemos pedirte que crees un perfil de Google visible públicamente que puede incluir tu nombre y tu foto.

Recogemos información sobre los servicios que utilizas y la forma en la que los usas (por ejemplo, cuando ves un vídeo en YouTube, visitas un sitio web que utiliza nuestros servicios de publicidad o ves nuestros anuncios y nuestro contenido e interactúas con ellos. Entre la información obtenida de esta forma, se incluyen los siguientes datos:

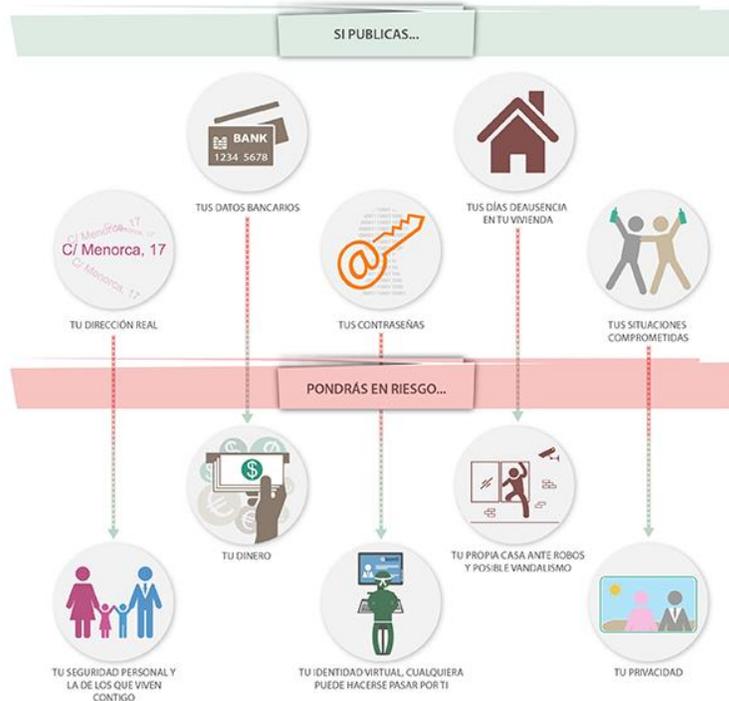
- Información del dispositivo

- Datos de registro
- Datos sobre ubicación física
- Números exclusivos de la aplicación
- Almacenamiento local
- Cookies y tecnologías similares

Es decir que los servicios de Google enlazan a otros servicios en los cuales los plantea como facilidad de acceso a la información, sin embargo esto puede llegar a ser un riesgo si el dispositivo (computadora, teléfono móvil, tableta) es robado abre la posibilidad de que se pueda acceder fácilmente a esa información. Otro riesgo es la creación de programas o páginas web diseñadas precisamente para robar datos de ese estilo.

A pesar que los datos o información de usuarios es la materia prima de varias empresas que tienen actividad por internet esto se torna peligroso a la intimidad de los datos adquiridos. El compartir información en las páginas de servicios web, las mismas redes sociales o del comercio electrónico crea una vulnerabilidad ante actos de revelación que pueden llegar a afectar al usuario, cliente o a la persona quien esté proporcionando dichos datos. Sin embargo, esto es requisito para poder sobrellevar cierta seguridad y de veracidad de identidad de la persona con la que se está interactuando (Fundación Telefónica, 2013).

En estos casos la brecha entre la información privada de los datos personales en la red y la información pública es muy delgada, a pesar que cada página web dentro de sus servicios ofrezca cierta seguridad o privacidad con la información requerida se ve amenazada por otros mecanismos mal intencionados que se crean para poder construir un ciberespacio criminal y lograr hechos concretos difíciles de detener o de descifrar su verdadero origen.



Esquema elaborado por la Oficina de Seguridad del Internauta (s.f).

1.3.3.3. Cibercrimen

Todas las malversaciones, alteraciones o acciones mal intencionadas son originadas por una organización criminal que llegó a existir en Internet. Con la facilidad que se tiene para que una persona se conecte con otra persona, es la misma facilidad para el criminal conectarse con su víctima. El cibercrimen ha sido un negocio también para todos aquellos que generan grandes ingresos económicos a través del juego sucio que se puede realizar en Internet.

Para Téllez (1998) plantea tres características del cibercrimen 1) es un acto ilícito practicado por una persona experta en aspectos técnicos, informáticos y digitales. 2) Dificultad para la detección del actor y en sí de la acción que se cometió, 3) así como el medio que se utiliza para efectuarlo.

Por su parte Sánchez (2012) describe al cibercrimen a todo acto delictivo como el fraude, robo, falsificación, espionaje, sabotaje, extorsión, piratería e invasión a la intimidad de la

persona. Todo esto ejecutado por medio del internet. Las prácticas de *hacking*, *phiship*, *spam* y *scam* descritas anteriormente, construyen el cibercrimen.

Se ha mencionado varias veces que se necesita de expertos para estas prácticas, ingenieros en sistemas e informática para lograr sabotear un gobierno, un país, una persona. No solo una virtud negativa como tentar a la vida, intimidad o integridad de alguien o grupo de personas, sino estudios previos para poder efectuar un delito en el ciberespacio. Para ello, se definen algunos actores expertos en la materia del cibercrimen, considerandos los que han sido descifrados hasta el momento:

- Sicario digital:

Según Assardo (2016) un sicario digital es el encargado de hacer el trabajo sucio en Internet, contratado por una persona u organización para cometer el crimen hacia una entidad o personaje, "asesinando" la reputación de la misma. Estas dinámicas han sido reflejo en las redes sociales, donde personas sin una identidad realmente definida ridiculizan a cualquiera, sin dar explicaciones y sin un motivo alguno. No actúan físicamente, pero al ser perpetrado en la red provoca que la información se altere globalmente.

- Trol:

Para Meneses (2012) un trol o trolls son personas mal intencionadas que se dedican a molestar o fastidiar a todo usuario que tiende a abordar temas sociales o políticos, con tal de desviar la atención del resto de usuarios con el simple propósito de provocar un linchamiento o descontrol dentro de la red.

Según la RAE un trol es un usuario de Internet que escribe comentarios para llamar la atención e interrumpir el diálogo racional en un foro.

- Bots:

La misma autora explica que un bot o robot es creado para realizar las tareas rápidamente de un humano y muchas veces es utilizado para maniobrar en la información. Las prácticas

de estos robots son delictivas porque son creados para realizar tareas de un trol o un sicario digital, sin embargo su rendimiento y su velocidad de ejecución es más acelerada, con capacidades humanamente inalcanzables.

Sicario, troll, bot, hacker, no importa cómo se nombre o defina, las prácticas que realiza son similares, depende su fin y el hecho delictivo que cometa. Lo importante acá es la capacidad que tiene para provocar un ambiente tenso e inseguro en la red. Un ambiente poco estudiado, poco conocido y poco controlado.

La capacidad del cibercrimen es demasiada que se puede provocar una guerra, un ataque terrorista o sabotear un gobierno. Como se ha mencionado repetidas veces el control en el Ciberespacio es muy difícil de realizar por la forma en la que fue creado, siendo vulnerable a actos delictivos o altamente peligroso.

En cuanto a la ciberguerra es una confrontación de estados por medio de herramientas digitales. No se tiene armamento físico pero sí se tiene la capacidad de perjudicar la infraestructura digital de gobierno, militar, económica de una nación (Chatfield, 2011).

"Las redes de transporte -por carretera, aire, ferrocarril, y mar- se apoyan todas ellas en mayor o menor grado en la tecnología para funcionar... la bolsa de valores... pueden quedar gravemente alteradas por los ataques digitales", expresa el mismo autor (p. 104).

En el caso del ciberterrorismo no es una simple delincuencia pues como se sabe el fin del terrorismo es afectar a un colectivo de gran número con intenciones políticas y religiosas. Ahora las armas, bombas o misiles son programados por computadoras que se valen del ciberespacio para poder perpetrar en el blanco (Sánchez, 2012).

Por su parte Chatfield (2011), determina dos tipos de técnicas en la ciberguerra. "El espionaje: recabar información secreta para ganar ventaja... y sabotaje: infringir daños en un aspecto de la infraestructura digital", (p. 105). En cuanto al espionaje narra que hay varios tipos pero esta práctica hace que las naciones obtengan mucho si recolectan información de manera encubierta de sus naciones adversarias, sin embargo esto no genera

una guerra como tal, sino que una simple ventaja en información. Caso contrario del sabotaje y vandalismo ya que su fin es llegar a una guerra por medio del ciberterrorismo.

Otro tema a abordar, específicamente en las redes sociales es la creación de cuentas falsas o cuentas con identidades digitales robadas. La dinámica es actuar bajo un perfil cuya actitud es manipulante, impotente y grotesca. Para ello, Redondo (2016), explica en su artículo "Sobre los perfiles falsos en redes sociales", que existen distintos tipos de usuarios "*fakes*"/ falsos que se pueden detectar fácilmente:

- Usuario que se esconde tras un perfil falso para atacar: sus post o tuits están cargados de insultos y groserías. Orientan al odio.
- Usuario que se esconde tras un perfil falso para expresar algo que no quiere hacerlo de manera transparente: usa la red social como válvula de escape para expresar lo que no se atreve a hacerlo en su entorno y de esta forma suele sentirse en su zona de confort.
- Usuario que se esconde tras un perfil falso para dar rienda suelta a su ingenio (con humor o de mal gusto): crean contenido de manera viral ya sea para burlarse de alguien o hacer reír al resto de usuarios con temáticas sociales o políticas.
- Usuario que se esconde tras un perfil falso para expresar bondad a través de acciones benéficas: cuentas cargadas de contenido de solidaridad y obras de caridad bajo un anonimato alto sobre quién realiza la acción. Su objetivo principal es "evangelizar" con acciones benéficas.
- Usuario que se esconde tras un perfil falso para obtener beneficios de forma fraudulenta: cuentas cargadas de links de páginas virtuales que roban información confidencial a todo usuario que ingresa. De esta forma logran realizar movimientos bancarios maliciosos.

Según Assardo (2016) una cuenta falsa es fácil de identificar la mayoría de veces, sin embargo existen casos que manejan un estilo tan real que es fácil caer en esas oscuras redes. La suplantación de identidad da cabida a que muchas personas acepten solicitudes de amistad sin pasar desapercibido de la veracidad del usuario que se acaba de agregar a la lista de amigos o seguidores. Otras características:

- El avatar o foto de perfil que muestra da un contexto de odio o de "perfección". Fotografías bajadas en buscadores o montajes bien hechos.
- El *user* o el nombre de la cuenta puede ser burlesco o intencional con alguna persona determinada.
- El número de amigos o seguidores puede ser un factor importante para ser identificados, pues si la cuenta tiene pocos seguidores a comparación de las personas que sigue o viceversa puede dar señal que es una cuenta falsa.
- Así también, la interacción o la forma de actuar con otros usuarios ya sea en sus comentarios o posts es una señal muy importante para detectar el discurso que maneja la cuenta.
- El contenido que publica depende del discurso y el fin de la cuenta.

Hoy en día existe la idea de *net centers* y su forma de operar. Mediáticamente y socialmente se percibe como algo negativo o acciones delictivas, sin embargo en el caso de Guatemala no existe dentro de la Constitución un artículo o reglón que hable sobre algún delito sobre este tipo de empresas. Según Enríquez (2016, s.p) los net centers: "agencias que no son “buenas” ni “malas” per se, simplemente ofrecen un servicio de manejo de redes, presencia web, publicidad digital, etc. Es otra historia si eso degenera en un uso inadecuado o inapropiado (como campañas negras, ataques, insultos, bullying, etc.)".

Para Assardo (s.f) los net centers actúan "bajo de agua", por esta razón es difícil obtener un tipo de dominio o página al cual ponerse en contacto. En este sentido, el único contacto que se puede llegar a tener es a través del mismo perfil falso creado por la agencia.

Cronología	
1999	<i>Hackers</i> serbios atacan sistemas de la OTAN.
2007	Se produce el mayor ciberataque en la historia de EE.UU.

2008	Se determina la política de ciberdefensa de la OTAN.
2010	EE.UU. nombra a su primer general de la ciberguerra.

(Chatfield, 2011, p.104-105).

a) El cibercrimen en medios de comunicación

El cibercrimen se refleja en cualquier rincón de la red hasta llegar a afectar a los que se describen como los expertos en la información, es decir los sitios web de los medios de comunicación. Medios digitales que han recibido amenazas o han sido víctimas de ataques cibernéticos o bien han formado parte del cibercrimen para obtener información de manera clandestina.

En este mundo digital se sabe que todo está expuesto a la vista de muchos cibernautas y en este sentido los medio digitales han sido víctimas de los usuarios trol pues estos se han dedicado a desviar información por medio de comentarios groseros, prepotentes y amenazantes. Estos casos han hecho que los medios caigan en duda de su veracidad con la que trabajan y publican la información. Es común que este tipo de usuarios manejen una identidad falsa o un perfil falso para realizar estas prácticas, por el simple hecho que temen a ser descubiertos (Finoll, 2014).

En este sentido los mismos medios de comunicación difunden un juicio en contra de los hackers, presentándolos como piratas, ciberpiratas, delincuentes informáticos y que actúan con malas intenciones para agredir, atacar y con esto provocar un ambiente negativo en la red. Este fenómeno, se da por cómo los medios han sido víctimas de este tipo de personajes en sus sitios web, de lo contrario los catalogan como colaboradores para asuntos policíacos, resolución de casos de alto impacto que requieren de un experto en manejo de información para obtener pruebas contundentes en dichos casos, explica Rodríguez (2001) en su estudio Feos, sucios y malos: la imagen de los hackers en los medios de comunicación, presentado en el IV Congreso Chileno de Antropología.

Un caso nacional que se puede mencionar son los insistentes ataques que ha presenciado el sitio web del medio digital Nómada.gt, pues su director general, Martín Rodríguez Pellecer ha dicho públicamente dentro de sus artículos o cuentas oficiales en redes sociales los ataques que han recibido. Según él, es por la línea del medio, investigar y sacar la verdad de diferentes situaciones en Guatemala.

Para Finoll (2014) estas prácticas irrumpen con las dinámicas de los medios de comunicación, porque formulan un debate impuesto por los trol o usuarios criminales. Los comentarios o el feedback de la audiencia hacia el medio se ve también afectados en el momento que se topa con un usuario de dudosa procedencia y que se suma a reclamar, amenazar o intimidar a todo aquel que demuestre interés por el contenido que se difunde.

Por eso es importante establecer protocolos de seguridad para los periodistas que publican en medios digitales. El riesgo que corre el periodista sobre ataques en Internet es mayor, porque la información personal sobre el mismo es de fácil acceso para el victimario. Desde su nombre, rasgos físicos, hasta su ubicación (Assardo, s.f).

b) El cibercrimen en la ciberpolítica

La ciberpolítica también se ve amenazada tanto para sabotear la democracia de las naciones que la practican como para destruir la imagen pública de algún personaje político. Es un tema que los mismos políticos y sus asesores no han atendido a profundidad. Se utilizan las redes sociales o el ciberespacio con muchas deficiencias durante una campaña política o comunicación constante con la sociedad, sin embargo esto se ve vulnerado ante la gran organización del cibercrimen (Assardo, 2016).

Este mismo autor explica que la efectividad de una campaña negra no es tan alta en la actualidad como el trabajo que puede llegar a generar un *netcenter*, el impacto puede ser más trascendental: "Los *webcenters* o *netcenters* por aparte son empresas digitales que responden a un cliente. Son más peligrosos y, por ende, más caros".

El cibercrimen puede llegar a desestabilizar a un Estado, sabotando los servicios públicos brindados al ciudadano. Códigos de programación, infiltraciones a sitios web importantes

para un gobierno son algunas de las prácticas que puede llegar a alcanzar la delincuencia en Internet (Miró, 2012).

Para Sánchez (2012) el cibercrimen se vale del Internet para obtener grandes cantidades de dinero, encargos delictivos para bloquear páginas web con fines políticos, propagar virus que dañen o puedan robar información importante y finalmente la construcción de espacios para el crimen organizado de manera virtual e impactante.

Se necesita de profesionales en la informática para realizar estos actos delincuenciales y es evidente que la remuneración a este tipo de trabajos es alta. En el caso de la contratación de *net-centers* para el desarrollo de una campaña política en temporada electoral en un determinado país tienen la modalidad de edificar el contrato a favor del operador o del colaborador, pues en el caso que el personaje político sea electo a determinado puesto público, este último automáticamente tiene que brindarle un espacio laboral, según explica Assardo (2016) en su artículo sicarios digitales:

Tanto sicarios digitales, como *netcenters*, incluyen dentro de sus contratos que cuando los partidos políticos lleguen al poder les den empleo. Aquí es donde empieza el peligro real. Con recursos estatales y mezclados con personajes oscuros que hacen inteligencia pueden tener acceso y, a partir de ese momento, su poder puede ser letal. A eso sumemos que no existe legislación ni entidades destinadas a la investigación criminal en Internet, que vaya más allá de buscar pedófilos.

Según Meneses (2012) las elecciones mexicanas en el año 2012 fueron procesadas a través campañas y acciones realizadas por medio de las redes sociales. Facebook, Twitter y YouTube fueron las redes más utilizadas por los partidos políticos. La estrategia de campaña de la mayoría de candidatos era más para su beneficio que para la inclusión o involucramiento de los ciudadanos.

Sin embargo, la autora expone que la utilización de redes sociales en las campañas electorales en México reflejó mañas o similares trampas evidentes en el medio televisivo,

pues en el caso de Twitter se utilizó la compra de usuarios, bots y expertos informáticos para generar un acarreo digital.

En las redes sociales se pueden detectar perfiles de dudosa procedencia. Esto inicia desde el gran impacto que ya se conoce y cómo estas plataformas pasan a ser espacios de protestas o de expresión para abusos o injusticias políticas, sociales y económicas. Por esta razón, los actores políticos por conveniencia propia o "estabilidad" en su imagen se ven presionados a recurrir a la creación de perfiles falsos para desviar o manipular el mensaje que se torna amenazante para ellos. Así también estos perfiles son utilizados tanto a favor como en contra para un determinado político (Assardo, 2016).

Por lo cual Meneses (2012) cita un estudio avalado por el Tecnológico de Monterrey y realizado por Paola Ricaurte donde se evidencia la creación masiva de cuentas artificiales de seguidores en la cuenta oficial de Enrique Peña Nieto y Josefina Vázquez Mota.

Se pudo evidenciar por el volumen, la fecha, hora y lugar de creación de cuentas. Para el caso de Josefina Vázquez Mota, en una muestra de seguidores tomada por la investigadora el 25 de abril, aparecía que el 57% de cuentas sin tuits habían sido creadas en octubre de 2011, con diferencias de minutos y, de ese porcentaje, el 90% tenían su origen en Estados Unidos y Canadá. Esta fue la estrategia electoral en las redes que predominó en el proceso electoral por parte de los partidos políticos ("Entre bots y trolls", párr. 4).

Siempre en el tema de las elecciones políticas, el caso que vale la pena mencionar es el de Estados Unidos pues la campaña presidencial del 2017 mantuvo mucha interacción y utilidad en las cuentas de los dos candidatos más influyentes. Los ataques en redes sociales entre Donald Trump y Hillary Clinton, provocaron que ambos candidatos a la presidencia iniciaran una persecución de datos delatores para interferir en la campaña política de cada quien. Trump llegó al punto de expresarle a Rusia su deseo de que "hackearan" la cuenta de Clinton para obtener correos que tenían información reveladora, esto causó un caos en la campaña de la candidata Demócrata.

En el caso de Guatemala el uso de redes sociales en cuanto al marco político se fortaleció en las elecciones 2015. Un espacio virtual saturado de propagandas o etiquetas que identificaban a cada candidato que estaba en campaña electoral.

#UsemosElBisturí, #LeToca, #NiCorruptoNiLadrón formaron parte del espacio de las redes sociales, con discursos que creaban un ambiente dinámico y tenso al mismo tiempo entre los usuarios y los candidatos. A raíz de eso surgieron usuarios que se encargaban de ridiculizar los discursos o etiquetas que publicaban en Facebook o Twitter. Así como estar en contra o a favor de cierto candidato. Y por qué no, contratar empresas o agencias de publicidad encargadas de posicionar marcas de manera digital, solo que en este caso, en el año 2015 candidatos como Baldizón decidieron posicionarse a través de estas prácticas "publicitarias".

Fue en ese año que los net centers surgieron como la nueva estrategia política para lograr una presidencia. Para Enríquez (2016) estas agencias van creando cortinas de humo, manipulando la opinión pública a través de cuentas falsas o trolls y esto cada vez es mayor. Estos usuarios están al pendiente de publicaciones específicamente de Gobierno o de política para atacar al emisor, ya sea este un medio de comunicación o un ciudadano practicando su derecho a la libre emisión del pensamiento.

El primer net center que se detectó en el período electoral en Guatemala fue el de Manuel Baldizón, esta empresa se dedicó durante meses a posicionar el famoso "Le Toca". En cierta forma fue tendencia, sin embargo el destape del caso de La Línea y la agrupación de corruptos de Otto Pérez Molina y Roxana Baldetti provocó un desgaste de expectativas dentro de la población. Tanta fue la indignación social que el sentir y pensar se enfocaron en contradecir la idea principal de Baldizón y dejarle claro que el "No Te Toca" iba a ser su único logro. Posteriormente en el año 2017 salió a la luz que el Movimiento Cívico Nacional (MCN) fue parte del financiamiento del equipo de trabajo para posicionar la frase e imagen de Baldizón en redes sociales.

De manera indirecta Jimmy Morales durante el año 2017 fue acusado de ser parte de los políticos que utilizan estas herramientas como manipulación, pues se llegó a la conclusión

bajo una investigación de la Revista ContraPoder y Diario Digital que el net center destinado para Baldizón fue el mismo que ayudó a posicionar la campaña de Ni Corrupto, Ni Ladrón. La mecánica la misma, el fin el mismo, sin embargo el personaje era distinto.

Según Assardo (2016) el surgimiento de espacios de denuncias en las redes sociales como Twitter o Facebook en Guatemala fue a partir del caso Rosemberg. Desde ahí los políticos se han enfocado en desviar y manipular la opinión pública.

En febrero del 2011 publiqué un artículo sobre las porras virtuales que aparecían en temas relacionados a sus partidos. Eran centenares de perfiles falsos que aplaudían al político que apoyaban y lanzaban toda clase de insultos y ataques al contrario. En el espacio de comentarios se podía identificar la dirección IP desde donde venían los comentarios, así pude darme cuenta del intento de confundir al resto de lectores del medio (s.p).

El mismo autor considera que conforme el paso del tiempo cada gobierno en turno ha creado *webcenters* o *net centers* para administrar infinidades cuentas con el objetivo de aplaudir o atacar acciones políticas o sociales. También menciona que pueden ser los mismos personajes políticos que crean perfiles de su persona para crear espacios de doble lenguaje/doble discurso. "Eventualmente pueden desviar temas de conversación o *trending topics*".

En el texto "El complejo mediático-tecnológico- militar-industrial" de Justin Schlosberg (2017) describe como grupos de élites están concentrados en la red que a través de prácticas "bajo de agua" por medio de la tecnología puede ser capaces de sobre poner o sobre crear la agenda mediática. Es decir, algunos grupos de poder por un lado manejan un discurso limpio/ transparente ante la sociedad mientras por el otro están invirtiendo en colocar nuevos temas u opiniones de manera masiva y manipulante.

c) Delitos en el ciberespacio

Como se ha mencionado en ocasiones anteriores en sí no existe una ley o una norma eficiente para regular los ciberataques. Es algo difícil de controlar y más por su capacidad

global y virtual. En la página de la Oficina de Seguridad del Internauta explica que los ciudadanos españoles tienen derecho sobre la protección de datos personales, sin embargo la ley que resguarda la privacidad de las personas puede de que no aplique en sitios web que tienen una dirección IP de otro país.

"A pesar de los esfuerzos realizados dentro de la cooperación internacional, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias. Corresponde a los Estados nacionales la definición de lo que sea o deba considerarse como ilícito", explica Bravo (2003, 124).

Es decir, la regulación es por cada país, pero esto dificulta a que la red sea segura pues algunos sitios actúan bajo las leyes de su país de origen. Es tanta la extensión de la red que el descontrol es evidente. "El Internet es inexplicable y carece de significado (Silverstone, 2007)", citado por Sánchez (2012).

Por esta razón es necesario que las leyes sobre delitos se vayan enfocando en el ciberespacio, para que los actos ya mencionados sean condenados y puedan regularse bajo leyes específicamente en las acciones y comportamiento en el mundo virtual. En esta idea Trejo, Chimbo y Cisneros (2016, p. 81) mencionan varios delitos cibernéticos, tal es el caso de Suecia el 20 de junio de 2013 cuando condenó a Gottfrid Svartholm Warg, cofundador del portal The Pirate Bay por el delito de piratería informática, fraude e intento de fraude. En el 2010 se realizó un ataque a la empresa Lógica, encargada de almacenar datos de hacienda de varios clientes en ese país.

Por su parte la Organización de Naciones Unidas (ONU) y la OCDE han discutido en varios foros internacionales cómo el Diálogo Empresarial Global y el Diálogo Empresarial Transatlántico. Así como la Unión Europea (UE) ha generado medidas legislativas en el área de derecho de autor, privacidad, protección de datos, firma digital y comercio electrónico (Bravo, 2003).

La pornografía infantil, acoso virtual, fraudes monetarios son temas que tienen gran impacto dentro del cibercrimen. Estos delitos son el debate actual de varias naciones para

poder combatir los ataques cibernéticos, pues esto ha provocado que los usuarios virtuales sean aún más vulnerables, explica Bravo.

Mientras tanto, para Valladolid (2009) los delitos que se pueden llegar a cometer en el sistema informático es el almacenamiento de material ilícito: pornografía, medio para intentar acceder a espacios prohibidos, herramienta para practicar el ciberbullying y accesos para alterar o destruir datos, por último la utilización de proxys (servidor intermediario para realizar peticiones de seguridad, control y anonimato) que posibilitan la navegación anónima en Internet.

Para Téllez (1998, p.115) existen dos tipos de clasificación de delitos en el ciberespacio. En cuanto a los delitos según su instrumento o medio el autor menciona que se enfoca en la falsificación de documentos por medio de computadoras, alteración contable de los activos y pasivos de una empresa, planeación de delitos tradicionales como el homicidio, robo de tiempo de computadora, sustracción de información confidencial, implementación de códigos para entrar de manera indebida a sitios inapropiados, variación o desvío de dinero, creación de interrupciones en algunos programas para obtener grandes beneficios.

En cuanto a los delitos en la categoría como un fin u objetivo se encuentran la programación de instrucciones que producen un bloqueo total a sistema de ingreso, destrucción de programas por cualquier método, daño a la memoria, ataque directo a computadoras, sabotaje político o terrorismo y secuestros de soportes magnéticos (p. 116).

Trejo (2016), menciona que en Ecuador se ha trabajado junto con autoridades policíacas de Perú para mantener un línea de control y seguridad en ambos países, y de esta forma realizar una operación policial a través del uso de la tecnología y almacenamientos de una base de datos con la cual puedan registrar a los actores delictivos y el crimen que comenten. El 13 de Junio del año 2015 se lanzó un comunicado por parte de las autoridades de Ecuador para que se justificara la presencia de la policía peruana en el país. Así también comunicaron que los delitos que se iban a controlar en los dos territorios eran desde fraude hasta espionaje.

En el momento que se comente algún delito cibernético llega a afectar a gran parte de entidades que se encuentran tanto en el ciberespacio como en el espacio terrestre. Empezando por la vulnerabilidad de la humanidad, así como los gobiernos, corporaciones, las integridades económicas, la soberanía de las naciones, las industrias, entre otras (Téllez, 1998).

En la Comisión Internacional de los Derechos Humanos (CIDH) se establece la regulación y persecución de delitos cibernéticos como el acoso, pornografía infantil, ciberbullying, fraudes bancarios entre otros. Sin embargo, en Guatemala no existe una legislación fuerte o enfocada en estos tipos de temas.

Sí hay unidades dentro de la Policía Nacional Civil y el Ministerio Público sobre la pornografía, piratería y ciberbullying pero esta no es capaz de cubrir la gran cantidad de delitos que se llegan a cometer diariamente por medio del Internet. Existen iniciativas de ley presentadas por distintos grupos. Tal es el caso de la iniciativa 4055 y la reforma del artículo 274 literal D, del Código Penal, en la sección de registros prohibidos presentados al Congreso de la República.

En el caso de la iniciativa 4055 presentada en el 2009 (publicada en la página web del Congreso de la República) por la bancada Centro de Acción Social - CASA - representada por el diputado Francisco José Contreras Contreras. Esta contemplaba en sumar la Ley del Cibercrimen, la cual velaba regular de manera legal los ataques cibernéticos/informáticos. Actos como el *hacking*, *cracking*, *phishing*, *smishing*, *vishing* y pornografía infantil se toman como los nuevos delitos sancionados y regulados específicamente en el marco informático realizado dentro del territorio de Guatemala.

El partido TODOS presentó en enero de 2017 la reforma del artículo 274 literal D, del Código Penal, en la cual sancionará a toda persona que tengan de nombre una abreviatura o actúen de manera anónima con el objetivo de afectar la intimidad, privacidad, dignidad y honorabilidad de las personas ya sea para efectos ilícitos.

Estas dos acciones por parte del sector legislativo en Guatemala es el único acercamiento a formar parte de las naciones que están en contra de los actos ciberdelicuenciales e ilícitos. Sin mayor resolución en el pleno, pues se consideran algunos errores o cuestionamientos entre bancadas para ser aprobadas.

Otro punto a mencionar es la acción por parte de CSIRT - en español: equipo certificado de respuesta cibernética en tiempo real- esta agrupación cuenta con el apoyo de gobierno y fue en 1990 que se le otorga la Organización FIRST poder monitorear acciones en el ciberespacio. "En Centroamérica se cuenta con un equipo certificado de respuesta cibernética en tiempo real, con sede en Guatemala, y Latinoamérica registra un total de 18". "Cualquiera de los 289 miembros de la red es capaz de detectar y bloquear el evento o la IP dependiendo de la intensidad" (Siles, 2014, s.p).

Ejemplo a esto y sin ir tanto hacia la ciencia ficción, sino que se trata de acercarse a la realidad, en la línea económica de un Estado vale la pena mencionar la película Hacker: amenaza en la red, lanzada en el 2015 donde narra cómo un solo individuo está armado por un equipo de terroristas expertos en la red. Capaces de sabotear la bolsa de valores de China para elevar el precio de la soya y poder realizar millonarias transacciones de dinero y así obtener el control de las minas de uranio en ese país. Todo esto fue capaz de lograrlo por medio de direcciones IP's y proliferación de virus en las computadoras estatales de China.

1.3.3.4. Anonimato en el ciberespacio

El reto de la legislación reguladora del ciberespacio es el anonimato. Cualquier persona puede navegar de manera anónima sin dejar rastro o registro del sitio visitado. Esto provoca que exista mayor facilidad para efectuar crímenes en Internet sin que haya algo que lo evidencie.

El anonimato es algo normal en el ciberespacio y eso facilita esconder la verdadera identidad, en este sentido las leyes y normas sociales se les hace imposible que se apliquen en el espacio virtual (Lessig, 2014).

La navegación anónima consiste en la utilización de cadenas de proxys para que, en vez de realizar peticiones directas contra el servidor que visitemos, éstas pasen por distintos servidores pertenecientes a instituciones que han declarado públicamente que no guardan logs relacionados con la privacidad del usuario, define Valladolid (2009, p. 6).

Por otro lado, la navegación anónima puede ser de gran beneficio en cuestiones de seguridad para quienes se dedican a investigar casos de alto impacto del cibercrimen o para periodistas que pueden ser perseguidos por la información relevante que pueden llegar a publicar en determinado medio o de forma independiente. Es decir, el anonimato en Internet también puede ser utilizado con un buen fin.

La utilización de contraseñas seguras, sitios web seguros, navegación anónima y correos encriptados pueden llegar a ser de gran utilidad para velar la seguridad de la identidad personal y virtual. Siempre y cuando no se atraviere la línea de abuso de poder para generar terror en la red, cuenta como una estrategia para salvaguardar vidas. Assardo menciona en su texto Seguridad Digital, algunas herramientas de encriptación: "www.hushmail.com: encripta mensajes electrónicos, Mozilla Thunderbird: servicio de seguridad electrónica, GnuPG: Versión de código abierto de Pretty Good Privacy (PGP), por último, www.truecrypt.org: encripta drives completos" (s.f., p. 33).

La herramienta más utilizada y más conocida hasta el momento para poder navegar anónimamente es The Onion Router (Tor), este sitio ofrece proxys o diferentes nodos donde pasan los datos, esto provoca que la navegación sea lenta pero garantiza mayor seguridad en cuanto a la identidad virtual se refiere. Como todo en esta vida nada es perfecto, Tor tampoco lo es pero su objetivo principal es garantizar navegación anónima, sin embargo, igual se corren riesgos de que no se utilice correctamente y logren un rastreo (Flores, 2014). Este mismo autor utiliza un esquema para explicar el proceso del tráfico de datos cuando se navega por medio de Tor (p. 2):

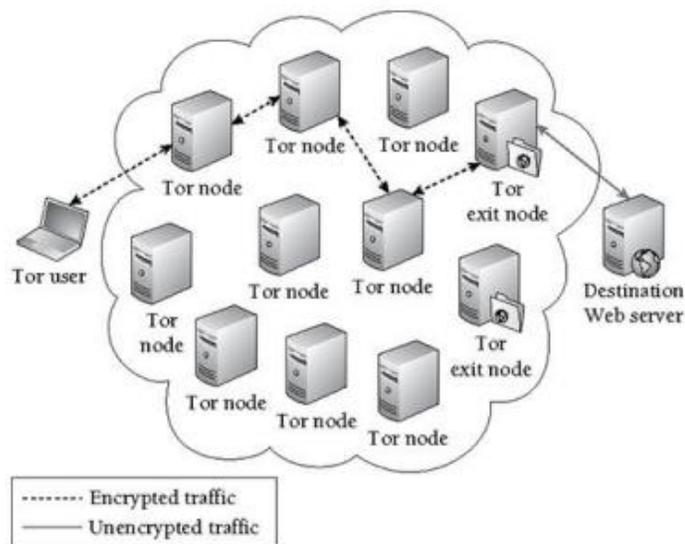


Figura 3.1.0 Trafico de Datos

Chatfield (2011) presenta una web profunda, es decir que "una buena parte del mundo digital yace bajo una superficie", (p. 99). Esta superficie está oculta, una parte de la red no es visible para los usuarios informales en la web, sino aquel que sea experto en asuntos informáticos. Como se menciona, existe una parte oscura de la web, por ende existen redes sociales oscuras y en estas se almacenan grupos privados u ocultos que comparten información, comunicación y archivos fuera del alcance de los usuarios comunes y corrientes. También menciona que existen programas especiales para navegar de manera oculta y que no requieren del acceso a la Worl Wide Web. WASTE, uno de ellos.

1.3.3.5. Censura en Internet

La censura es un tema de discusión en los grupos de poder, siendo esta una estrategia para combatir publicaciones no favorables para ellos y así fortalecer el control de cierta forma de los mensajes difundidos por pequeños grupos sociales, medios de comunicación entre otros. Sin embargo, la garantía del derecho a la Libertad de expresión se ve afectada por este tipo de actos, es en este sentido que algunos países no pueden procesar con mayor libertad la aplicación de la censura.

Ahora con el ciberespacio la censura de contenidos tiene dificultad en su desarrollo por las características virtuales y globales de la red. A pesar de ello, no evita que exista, con mayor esfuerzo y presión logran censurar usuarios virtuales, sitios web, etc. Este es el caso de

Estados Unidos y su lucha legislativa para aplicar la censura en algunos espacios virtuales que causan ruido para algunos sectores de poder en ese país. Discusiones extensas en el Congreso sobre censurar algún sitio o usuario en la red han sido constantes, comenta Johnson (1996). También explica:

La ley sobre libre expresión electrónica está evolucionando. Algunos tribunales de primera instancia han señalado que los esfuerzos de censura por parte del Congreso violan la Primera Enmienda (la garantía de «libertad de expresión»). Los ciudadanos de los EE.UU. aún pueden ayudar a modelar la política de la Internet, pero no por mucho tiempo (párr. 2).

Castells (2001) en su texto cita a John Gilmore donde afirma que es difícil que la censura se lleve a cabo en la red, pues no hay fronteras que detengan la información que se almacena. Por lo que Castells indica que la única manera de que exista censura es no estar presentes en la red. Negar el acceso al Internet. Así también explica que la censura no puede existir en su totalidad en Internet por la protección a la libertad de expresión bajo el derecho que concierne. Sin embargo, existen censores que desconectan servidores de acceso a la red, penalizan a los administradores o rastrean algún mensaje no permitido, esto se refleja en China, Malasia y Singapur. Este tipo de legislación pretende aplicar en Europa.

1.3.3.6. Contenidos virales

Otra característica del ciberespacio es la capacidad de viralización de contenidos, la capacidad de que una imagen, video o información publicada en cualquier sitio web o red social puede llegar a diferentes nodos en cuestión de segundos y expandirse a través de la distribución de contenido.

Un virus es una forma primitiva de vida capaz de producir cantidades enormes de copias de sí mismo en poco tiempo; algo que lo ha convertido en la metáfora perfecta de la manera en que las ideas, las palabras, los sonidos y las imágenes se pueden reproducir en el mundo digital, explica Chatfield (2012, p. 172).

Para Ramos- Serrano (2007) la utilización de los nuevos medios tecnológicos provoca que existan nuevas formas de comunicación que principalmente han favorecido a la publicidad, basándose en una construcción de comunicación viral. Este tipo de comunicación se trata de elaborar de manera creativa contenidos que enganchen al usuario. Su objetivo principal es que se expanda por medio del público objetivo.

A esto concuerda Chatfield (2011, p. 172- 178) pues para él la viralidad es utilizado en el ámbito del marketing para reforzar su posición y ventajas en la mente de los usuarios por medio de la red. Sin embargo, este método puede ser “arma de doble filo”, ya que si el mensaje no es satisfactorio para los cibernautas puede llegar a ser motivo de burla y rechazo, lo que provoca otro tipo de viralización. Bajo esta idea, diseña la siguiente cronología:

Cronología	
1976	<i>Richard Dawkins</i> acuña la idea de los memes
1982	Uso del primer emoticono
1996	Aparición de los primeros memes en la red
2004	Se acuña el término de marketing viral <<usuarios alfa>>

1.3.4. Plataformas de Redes Sociales amenazadas por el cibercrimen

Como complemento para este estudio se definirán algunas plataformas de redes sociales en las cuales se considera que son las más utilizadas para fines comunicacionales, aparte de entretenimiento y ocio. En estas principales redes sociales se han reflejado desde

contenidos virales hasta almacenamiento de información de interés social, así como amenazas de malversación de información a través del sicariato digital.

Como se ha mencionado anteriormente las redes sociales son una enorme fuente de información. Así como conectores que pueden llevar a los usuarios a navegar en otros sitios web. La información que se obtiene por medio de estas plataformas es ilimitada, tanto que existen casos que no es manejada de una manera adecuada pues no se tienen políticas fuertes que regulen movimientos sospechosos o mal intencionados como los perfiles falsos o el crimen dentro de las redes sociales.

Una pequeña cronología del surgimiento de las plataformas de redes sociales durante la historia del siglo XXI, desde el año 2003 hasta el año 2006:

AÑO	PLATAF.	FUNDADOR/ES	PAÍS	ENFOQUE	USUARIOS
2003	My Space	Chris De Wolfe y Tom Anderson. Propietario actual: News Corp. (Fox Interactive Media)	EEUU	Generalista	+ 178 millones Mayo 2007
2003	Hi5	Ramu Yalamanchi, fundador y director general (Sona Networks)	EEUU	Profesional	Sin datos
2003	eConozco	Grupo Galenicom TI. S.L. (Propietario actual: Xing, antigua Open BC, que aglutina a Neurona)	ESPAÑA	Temática-profesional	6,5 millones Diciembre 2008
2003	Second Life	Linden Research Corp. (Relevancia en 2006)	EEUU	Mundo virtual	+ 13 millones Usuarios Marzo 2008
2004	Facebook	Mark Zuckerberg, Marc Andreessen, Chris Hughes, Don Graham	EEUU	Generalista	Sin datos
2004	Orkut	Google Corp.	EEUU	Generalista	Sin datos
2004	Flickr	Caterina Fake y Stewart Butterfield (en marzo de 2005, fue adquirida por Yahoo!)	EEUU	Generalista (Red y Plataforma de Fotografías)	Sin datos
2005	You Tube	Chad Hurley y Steve Chen (de Pay Pal, empresa de micropagos eBay) En 2006, adquirida por Google	EEUU	Generalista (Plataforma de videos)	Sin datos
2004	LinkedIn	Reid Hoffman	EEUU	Profesional	+ 30 millones profesionales
2005	Ning	Marc Andreessen y Gina Bianchini	EEUU	Profesional	Sin datos
2006	Tuenti	Zaryn Dentzel, director general	ESPAÑA	Generalista (estudiantes, universitarios)	+ 3 Mlns. Marzo 2008
2006	Twitter	Jack Dorsey y Evan Williams de Biz Stone (negocia su compra)	EEUU	Generalista (Plataforma de Microblogging)	Sin datos

Plataforma y cronología de las redes sociales

Esquema presentado por Flores (2009, p. 76)

Sin embargo los datos otorgados por el sitio web *Internet World Stats* <http://www.internetworldstats.com>, describe a través de una tabla la tasa de penetración de

internet a nivel mundial, siendo 7.519.028.970 el total de población en el mundo, manifiesta una penetración del 49,7% de internet, registrado el 31 de marzo 2017. A nivel continental Asia se lleva el 50.1% de usuarios de Internet, segundo lugar Europa (17,0%) y tercer lugar América Latina/ Caribe (10,3%).

ESTADÍSTICAS DE USO DEL INTERNET
El Internet Big Picture
Usuarios de Internet del mundo y Estadísticas de Población 2017

ESTADÍSTICAS MUNDIALES DE UTILIZACIÓN DE INTERNET Y POBLACIÓN						
31 DE MARZO DE 2017 - Actualización						
Regiones del mundo	Población (2017 Est.)	Población % del mundo	Usuarios de Internet 31 Mar 2017	Tasa de Penetración (% Pop.)	Crecimiento 2000-2017	Usuarios de Internet %
África	1.246.504.865	16,6%	353.121.578	28,3%	7.722,1%	9,4%
Asia	4.148.177.672	55,2%	1.874.136.654	45,2%	1.539,6%	50,1%
Europa	822.710.362	10,9%	636.971.824	77,4%	506,1%	17,0%
América Latina / Caribe	647.604.645	8,6%	385.919.382	59,6%	2.035,8%	10,3%
medio Este	250.327.574	3,3%	141.931.765	56,7%	4.220,9%	3,8%
Norteamérica	363.224.006	4,8%	320.068.243	88,1%	196,1%	8,6%
Oceanía / Australia	40.479.846	0,5%	27.549.054	68,1%	261,5%	0,7%
TOTAL DEL MUNDO	7.519.028.970	100,0%	3.739.698.500	49,7%	936,0%	100,0%

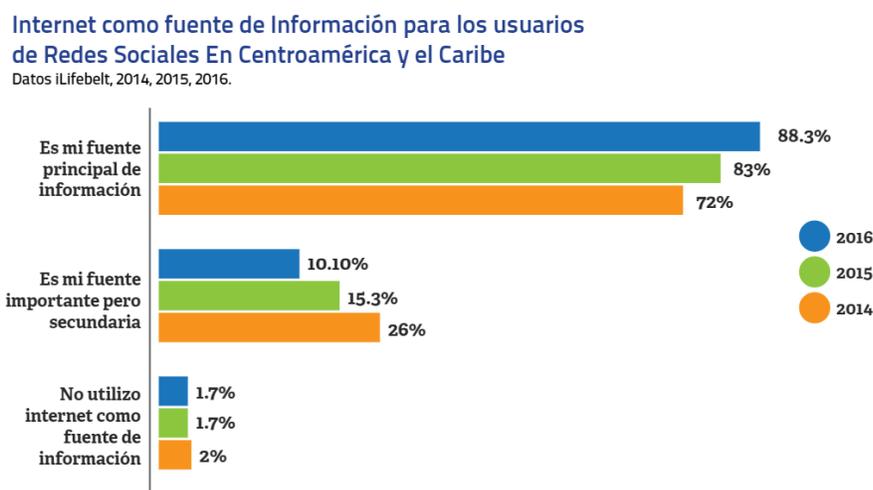
Esquema presentado por *Internet World Stats* (2017)

Si se observan los datos a nivel Centroamérica y el Caribe existe mayor penetración en Costa Rica con un 86,9% poblacional, sin embargo el país que cuenta con más usuarios en Internet (5,300,000) y usuarios registrados en Facebook (5,300,000) es Guatemala.

Estadísticas de Uso y Población en América Central						
CENTROAMÉRICA	Población (2016 Est.)	% Pop. California	Uso de Internet, 30-jun-2016	% Población (Penetración)	% Tabla de Usuarios	Facebook 30-Junio-2016
Belice	353.858	0,2%	165.014	46,6%	0,2%	160.000
Costa Rica	4.872.543	2,9%	4.236.443	86,9%	4,7%	2.900.000
El Salvador	6.156.670	3,7%	3.100.000	50,4%	3,5%	3.100.000
Guatemala	15.189.958	9,0%	5.300.000	34,9%	5,9%	5.300.000
Honduras	8.893.259	5,3%	2.700.000	30,4%	3,0%	2.700.000
Méjico	123.166.749	73,2%	69.000.000	56,0%	77,4%	69.000.000
Nicaragua	5.966.798	3,5%	1.900.000	31,8%	2,1%	1.900.000
Panamá	3.705.246	2,2%	2.799.892	75,6%	3,1%	1.700.000
TOTAL AM. CENTRAL.	168.305.081	100,0%	89.201.349	53,0%	100,0%	86.760.000

Esquema presentado por *Internet World Stats* (2017)

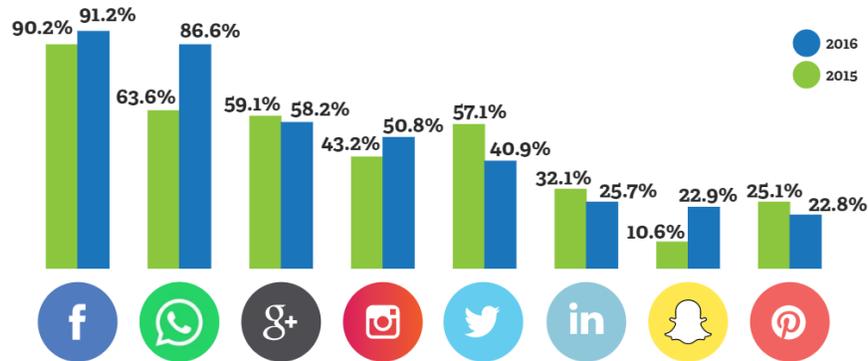
En cuanto a las redes sociales *iLifeBelt*, una firma que se dedica a la innovación para la publicidad en Guatemala, ha hecho distintos estudios sobre las tendencias, usos y funciones de las redes sociales. Recientemente presentó un informe del 6to Estudio de redes sociales en Centroamérica y el Caribe 2016, dirigido por Jose Kont, en el cual enlista datos actuales sobre el uso que le dan los usuarios a las redes sociales:



Esquema presentado por *iLifeBelt* (2016, p. 14)

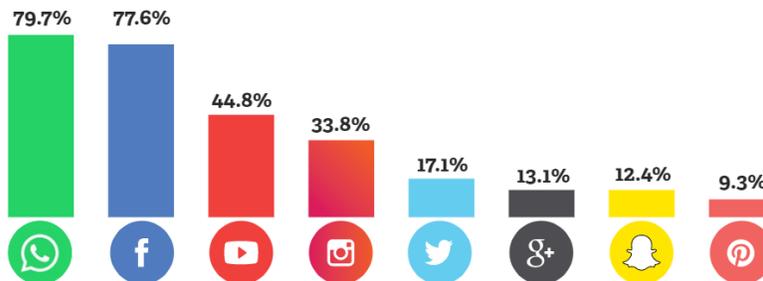
También presenta cuales son las redes sociales con más usuarios en los años 2015 y 2016:

Redes Sociales con mayor cantidad de usuarios en Centroamérica y el Caribe 2015 vs. 2016
 Datos iLifebelt Junio 2016



Así como las redes favoritas de los usuarios a nivel Centroamérica y el Caribe:

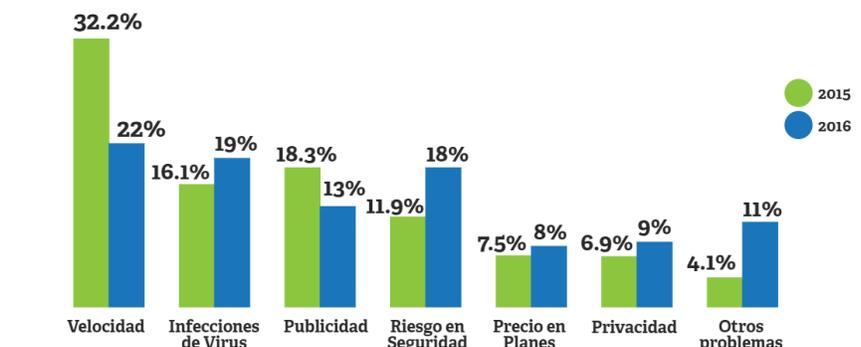
Redes Sociales favoritas de los usuarios de Internet en Centroamérica y el Caribe
 Datos iLifebelt Junio 2016



Por esta razón *iLifeBelt* (2016) explica que por la misma facilidad que existe hoy en día para tener acceso a la información, los usuarios están más conscientes que al estar en contacto dentro de la red se corren distintos riesgos o problemas que pueden afectar tanto la integridad de la persona como el equipo que se utiliza para estar en contacto.

Principales dificultades reportadas por los usuarios de Redes Sociales en Centroamérica y el Caribe
 Datos iLifebelt Junio 2016

Es evidente que cada día hay más conciencia en relación a los riesgos que vienen acompañados de la red (phishing o suplantación de identidad, fraude informático, hacking antiético o lesivo, entre otros).



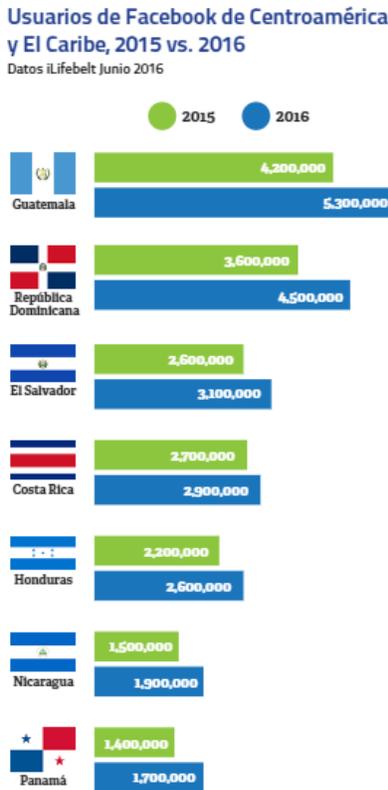
a) Facebook

En el caso de Facebook hay que tomar en cuenta el origen de esta pues nace con el objetivo de establecer una red virtual dentro de la Universidad de Harvard y luego se transforma en una red universitaria. En el prólogo escrito por Stephen Downes (2010) del libro *El Proyecto Facebook y la posuniversidad: Sistemas operativos sociales y entornos abiertos de aprendizaje*, explica que el creador de Facebook, Mark Zuckerberg estableció a la plataforma en el año 2004 como un espacio de conexión entre estudiantes universitarios pero su éxito dio luz verde para que estuviera disponible a toda persona que tuviera una cuenta de correo electrónico en el 2006. Desde entonces su crecimiento alcanzó que se lanzara en diferentes idiomas en el año 2008 y al siguiente año alcanzó 200 millones de usuarios (Ponce, 2012).

En el 2012 Facebook no solo es la red más famosa del mundo, sino que la encargada de interconectar a distintas partes del mundo. Esta plataforma funciona para crear una lista de amigos interminables, formados por afinidad e intereses personales o colectivos. Igarza (2010; 71) muestra la distribución de usuarios en Facebook de los países mayoritarios en estar conectados a la plataforma. El autor menciona que no son datos oficiales, sin embargo estiman una idea sobre la preferencia de su uso:

Posición	País	Usuarios de FB ¹⁰	Población TOTAL ¹¹	% de usuarios de FB sobre población TOTAL
1.	Estados Unidos	143.583.400	311.733.000	46%
2.	Indonesia	30.108.220	244.291.000	12%
3.	Reino Unido	28.413.560	62.523.000	45%
4.	Turquía	23.313.440	78.295.000	30%
5.	Francia	19.755.460	64.936.000	30%
6.	Filipinas	18.124.220	100.867.000	18%
7.	Italia	17.309.580	58.065.000	30%
8.	Canadá	17.207.140	33.896.000	51%
9.	México	16.975.220	113.097.000	15%
10.	India	15.402.180	1.181.141.000	1%
11.	Alemania	12.741.220	82.256.000	15%
12.	Argentina	11.825.140	41.557.000	28%
n.	Colombia	11.323.900	44.466.000	25%
n.	Brasil	7.346.980	202.267.000	4%
n.	Chile	7.386.280	16.818.000	44%

Para *iLifeBelt* (2016) Centroamérica contabiliza 22 millones de usuarios en Facebook, los cuales se distribuyen de la siguiente manera:



Cuestiones como el estado civil, las preferencias sexuales, la edad, el lugar de residencia, las creencias religiosas y políticas, las preferencias de ocio, el tipo de estudios, el lugar de trabajo, el currículum profesional, el correo electrónico son contestadas por los usuarios a la hora de crear un perfil dentro de redes sociales como Facebook o similares, afirma Caldevilla (2009; 40).

Estos datos personales pueden ser almacenados en:

- Perfil personal: Fernández (2011) cita a Romina Cachia (2008) que describe a un perfil como: Es la plataforma básica de entrada a cualquier red social. Cada usuario se presenta a sí mismo a través de una serie de datos personales o profesionales, o añadiendo fotografías, música o videos. Este contenido creado

por los usuarios está vinculado a sus propios intereses y a su vida personal (p. 24).

- Grupo: dentro de la plataforma se pueden crear comunidades por algún motivo laboral, educativo, interés particular o afinidad a determinado tema. Puede ser un grupo privado o público y su principal objetivo de construir un espacio donde se puedan compartir información, imágenes, vídeos, etc. de manera más personalizada. Este puede ser un espacio con objetivos de aprendizaje integral de forma digital.
- Página oficial: "Las empresas lo ven como una posibilidad de hacer llegar sus negocios a una cantidad importante de la población, por ello crean sus propias páginas donde mostrarán parte de sus productos, ofreciendo ventajas a aquellos usuarios amigos" (Fernández, 2011, p. 39).

En cuestiones de privacidad Facebook fue la primera en implementar una política de privacidad (Fernández, 2011). Exigir el uso de un nombre real y elegir que datos hacerlos públicos o visibles solamente para el círculo de amigos que se tiene en la lista del perfil personal.

Según los principios de Facebook almacenados en su página www.facebook.com, dictan puntos sobre la dinámica de la red social. Libertad para compartir y conectarse, propiedad y control de la información, flujo libre información, igualdad fundamental, valor social, plataformas y estándares abiertos, servicio fundamental (gratuito), bienestar común, proceso transparente, un mundo (conectar al mundo).

Sin embargo, Fernández (2011) analiza que la plataforma tiene tantos usuarios que esos principios han quedado obsoletos, pues no se actúa de manera transparente, ni se controla la información almacenada en la red como lo dictan en sus principios. Se sabe que han experimentado nuevas funciones por medio de algunos perfiles sin consultarles a los usuarios.

Otra problemática que enfrenta Facebook hoy en día provocada por la misma saturación de usuarios es la el descontrol de la privacidad como de alteraciones de perfiles sospechosos creados con el objetivo de implementar cierto crimen u otros actos alineados a un enfoque criminal malversando la información adquirida por la red social.

En este sentido en términos y condiciones de Facebook dicta que no se responsabiliza por la información brindada en cuanto al total control sobre ella, ni tampoco que esa información sea víctima de actos de amenazas informáticas. Por más que ellos como corporación informática tengan resguardada toda la información del usuario en cualquier momento pueden ser el blanco de trol, *spam* o sicariato digital (Fernández, 2011).

b) Twitter

Según Caldevilla (2009) Twitter tiene la característica de ser un sistema de microblogging donde se puede realizar una lectura rápida y estar básicamente informado sobre alguien o algún suceso. Se dice que es la revolución del periodismo por su línea de inmediatez y breve en dar una noticia. Ha sido de gran ayuda para la realización de foros o congresos, presentaciones mundiales, eventos sociales, encuentros deportivos entre otros acontecimientos.

"Las redes de microblogging se basan en una actualización constante de los perfiles a través de unos mensajes de texto que no pueden superar los 160 caracteres", explica Fernández (2011; 27).

Por medio de 140 caracteres (tweet/tuit) permisivos para escribir en esta plataforma es importante resaltar que llega a generar movimientos globales muy dinámicos y no es limitante para generar mayor impacto. Este al contrario de Facebook, no tiene tantos espacios de interacción más que un chat y una línea de tiempo interminable donde va corriendo cada tweet publicado por las personas que participan en la red.

Twitter fue lanzado en 2006 por Jack Dorsey, Noah Glass, Biz Stone y Evan Williams, dándole un sentido más conversacional. Según E. García, L. Yezers'ka, A. Rost, M. Calderín, C. Edo, M. Rojano, E. Said, P. Jerónimo, C. Arcila, A. Serrano, J. Sánchez y L. Corredoira (2011, p. 618) en Facebook se puede consultar información personal o grupal,

imágenes, vídeos, eventos, etc, mientras que en Twitter se interactúa con rapidez y crea comunidades al instante. La utilización de hashtags (#) encierra el "modus operandi" de la plataforma. De esta manera se forman las tendencias sobre varios temas. La palabra favorita de Twitter es última hora y cuenta con la capacidad de transformar a los usuarios en testigos de algún hecho.

En el artículo "Twitter, del sondeo a la sonda: nuevos canales de opinión, nuevos métodos de análisis", escrito por Congosto y Aragón (2012) mencionan algunas reacciones de interacción que se pueden realizar en esta plataforma y explican que los "tweets" (texto de 140 caracteres) son:

Pequeñas piezas de información que pueden contener además del texto una serie de componentes que enriquecen el contenido como etiquetas (#hashtags) para enfatizar el contenido del mensaje y hacer que se propague mejor por la Red, marcas que determinan que el mensaje no es original sino una retransmisión (RT, Via), menciones específicas a otros usuarios de Twitter (@usuario) y enlaces a sitios Web que amplían el contenido del mensaje. Todos estos componentes debidamente analizados en su conjunto pueden proporcionar información sobre qué tipo de actividad se está produciendo en las campañas electorales, qué lemas son los que más se están usando, qué mensajes se están difundiendo, qué candidatos o partidos están captando la atención de los ciudadanos, qué medios de comunicación o blogs están siendo más citados y qué tipo de relaciones existen entre los usuarios que están interactuando (2012 p. 51).

En el 2011 Twitter ya tenía más de 200 millones de cuentas de usuarios, no cabe duda que esta red social representa una revolución para el internet pues gracias a los smartphones y los dispositivos móviles las personas se mantiene informadas y conectadas la mayor parte de su tiempo diario (Chatfield, 2011).

En este caso el usuario se convierte en seguidor y en vez de amigos tiene seguidores, al mismo tiempo puede ser seguidor de sus seguidores. En esta línea se van formando las comunidades seguidas por afinidad o algún interés. "También permiten seguir a otros

usuarios, aunque esto no establece necesariamente una relación recíproca, como los seguidores o followers de los famosos en Twitter", expresa Ponce (2012, p. 4).

En cuanto al manejo de privacidad y seguridad en Twitter a comparación de Facebook no tiene políticas para vigilar por completo la información almacenada en su web social. Dentro de sus reglas y condiciones se refleja el principal objetivo de hacer ejercer la libertad de expresión y por consiguiente no puede actuar sobre los tuits publicados porque violaría su principio de existir.

Sin embargo, plantea excepciones que efectuaría su acción hacia todo usuario que realice lo siguiente:

La suplantación de identidad, las condiciones específicas del uso de una marca comercial, la publicación de información privada de otra persona sin su consentimiento, la publicación de amenazas de violencia, la violación de los derechos del autor, el uso de la plataforma para un fin ilegal y el uso indebido de insignias de Twitter, Cano (s.f, p. 492) cita el documento de legalidad de Twitter publicado en www.twitter.com.

Así también menciona la utilización de medios Spam, el cual lo define como la creación de cuentas en serie con finalidad abusiva o perjudicial, el abuso y acoso dirigido a una persona, la apropiación de nombres y la venta de nombres de usuario, la suplantación de identidad, etc.

Por último, Twitter desde el año 2012 realiza informes de transparencia para dar a conocer que instituciones autorizadas por cada gobierno del mundo han solicitado información, desaparición o eliminación de usuarios. Cada vez más ha aumentado la censura de tuits (Cano, s.f).

Al conocer la legalidad y políticas de cada red social es evidente que el cumplimiento no es del todo satisfactorio, pues últimamente dentro del círculo de amigos en ambas redes sociales existen personas que tienen más de dos perfiles o usuarios, en el caso de actores políticos, actores públicos o artistas se han visto usuarios falsos o con la misma identidad.

Así como movimientos virtuales malintencionados o violentos. Publicaciones de contenido pornográfico, acosador y aterrador. Un desafío por trabajar en el mundo digital.

II. Planteamiento

La transformación de la comunicación a través del avance tecnológico cada vez es más evidente, pues con el uso de las redes sociales construidas dentro del Internet provoca que los flujos comunicacionales sean inmediatos, interactivos, multidireccionales y globales. Esto puede ser de gran ayuda para distintos grupos de poder.

El estudio de Barry Wellman, de la Universidad de Toronto describe la realidad de la vida social en Internet y explica que también se forman comunidades pero en vez de que sean físicas, son de manera virtual. Son comunidades basadas en intereses individuales y en las afinidades de cada uno de sus miembros (Castells, 2001). En la actualidad el mundo de las redes sociales o comunidades virtuales ha ido incrementando, así como la conectividad y acceso a estas.

Cualquier persona puede ser proveedor de contenido y si la información brindada es de interés o afín de una o varias personas puede llegar a viralizarse por medio del ciberespacio (alcances globales). Herramientas como Facebook, Twitter o un blog en Internet existen para poder almacenar comunidades virtuales y con esto crear una interacción simultánea en tiempo real.

Las redes sociales, se han convertido en un instrumento esencial para transmitir mensajes con mayor fluidez, rapidez e impacto. Según Castells la comunicación en las redes tiene dos caminos: el despertar social o la represión/persuasión social. Asimismo se obtiene poder con las comunidades virtuales pues se emplea bajo distintas condiciones.

La existencia del anonimato en Internet puede ser de gran provecho para darle una utilidad en algunos casos políticos, en otros sociales y por último, económicos. Crear movimientos sociales, una campaña negra, un crimen de manera anónima son algunas cualidades de la elaboración de los denominados perfiles sospechosos, dentro de las redes sociales. En otras palabras: un perfil falso o "bot". Perfiles falsos sobre una identidad o figuras ya existentes.

El juego de este tipo de perfiles tiene dos vertientes, estar a favor o en contra de algo o de alguien. De esta forma, también se puede llegar a obtener poder sobre la imagen o identidad de una persona.

En el contexto reciente de la política guatemalteca, los perfiles falsos han formado parte importante de la opinión pública sobre la imagen de una figura política. De esa cuenta, entre el año 2015 hasta de lo que va del año 2017, se ha observado un aumento en el manejo de redes sociales, tanto por los ciudadanos como las figuras políticas que han decidido transportar sus tácticas tradicionales de persuasión a la red virtual. Sin embargo, dentro de tanto manejo de contenido existe la impresión que fomenta el uso de perfiles falsos capaces de crear interacción y efecto en las personas.

Por esta razón, en la presente investigación se plantea la siguiente pregunta:

¿Cuál es el uso de perfiles falsos de figuras políticas en Guatemala durante los años 2015-2017?

2.1. Objetivo

Objetivo General

Analizar el uso de perfiles falsos de figuras políticas en Guatemala a través de la red social Twitter durante los años 2015 - 2017.

Objetivos Específicos

- Identificar los usos de perfiles falsos de los personajes políticos en Guatemala.
- Categorizar los mensajes transmitidos por medio de perfiles falsos de personajes políticos de Guatemala durante el año 2015 al 2017
- Identificar las dinámicas de comunicación e interacción que generan la utilidad de perfiles falsos.

2.2. Variables o Unidades de análisis

a) Perfiles Falsos

Definición Conceptual

Temperini y Macedo (2015) los perfiles falsos en las redes sociales son aquellos que no cumplen con los términos y condiciones que establece la plataforma, no pertenecen a personas reales, no pertenecen a la persona que indican, y, se hacen pasar por perfiles reales existentes. También indican que existen perfiles falsos, manuales o artesanales (creados por personas) y los que son generados y manipulados de forma manual y automatizada (bots o robots). Mencionan que existen diferentes tipos de "tareas" de un perfil falso: *stalker*, ciberbullying, *gamers*, *spammers*, pornografía, reputación digital, manipulación mediática, cibercrimen.

Definición Operacional

Para fines de esta investigación se entiende como perfil falso a todo usuario que utilice la identidad digital de figura política guatemalteca con el fin de usurpar, manipular y generar una nueva reputación digital, entiéndase, creados para crear contenido político y argumentos sobre el personaje a través de memes, vídeos, "hashtags", tuits y otros elementos, publicados en Twitter.

b) Figuras Políticas

Definición Conceptual

De Gracia (2013, p. 3) expone en el Foro Derecho a la Privacidad vs. Derecho a Información de Organizaciones Políticas y Candidatos que para la Suprema Corte de Justicia en México:

“las personas públicas o notoriamente conocidas son aquellas que, por circunstancias sociales, familiares, artísticas, deportivas, o bien, porque han difundido hechos y acontecimientos de su vida privada, o cualquier otra situación

análoga, tienen proyección o notoriedad en una comunidad y, por ende, se someten voluntariamente al riesgo de que sus actividades o su vida privada sean objeto de mayor difusión.

Mientras que Elizondo (s.f) expresa que toda persona políticamente expuesta es aquella que ejerce un puesto o actividad administrativa desde los tres poderes del estado – legislativo, ejecutivo y judicial- también como las labores autónomas y desconcentradas del gobierno. Incluyendo los líderes políticos y líderes de movimientos sociales suelen estar dentro de la esfera pública. Para finalizar, la misma autora describe que los familiares y parte del entorno de la figura pública llegan a formar parte del acceso público/social.

Para finalizar, según el Diccionario de Ciencias Jurídicas, Políticas y Sociales, escrito por Manuel Ossorio (s.f) es la persona que desarrolla una función o servicio público ya sea como empleado público o como funcionario público. En cuanto al funcionario público recibe una retribución administrativa (ministro, alcalde, jueces, presidente, legisladores y vicepresidente).

Definición Operacional

Para fines de esta investigación se entiende como figura política aquel ente relevante en los años 2015 al 2017 siendo funcionario público activo o inactivo dentro del período antes mencionado. Cubriendo los tres poderes del Estado: legislativo, ejecutivo y judicial. En este sentido, también se tomó en cuenta a candidatos políticos que surgieron en período de elecciones del año 2015. Así como alcaldes relevantes en las redes sociales.

2.3. Alcances y Límites

Esta investigación se centra en las nuevas dinámicas que se han generado en las redes sociales como la creación de perfiles falsos para influenciar y generar efectos en la opinión pública sobre la imagen de los personajes políticos de Guatemala. En el caso de esta investigación se efectuará el análisis en la plataforma Twitter, pues se considera que en la misma es posible una mayor accesibilidad a dichos perfiles y al mismo tiempo las condiciones de privacidad no son tan restringidas, a diferencia de otras redes sociales. Al

mismo tiempo se hará una muestra de perfiles falsos de los personajes políticos que serán considerados en esta investigación, para tener mayor enriquecimiento en los resultados. Por límites de tiempo solo se analizarán las reacciones de interacción generadas por las publicaciones dentro de los perfiles, categorizando los mensajes de manera general de cada perfil.

2.4. Aporte

Para la comunicación política es importante este tipo de estudios pues de esta manera se puede llegar a entender las nuevas dinámicas que se han estado generando conforme la utilización de las redes sociales y como esto puede llegar a modificar la percepción a través de la construcción de comunidades virtuales enfocadas a la política.

Para los asesores y promotores de campañas políticas es importante saber que no solo el personaje político puede ser gran influenciador en la sociedad por medio de las redes sociales, sino que existen grupos o personajes anónimos que actúan bajo la identidad de una misma figura política para generar otro tipo de percepción. Esto puede llegar a alcanzar resultados no deseados para todo político que desea posicionarse en la afinidad de los ciudadanos.

Este estudio aporta conocimientos nuevos sobre la ciberdemocracia, que actores políticos se manejan dentro de redes sociales, que elementos o herramientas se utilizan en las redes sociales y qué papel juegan las redes sociales dentro de la opinión pública o percepción de las personas. Por otro lado, el estudio pretende mostrar el otro "lado de la moneda" ya que solo se ha estudiado las dinámicas de campañas electorales y políticas efectuadas en Internet y no como estas pueden llegar a ser afectadas por actores anónimos. En otras palabras, creación de "campañas negras" en redes sociales.

Por último, para futuros estudios en materia de comunicación política, será una referencia sobre las nuevas dinámicas que se manejan a través de redes sociales sobre las figuras políticas. Para los y las estudiantes de la Universidad Rafael Landívar servirá como una herramienta con la que se puede ayudar y así brindar al desarrollo político, social y económico de Guatemala.

III. Método

3.1. Sujetos de estudio

Según Hernández, Fernández y Baptista (2010) la selección de la muestra en el estudio es a qué o quiénes se realizarán la evaluación para la recolección de datos. Estas unidades pueden ser sujetos, objetos, sucesos o contextos. En este sentido para fines de esta investigación se plantea como sujeto de estudio a todo perfil falso en Twitter que tenga relación o vinculación con personajes políticos guatemaltecos o referentes a casos políticos en Guatemala, con su debida relevancia en los años 2015 al 2017.

Se escogió la red social Twitter por su sistema de privacidad, ya que cuenta con la facilidad de acceder a dichos perfiles por medio de la opción de búsqueda de usuarios en la red. En cuanto a los personajes políticos, serán hombres y mujeres que estén o estuvieron en un cargo en el gobierno y han sido relevantes dentro del rango de años 2015-2017, tales como:

- Presidente Jimmy Morales, presidente actual y fue relevante durante la campaña 2015 como candidato a la presidencia.
- Álvaro Arzú y su esposa Patricia de Arzú, Neto Bran, Edwin Escobar los tres alcaldes con más afinidad y participación en redes sociales.
- Juan Manuel Giordano, diputado del Congreso de la República de Guatemala 2016-2020 que ha tenido mayor controversia y participación legislativa, así como interacción en redes sociales.
- Iván Velásquez, personaje icono desde el año 2015 hasta la fecha por su labor sobre la justicia y persecución en contra de la corrupción en el país.
- Sandra Torres, Zury Ríos, Manuel Baldizón, candidatos presidenciales posicionados en los cinco primeros lugares en las elecciones del año 2015 y siendo también los más activos en las redes sociales para dar a conocer sus propuestas de gobierno
- Otto Pérez Molina, Roxana Baldetti, ex funcionarios implicados en asuntos de corrupción en la administración 2012- 2015. Por ende, fueron enfoque principal en distintos discursos de las redes sociales.

En cuanto a los sujetos entrevistados, se contó con la participación de expertos en el tema, así como la experiencia de un "netcentero" y un candidato a alcalde en el 2015.

María Mercedes Zaghi, especialista en seguridad informática, consultora de diferentes proyectos relacionados con la innovación e implementación de la TIC's en los negocios por más de 25 años, así como su aporte hacia la agenda digital de Guatemala para las entidades de Gobierno. Actualmente está a cargo de la parte comercial de Grafiaetc, empresa que forma parte del parque tecnológico Campus Tec en Guatemala. El cuestionario se enfocará en establecer los términos y condiciones de seguridad, privacidad e identidad en las redes sociales, la proliferación y viralización de contenido actual.

El segundo entrevistado es Luis Assardo, periodista y consultor informático de RepúblicaGt, experto en investigaciones informáticas sobre seguridad y crímenes en el ciberespacio. Se especializa en asesoramientos tanto en la parte técnica como en la comunicacional, así como en la académica sobre temas digitales, de seguridad y de emergencias (<http://www.luisassardo.com/>).

El tercer entrevistado, siendo este un personaje político en las elecciones del año 2015, Jorge Marroquín, candidato a alcalde para Santa Catarina Pinula por el partido TODOS. Es abogado y notario, ha sido asesor y consultor en el Congreso de la República. Esta forma se dio a conocer las estrategias y riesgos que se corren al ser un candidato participativo en las redes sociales, ya que su campaña que desarrolló y se enfocó en tener un mayor acercamiento con los votantes a través de las redes sociales y con esto darse a conocer.

Finalmente se contó con un cuarto entrevistado, manejándolo de manera anónima, pues se pretende presentar la experiencia de trabajo en un net center. De esta forma se pudo incluir entre los resultados de esta investigación las dinámicas y mecanismo de trabajo de un "net centero" en el marco político.

3.2. Técnicas e instrumentos

Una de las técnicas que se estableció para este estudio fue un análisis de contenido y por medio de este se recolectó la información necesaria para categorizarla según las temáticas establecidas. De esta forma se puede dar a conocer su estructura, organización y dinámica.

En este caso el análisis de contenido permite analizar textos, documentos, imágenes, videos que hacen referencia a un hecho o a una persona. Por medio de los instrumentos que plantea el análisis de contenido se pueden categorizar la información recolectada. De esta forma el análisis puede llegar a ser de profundidad y estadísticamente confiable (Hernández, Fernández y Baptista, 2010).

Mientras tanto, para Gaitán y Piñuel (1998) el concepto de análisis de contenido es un conjunto de procedimientos interpretativos y de refutación aplicadas a productos comunicativos o cualquier relación con comunicaciones previamente registrados como un documento. Esta técnica extrae y procesa datos relevantes sobre el producto evaluado.

Para el análisis de contenido se utiliza como instrumento tablas de cotejo. Según los autores Hernández, Fernández y Baptista (2010) las tablas de cotejo se logran la categorización, recolección e identificación de datos dentro de los documentos, textos o cualquier material visual a analizar. En este instrumento se presentan una serie de puntos a evaluar con el cual se logra mayor detalle según los propósitos específicos que se planteen.

Con el fin de analizar los perfiles falsos que se encuentren en Twitter se utilizaron dos tablas de cotejo:

En la primera tabla de cotejo (Anexo I) sirvió como primer filtro para poder catalogar al perfil encontrado en Twitter como: falso. Se distribuyó de la siguiente manera:

- Usuario y a que personaje político hace referencia.
- Se enumerarán las características que tiene un perfil falso para poder catalogarlo como tal y así pasar al siguiente análisis.

En cuanto a la segunda tabla de cotejo (Anexo II), sirvió como análisis para las dinámicas de comunicación y con qué fines fue creado, así como los mensajes y reacciones que se observan en el perfil falso.

- Según los fines: burla, a favor, en contra, crítica
- Según los mensajes: discriminación, odio, alentadores, apoyo y rechazo.
- Según dinámicas de comunicación: texto, vídeo, gif, enlaces, fotografías.
- Según la interacción: RT, comenta, me gusta, respuesta e impacto.

Por otro lado, para fines de profundizar y responder aún más los objetivos planteados en este estudio, se establecieron entrevistas de profundidad, en las cuales se abordó sobre cómo los perfiles falsos pueden ser una herramienta clave de comunicación política y cómo pueden llegar a formar parte de la opinión pública o bien influir en la percepción de las personas, asimismo dar a conocer las dinámicas de los mismos.

Para el método cualitativo la entrevista es un espacio más íntimo, flexible y abierto (King y Horrocks, 2009) (Hernández, Fernández y Baptista, 2010 p. 418). En ese espacio se puede alcanzar un diálogo donde el entrevistado dé a conocer datos e información relevante para un determinado tema y ser el entrevistador el encargado de sacar a relucir la información adquirida (Hernández, Fernández y Baptista, 2010).

Para realizar las entrevistas de profundidad se formula un cuestionario que ayuda a construir una conversación de preguntas y respuestas para llegar a la idea objetada. Según Arribas (2004) el cuestionario "es un instrumento utilizado para la recogida de información, diseñado para poder cuantificar y universalizar la información y estandarizar el procedimiento de la entrevista"... "Antes de proceder a medir algo debemos tener una idea muy clara de lo que queremos medir" (p. 23-24).

Se contó con la participación de expertos en la materia y para ello se establecieron cinco subtemas dentro de la entrevista (Anexo III): seguridad en la web, el comportamiento de los

perfiles falsos, las dinámicas de comunicación de los perfiles falsos, los perfiles falsos en la ciberpolítica y una campaña electoral en redes sociales.

Hernández, Fernández y Baptista (2010) proponen la entrevista semiestructurada, la cual da la oportunidad al investigador de realizar según la obtención de datos durante el período de análisis del estudio. Así también, se pueden ir agregando o replanteando las preguntas en el cuestionario, según lo requiera la investigación.

Por último se utilizó la aplicación TwitterAudit (www.twitteraudit.com) para verificar la veracidad y calificación de efectividad del perfil falso. Según la descripción del sitio de la aplicación indica que la puntuación se basa en el número de tuits, la fecha de la última publicación y la proporción de seguidores. Por medio de estos datos verifican si el perfil es falso o verdadero. Aclara que puede llegar a ser una puntuación no perfecta pero da pauta a la efectividad y veracidad de los perfiles evaluados. Asimismo, resalta que no están aliados a la plataforma Twitter.

3.3. Procedimiento

- Selección de tema a investigar.
- Se planteó el problema, la pregunta de investigación y los objetivos del estudio.
- Las variables fueron identificadas y definidas de manera conceptual y operacional.
- Se plantearon los alcances/límites y el aporte del estudio.
- Se determinó la búsqueda y redacción de antecedentes nacionales e internacionales que respaldan que la investigación es novedosa.
- Para el respaldo teórico se realizó una búsqueda de bibliografía que complementaran la estructura del marco teórico.
- Se construyó y estructuró el marco teórico en cuatro temas principales. Procediendo a la redacción del mismo.
- Determinación de la metodología del estudio, el tipo de estudio y como se pretende alcanzar los objetivos anteriormente establecidos.
- Búsqueda de una muestra para analizar, según los requisitos del estudio.

- Se plantearon las técnicas de estudio: análisis de contenido y entrevistas de profundidad.
- Determinación de los instrumentos de estudio: tablas de cotejo, cuestionario (semiestructurado) y el uso de la aplicación TwitterAudit.
- Se presentó el anteproyecto para su debida evaluación y validación.
- Se analizó el contenido establecido en la muestra de estudio.
- Se inició con el trabajo de campo.
- Se presentaron y analizaron los resultados obtenidos.
- Se establecieron conclusiones y recomendaciones sobre la investigación.

3.4. Tipo de Investigación

Para lograr los objetivos de esta investigación se basará en un enfoque cualitativo pues según Sampieri (2010, p. 549-550) este se enfoca en comprender fenómenos y explorarlos con distinta visiones, técnicas por medio de la interpretación de los datos recolectados.

En cuanto la recolección y análisis de datos, es probable que vayan surgiendo otro tipo de cuestionamientos que hagan del estudio más dinámico en el que se puedan llegar a recorrer distintos espacios no tomados en cuenta al principio de la investigación. Asimismo la recolección de datos es mucho más abundante y variada, esto posibilita tener distintas visiones. El procedimiento de este tipo de investigaciones da la oportunidad de realizar valoraciones críticas completas. Por último la credibilidad y dinámica de los resultados es característico de este tipo de enfoque.

En el libro La investigación en comunicación, del Río (2011) plantea que la investigación cualitativa intenta descubrir los significados de acciones, sucesos o hechos y comportamientos sociales.

IV. Presentación y análisis de resultados

Durante el periodo de la investigación se lograron detectar 35 perfiles falsos relacionados a los personajes o figuras políticas guatemaltecas designadas en la parte metodológica del estudio. La búsqueda fue a través de la opción que incluye la plataforma Twitter, se empezó a buscar por el nombre del personaje político, luego por medio de etiquetas que se han dado a conocer en los eventos o casos específicos de la política guatemalteca durante el 2015 hasta el 2017.

Se definieron como falsos al coincidir con las características establecidas en el Anexo I. Posteriormente se realizó una elección de 15 perfiles, pues estos eran afines a los objetivos del estudio. Por medio de estas cuentas se pudieron detectar las dinámicas de comunicación y lenguaje que manejan, cómo se comportan y la efectividad de modificar o manipular la percepción en los usuarios de la plataforma Twitter.

Como menciona Assardo (2016) una cuenta falsa es fácil de identificar la mayoría de veces, sin embargo existen casos que manejan un estilo tan real que es fácil caer en esas oscuras redes. Características de la fotografía de perfil, número de seguidores y personas a las que sigue, contenido audiovisual que publica, fecha de creación y descripción, así como los tuits y contenido que replica fueron claves para la detección de las cuentas.

El monitoreo de las cuentas se basó según el fin, el mensaje, según las dinámicas de comunicación y según el nivel de reacción e interacción. En esta parte se describió de manera detallada las características de cada perfil y su comportamiento en Twitter.

Hay que recordar que el juego de la creación de cuentas falsas va de la mano con el objetivo de la cuenta y a quién se quiere atacar, de esta forma se puede llegar al tipo de discurso que maneja cada cuenta. Asimismo es necesario aclarar que este estudio no detectó el origen de las cuentas ni definió por quién/quienes fue creado. En esta ocasión solo se definió si era falso, a qué personaje político hace referencia y cómo actúa en la red.

Por otro lado, los datos básicos como: número de los que sigue o seguidores, así como el número de tuits puedan que hayan cambiado en las cuentas que siguen en actividad esto

puede ir variando día a día. Es decir que se presentarán con los datos que fueron capturados en un día determinado entre los meses de Junio a Noviembre del año 2017.

Jimmy Morales:

Se detectaron seis cuentas falsas en referencia a Jimmy Morales, la mayoría eran con fines de burla o parodia como bien indicaba en cada una de las descripciones. Otras cuentas fueron creadas para la época electoral y el resto actualmente siguen en actividad con el fin de estar al tanto de las acciones que ha tomado el político como presidente de Guatemala.

Cuentas:

1. @jimmymoralesgua
2. @jimmymoralesc
3. @jimmymorales_gt
4. @Plaid_JMorales
5. @MafiaJimmy2016
6. @jimmymoralesgt

De las cuentas que se detectaron se analizaron las más activas, entre ellas:

- **@jimmymoralesgua**

El perfil está en actual actividad, utiliza una fotografía del personaje político, cuenta con 868 usuarios a los que sigue y 2,328 seguidores. Fue creada en el año 2014, en la descripción del perfil indica que es para fines humorísticos en base a las acciones de Morales. Atentos a las declaraciones u otro tipo de publicaciones del Presidente, pues de eso depende la cuenta. El mensaje que se maneja es negativo, con rasgos de discriminación y rechazo. Se hace pasar por Jimmy Morales de manera sarcástica, con eventual utilidad de palabras soeces.

Se comunica a través de la utilización de los 140 caracteres que permite la plataforma Twitter, así como el uso de fotografías o memes en referencia a los temas presidenciales.

Según las dinámicas que se detectaron sobre la interacción se puede mencionar que los tuits sin ningún tipo de material multimedia (video, fotografía, entre otras) reciben mayor aceptación o reacción de los usuarios.

La reacción más relevante es el de “Me gusta”, le sigue la opción de RT (Retweet) y por último la reacción menos utilizada es la de “Responder”. El perfil no responde a ningún tuit que publican los usuarios, sin embargo la cuenta es dinámica al observar que los usuarios responden por medio de las mismas dinámicas de comunicación que utiliza el perfil. Sí hay continuidad humorística y sarcástica por parte de los usuarios hacia las publicaciones que realiza el perfil.

Por último se puede determinar que el perfil se encarga más de replicar publicaciones de otras cuentas, así como de las publicaciones de los medios de comunicación en referencia a Jimmy Morales, sin embargo en cada una de estas las acompaña con un tuit sarcástico, discriminatorio y con un fin de burla. El perfil al hacerse pasar por el presidente esto provoca confusión al usuario que no tenga la capacidad de poder verificar la oficialidad de la cuenta o bien por medio del discurso que maneja engancha a los usuarios por ser afín al humor guatemalteco. En este sentido se puede justificar el número de seguidores.

En cuanto los resultados que presenta TwitterAudit sobre la cuenta:



De 2,328 seguidores, 38 son falsos y el resto son reales. Por lo tanto tiene una calificación del 98% de efectividad. Esto quiere decir que logra enganchar a usuarios reales por el tipo

de contenido que maneja, así como el discurso y su forma de comunicarse por medio de réplicas de publicaciones y sentido humorístico.

- **@jimmymorales_gt**

Cuenta creada en Julio del 2015, con 425 seguidores y a 1553 que sigue. Actualmente se encuentra sin actividad, registra 135 tuits con un fin de apoyo hacia Jimmy Morales durante su candidatura como presidente en el mismo año de su elaboración. Cuenta con una de las fotografías utilizadas en campaña como avatar.

El objetivo de la cuenta puede determinarse que fue replicar las publicaciones del partido que representaba Morales, así como las publicaciones oficiales del candidato. Esporádicamente tuiteaba para manifestar su apoyo y afinidad con el discurso de campaña que manejó Jimmy Morales.

El mensaje que manejaba se determinó como positivo pues el contenido que publicaba eran en pro a Jimmy, asimismo el lenguaje que se observó es breve, coherente y conciso. Se percibió que algunas publicaciones eran manejadas con un lenguaje político. Sin ofensas, ni insultos.

Las dinámicas de comunicación se vieron reflejadas en los tuits, replica de videos o enlaces publicados en la cuenta oficial de Jimmy Morales. Respecto al uso de las fotografía las publicaba para exhortar al votante, así como pequeñas descripciones de los logros y las actividades del candidato.

Por otro lado, lo que reflejó en las dinámicas de interacción fue que las publicaciones que contiene material multimedia, obtuvo mayor aceptación y reacción de usuarios. La mayor reacción detectada fue la de RT (Retweet), segundo plano “Me gusta” y de último “Responder”. No existe respuesta del perfil hacia los usuarios que interactúan. Sin embargo, por parte de los usuarios se observaron respuestas que coinciden con el discurso de la cuenta y en otros casos ataques de rechazo, insultos sobre alguna publicación determinada.

De esta manera se determina que sí influye en cuanto al manejo del discurso político, pues la mayoría de respuestas que recibe afirman su apoyo y voto hacia el candidato. Logra engañar aquel usuario que no tiene el conocimiento de la verificación de cuentas de Twitter sobre las personas públicas. Por consiguiente, el personaje sí logra el objetivo de apoyo hacia Jimmy Morales.

TwitterAudit:



Del total de seguidores hay 14 perfiles falsos, por lo tanto su calificación de efectividad es de 96%. Esto indica que el contenido que manejó durante la campaña hasta la toma de posesión de Jimmy Morales, resultó a fin a muchos usuarios reales.

- **@Plaid_JMorales**

El perfil sigue los alineamientos de The Plaid Avengers, este sitio web se basa en construir espacios humorísticos sobre líderes del mundo u organizaciones como la ONU o la UE. En el caso de Guatemala, la cuenta fue utilizada para el gobierno de Otto Pérez Molina por lo tanto fue creada en el año 2012 y por esta razón se pueden observar antiguas publicaciones de la época de su mandato. Otra característica que se logra observar de este perfil es que todas sus publicaciones manejan el idioma inglés.

Cuenta con 1,163 seguidores y sigue a 317 usuarios. Por el momento lleva publicados 662 tuits y cuenta con foto de perfil de Jimmy Morales. Como anteriormente se mencionó, este perfil está destinado para expresiones sarcásticas sobre Morales, de manera humorísticas sin llegar al punto de insultos u ofensas. Mantiene una agenda sobre las publicaciones, comparte enlaces de artículos sobre Guatemala, así como datos pocos conocidos sobre el país.

En cuanto al idioma que se maneja puede llegar a ser una limitante para la comprensión del perfil, por eso mismo no recibe mayor respuesta por parte de los usuarios, aunque se logró observar ciertos “Me gusta” y Retweets. No existe respuesta por parte de @Plaid_JMorales.

Se comunica a través de tuits sarcásticos referentes a las acciones de Jimmy Morales, así como los videos y fotografías. En otras publicaciones se pueden observar enlaces hacia sitios que tratan temas en relación a Guatemala u otro tipo de acciones en el marco político a nivel mundial.

Resultados de TwitterAudit:



Obtiene un 92% de efectividad, ya que del total de seguidores 98 son falsos y 1,219 reales.

- **@jimmymoraIesgt**

El usuario de este perfil tiene similitud con el usuario de la cuenta oficial del Presidente Jimmy Morales, por el cual logra causar confusiones con una cuenta y otra. En esta ocasión la letra “l” difiere la letra i (I) mayúscula. Tiene 5,345 seguidores y no sigue a ningún usuario. En cuanto a publicaciones tiene un registro de 213 tuits y fue creada en Enero del 2015.

Perfil humorístico sobre la imagen del Presidente Jimmy Morales, por esta razón alude al rechazo de su gestión a través de chistes, burlas y mensajes sarcásticos. Por medio de un lenguaje amigable al humor guatemalteco logra recibir un alto índice de feedback.

Las dinámicas de comunicación que utilizan son el tuit sin material multimedia o la elaboración de videos editados en los cuales enfatiza los errores de los discurso que ha hecho el Presidente. Uso alto de memes, así como fotografías reforzadas con tuits humorísticos o con un discurso de burla. También se manifiesta la utilización de gifs ridiculizando al mandatario.

Sí hay alto uso de las reacciones de interacción por parte de los usuarios que reciben las publicaciones del perfil, aunque este no tenga participación de respuesta. En este sentido recibe respuestas con material multimedia.

Se considera influyente, pues el user provoca confusión con el perfil oficial de Jimmy Morales. Logra engañar al usuario que no está familiarizado con la plataforma y no sepa identificar el perfil verificado de una persona pública. Por esta razón se puede justificar el número de seguidores y así también el mensaje y lenguaje que lleva a cabo logra enganchar las personas, creando un espacio humorístico sobre la imagen del Presidente.

Resultado de TwitterAudit:



Recibe una efectividad de 98%, dentro de sus seguidores hay 69 cuentas falsas. Al tener la misma fotografía y un usuario similar a la cuenta oficial logra obtener seguidores por motivos de confusión o afinidad con el discurso que se maneja.

Álvaro Arzú

El alcalde Álvaro Arzú es una de las figuras políticas que se consideran como la más activa en redes sociales. Asimismo sucede con algunos de sus familiares pues han sido expuestos desde que él inició su carrera política. Al buscar perfiles falsos en referencia a esta figura, se lograron detectar dos cuentas relacionadas con sus familiares. Se escogieron las dos cuentas más activas y con mayor movimiento en la actualidad.

Cuentas:

- @AlvaroArzu
- @Arzu_Tonatiuh
- @LaDonaPatydArzu (en referencia a su esposa Patricia de Arzú)
- @vidacotidiana21 (en referencia a su hijo Roberto Arzú)

Cuentas analizadas:

- @Arzu_Tonatiuh

En la actualidad esta cuenta cambió de usuario, ahora se encuentra como: @Arzu_Alvarito, con este cambio hace aún más referencia a Álvaro Arzú y como foto de perfil muestra una

caricatura de él. Tiene 887 seguidores y sigue a 576, fue creada en Septiembre del 2011 y cuenta con 735 publicaciones.

Empezando por la descripción del perfil, se determinó que la cuenta es con propósitos de parodia sobre el político. Maneja un discurso de odio y rechazo. El odio se manifiesta a través de tuits que indican que le desean el mal o se alegran por el tipo de “consecuencias” que trascienden de los casos actuales que han venido surgiendo como las denuncias y antejuicios en su contra. Mientras el rechazo se manifiesta por medio de las publicaciones que replican acerca de sus acciones o de otros usuarios que están en contra de él, asimismo las publicaciones de notas o reportajes de medios independientes.

Construye el discurso por medio de un lenguaje amigable al humor guatemalteco pues implementa la utilización de palabras soeces, insultos y burlas. Construye la comunicación por medio de todas las herramientas, es muy diverso y dinámico en las publicaciones, el uso de memes, videos y gif le dan personalidad.

Se determinó que logra obtener reacciones por los seguidores o de usuarios en general. Sí tiene alta interacción con los usuarios que le responden o comenta sus publicaciones. La misma dinámica que maneja el perfil es la misma que manejan los usuarios que le responden. Creando un espacio de discursos de rechazo, humor y libertad de expresión acerca del personaje y sus referentes políticos.

Más que influyente puede declararse una cuenta con intenciones de persuasión y manipulación sobre las acciones del alcalde, pues replica mucho el contenido que delata al personaje, así como contenido modificado para crear un discurso de rechazo y odio. Replica también notas de medios que siguen una línea en contra del personaje como en apoyo al discurso que se maneja. Así como publicaciones que deja en claro su apoyo a las autoridades de investigación e instituciones como CICIG y MP que últimamente han tenido varias confrontaciones con Arzú.

Resultados de TwitterAudit:



Según la evaluación y análisis de la aplicación, del total de usuarios que siguen al perfil, existen 8 cuentas falsas. En este sentido obtuvo un 99% de calificación.

- **@LaDonaPatydArzu**

Un espacio cómico sobre la imagen de Patricia de Arzú, haciendo referencia a que ella es la que publica y replica el contenido. Cuenta con la misma fotografía de la cuenta oficial y en su descripción indica: “5to primaria Colegio Cristiano de la Doble Moral Santa Tecla El Salvador”. Por el momento tiene 3,190 tuits publicados y fue creada en Agosto de 2011.

Se observó que realiza publicaciones acerca de asuntos de gobierno y situaciones coyunturales del país. Rechaza acciones de medios de comunicación (canales nacionales, GuateVisión y Prensa Libre), así como acciones de Congreso y otros personajes políticos. Publica contenido humorístico sobre Patricia de Arzú, sin embargo maneja el discurso de rechazo hacia otros personajes. Se crea un espacio de denuncias por medio de su imagen.

El lenguaje que se maneja es informal y amigable con el humor guatemalteco. Mensajes de recomendaciones o denuncias de acciones políticas. Haciendo referencia al estereotipo de cómo se comporta normalmente una mujer adulta. En algunas publicaciones maneja un discurso soez. Pero se limita a manejar un discurso sarcástico.

Utiliza más texto que otro tipo de material comunicacional. Casi siempre va acompañado con etiquetas que hace referencia a sucesos actuales o refuerzan el mensaje. En la mayoría de publicaciones no utiliza material audiovisual. Hace uso de memes referencias a acciones que caen en el “pecado”. Puede determinarse que las fotografías es el material más utilizado, acompañado por textos que refuerzan o explican el porqué de la fotografía.

En cuanto el nivel de interacción se puede mencionar que los tuits que van acompañados con algún material multimedia obtiene mayor peso o aceptación pues la respuesta de los usuarios es alta. Asimismo el perfil se toma el tiempo para poder responder e interactuar con los usuarios. En este sentido se puede determinar que sí es influyente porque se convierte en un espacio donde el perfil y los seguidores desahogan denuncias de acciones de gobierno y municipales pero con un sentido humorístico. El mayor gancho de eso es que se presenta un discurso que alude al estereotipo de “madre consejera”.

Según los resultados de TwitterAudit cuenta con 50 perfiles falsos dentro de sus seguidores y una calificación de 99%:



Neto Bran

Otra figura política que ha causado revuelo desde su toma de posesión como alcalde de Mixco es Neto Bran. Se ha caracterizado por ser muy activo en sus redes sociales, cercano a los vecinos y por dejarse exponer por muchos medios ha influido en la creación de cuentas de fanáticas, sin embargo no se salva de las cuentas falsas que hacen referencia a su persona.

Se detectaron tres cuentas falsas a su nombre, con usuarios despectivos o similares al usuario oficial:

- @netobron
- @MixcoBran
- @HuecoBran

Se tomó una sola cuenta para analizar.

- **@MixcoBran**

Este perfil fue creado en Junio de 2015, cuenta con 397 seguidores y sigue a 336 usuarios. Por el momento lleva 5,050 publicaciones. Como foto de perfil tiene un montaje de Neto Bran y se describe como “Vecino Mixqueño”.

Se determinó que el perfil es utilizado para resaltar errores, denuncias y ausencia de Bran en algunas áreas del municipio. Está totalmente en contra de la administración del alcalde y por esa razón maneja un mensaje negativo, La discriminación, rechazo y odio es lo que resalta en cada publicación. Deja mal visto al político y lo presenta con mala reputación por medio de ofensas y fotografías manipuladas.

El lenguaje es informal y en algunas publicaciones utiliza palabras soeces y ofensivas hacia Neto Bran. Utiliza mucho material multimedia, en especial memes y las fotografías es el material más utilizado, acompañado por textos que refuerza o explican el porqué de la fotografía. Enlaza a medios masivos ya sea en contra o favor de las publicaciones de dichos perfiles. Replica publicaciones de otros perfiles afines a la temática o discurso que maneja la cuenta.

No obtiene mayor respuesta, sin embargo las respuestas que se lograron detectar siguen la misma línea de la cuenta. Esporádicamente el perfil responde a usuarios que opinan sobre algún tema relacionado con la situación actual en el marco político.

Un perfil dedicado a denunciar y expresar su pesar, rechazo y odio a diferentes figuras políticas a través de la imagen de Neto Bran. Ataca a otros usuarios, así como a los perfiles oficiales de algunos políticos. Más que influyente es un es perfil de odio y rechazo dedicado a replicar denuncias y faltas de políticos.

Resultados de TwitterAudit



Recibe una calificación de 88% de efectividad y del total de perfiles 16 son falsos.

Edwin Escobar

En el caso del alcalde de Villa Nueva se detectó un solo perfil falso. Fue difícil determinarlo como tal pues en la cuenta oficial no lleva una misma línea, agenda o no se maneja con formalidad, sin embargo el número de seguidores, el número de tuits publicados y la descripción fueron útiles para definir e identificar cada perfil.

- **@EdwinEscobarGua**

La cuenta fue creada en Octubre de 2016, tiene 163 seguidores y sigue a 32 usuarios. Son 38 publicaciones las que se lograron registrar. El perfil se hace pasar por el alcalde y es con el fin de replicar la agenda de actividades que realiza por y en el municipio. Así como publicaciones en referencia a la situación actual del país.

Maneja un mensaje positivo en apoyo a Edwin Escobar. Asimismo manifiesta halagos y mensajes alentadores por medio de un lenguaje coloquial, amigable y fácil de asimilar. En

algunas publicaciones maneja discurso político, haciendo referencia a una crisis política del país, así como alentando al diálogo en Guatemala.

La mayoría de tuits van acompañados por fotografías. Utiliza altas cantidades de fotografías junto con texto, así como réplicas de fotografías que han sido publicadas en las cuentas oficiales de distintas instituciones de gobierno y municipales. Así como de los medios de comunicación.

Reciben mayor respuesta las publicaciones que van acompañadas de material multimedia. Lo Retweets manifiestan mayor uso, en segundo lugar los “Me gusta” y respuestas con halagos y reafirmación del apoyo hacia el alcalde. De esta manera se construye un espacio de apoyo hacia la administración de Edwin Escobar entre el perfil y los usuarios a los que está expuesto.



Según los resultados de TwitterAudit indican que del total de seguidores 8 seguidores son cuentas falsas con una calificación de 95% de efectividad.

Juan Manuel Giordano

De las figuras políticas del Congreso de la República de Guatemala, se detectó una cuenta falsa del diputado Juan Manuel Giordano del partido FCN-Nación. En la actualidad, según sus últimas declaraciones a medios de comunicación en el mes de Septiembre, indicó que cerró su cuenta oficial en Twitter, sin embargo se pudo detectar un perfil que se hace pasar por él con sentido de sátira y burla hacia su persona y el resto de diputados.



Captura de imagen en la plataforma Twitter. Al ingresar el usuario que utilizaba Giordano anteriormente.

- **@dipukid**

La cuenta tiene por el momento 1,089 publicaciones, 260 seguidores y sigue a 336 usuarios. Como fecha de creación tiene el mes de Enero en el 2016. El fin del perfil es para publicar contenido de sátira, burla y rechazo hacia el diputado. Maneja un mensaje negativo con expresiones humorísticas aludiendo incapacidad de ejercer el puesto de diputado, así también por ser uno de los diputados más jóvenes del Congreso.

Por medio de un lenguaje informal el perfil replica publicaciones humorísticas o informativos en referencia al congreso y al diputado. Así también textos humorísticos sobre supuestas actividades que realiza el diputado. Así como la réplica de videos y memes, en el caso de las fotografías delatan o son reforzadas con textos o burla a la acción que aparece en la imagen. Comparte varios enlaces de noticias de distintos medios masivos.

Obtiene mayor reacción los tuits que enlazan a otras publicaciones o bien las publicaciones propias acompañadas de fotografías o memes humorísticos. Los “Me gusta” tienen mayor utilidad de reacciones, segundo lugar RT y poca utilidad de la opción de respuesta. En cierto modo influye a los usuarios y seguidores del perfil, crea un espacio sarcástico sobre la imagen del famoso “dipukid”. Expresiones delatadoras como burlas sobre las acciones conocidas que han realizado en el 2017.

En el caso de los resultados de TwitterAudit indican:



Una calificación de 95% y detecta 12 seguidores falsos.

Iván Velásquez

Por el impacto que ha recibido la figura de Iván Velásquez en Guatemala es importante buscar perfiles de dudosa procedencia que se refieran a este personaje. La búsqueda fue tardada y difícil en una plataforma tan amplia, sin embargo, se pudo detectar un perfil que contiene la fotografía de Velásquez pero se presenta como @BobGramajo.

Según la explicación de Redondo (2016) se puede decir que un usuario que se esconde tras un perfil falso para atacar, sus post o tuits están cargados de insultos y groserías, como la orientación al odio. Este es el caso de la cuenta detectada, orienta el odio hacia la izquierda y a otras figuras políticas.

- **@BobGramajo**

Cuenta con 607 seguidores y sigue a 285 usuarios, se capturaron 1,073 publicaciones y fue creado en Marzo de 2017. Como se mencionó anteriormente, utiliza una fotografía de Iván Velásquez en alusión a que es un perfil pendiente de toda acción política. Que está a la mira de los demás. Alude estar en contra de la ideología izquierdista así como su rotundo rechazo a muchas acciones populistas. En contra del comisionado Velásquez, PDH, la CC, MP y líderes de izquierda.

Por medio de un mensaje negativo y de rechazo replica contenido de otros usuarios o información importante sobre casos manejados por la CICIG y MP. El lenguaje que se

maneja es con términos políticos y legales. Así también mensajes con un lenguaje que invita a cuestionar muchas acciones de CICIG y MP.

La comunicación que establece es por medio de Retweets de publicaciones de otros perfiles y los refuerza con una opinión o con palabras que indican que está a favor o en contra con lo que dice la publicación. Utiliza varias fotografías que cuestiona la percepción de los asuntos actuales en la política guatemalteca, reforzadas con textos, burlas o rechazo de las acciones que presentan.

Obtiene mayor reacción los tuits que enlazan a otras publicaciones o bien las publicaciones propias acompañadas de fotografías. La reacción más utilizada es la opción de RT, segundo lugar “Me gusta” y por último la opción de “Responder”.

Es un espacio donde el perfil por medio de la fotografía de Iván Velásquez deja en claro su rechazo a las acciones de este personaje político así como de sus referentes: Thelma Aldana, Jordán Rodas, Fundación Mirna Mack, entre otros.

Resultados de TwitterAudit



Una calificación de 98% de efectividad y reporta 11 usuarios falsos dentro de sus seguidores.

Candidatos en las elecciones 2015

Entre los perfiles falsos que hacen referencia a los candidatos políticos se pudo determinar que actualmente no se encuentran en actividad. De los tres candidatos designados se encontró un perfil falso por cada uno. Asimismo, vale la pena mencionar que dentro de la búsqueda de perfiles se encontraron siete cuentas falsas de Rigoberta Menchú.

Se decidió analizar dos perfiles ya que presentaban más información para poder ser monitoreados.

Cuentas

1. Manuel Baldizón: @UNNOABALDIZON

Este perfil contaba con 38 seguidores, 220 seguidos, 1758 publicaciones y fue creada en Mayo de 2015. Por el tipo de contenido se detecta que maneja un discurso en contra de Baldizón.

2. Sandra Torres: @SandritaExColom

Se detectaron 11 seguidores, 96 seguidos, 13 publicaciones y fue creada el mismo mes y año que la cuenta de Manuel Baldizón. En este caso, es un perfil dedicado a la parodia de la candidata.

3. Zury Ríos: @ZuryGuate

Esta cuenta tiene un fin de apoyo hacia la candidata durante la época electoral, maneja un mensaje positivo. Replica publicaciones del partido o bien del perfil oficial de la candidata. Así como agradecimientos hacia los seguidores y palabras en pro a Zury. Construye mensajes alentadores a través de un lenguaje coloquial o en algunos casos políticos, con un discurso en pro a la candidata, de manera convincente acerca del plan y propuesta de gobierno.

El perfil se hace pasar por Zury, manifestando rechazo hacia el resto de candidatos. También replica publicaciones de otros perfiles y los refuerza con una opinión o con palabras que indican que está a favor de la candidata, así como fotografías que cuestionan

las acciones de otros candidatos y las refuerza con tuits. Se detectó que enlaza publicaciones de varios medios masivos que y les agrega un mensaje de rechazo o apoyo con la noticia compartida.

Obtiene mayor reacción los tuits que enlazan a otras publicaciones o bien las publicaciones propias acompañadas de fotografías. No existe respuesta por su parte hacia los usuarios. Las respuestas que recibe acerca de sus publicaciones no utilizan material multimedia, sin embargo los tuits observados, en su mayoría, afirman o coinciden en opiniones e ideas con el perfil falso. En algunas ocasiones los usuarios etiquetan o mencionan tanto el perfil oficial de la candidata como el perfil falso. Sí influye en cuanto a las publicaciones compartidas por medios de comunicación o del perfil oficial de la candidata, pues recibe mayor reacción en cuanto a los RT y “Me gusta”.

Según los resultados de TwitterAudit indican que existen 3 perfiles falsos como seguidores y le recibe una calificación de 97%.



4. Rigoberta Menchú:

Durante la búsqueda de cuentas falsas referentes a los candidatos de las elecciones del 2015 se encontraron diferentes cuentas referentes a Rigoberta Menchú, en cuanto a eso se tomó la decisión de analizar la cuenta que contaba con mayor información.

- @MenchuDice
- @LaMenchu
- @Soy_laRigoberta
- @LaRigoMenchu
- @LaMenchuDice

- @rigobert0menchu
- @amante_indigena

Cuenta analizada:

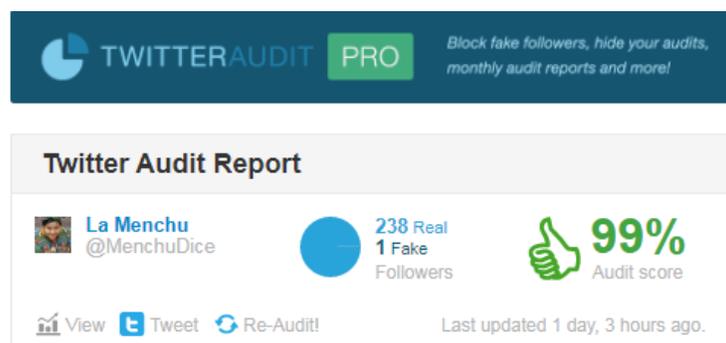
- @MenchuDice

Un perfil creado con fines de sátira, burla y ofensa hacia Rigoberta Menchú. La cuenta hace referencia que ella es la que la maneja y la mayoría de publicaciones utiliza un mensaje negativo con discriminación. El lenguaje que se maneja es coloquial amigable al humor guatemalteco, respondiendo a los prejuicios de discriminación que existen en Guatemala hacia los indígenas.

Textos humorísticos y en ciertas ocasiones refleja opiniones sobre acciones políticas. Poco uso de material multimedia, sin embargo cuando hace uso hace referencia a Menchú con intenciones de burla y ofensa.

No obtiene mayor respuesta o reacción por parte de los usuarios y al mismo tiempo no interactúa el perfil tampoco brinda respuesta hacia los usuarios. El perfil no es muy influyente pues en la actualidad que encuentra inactiva. Sin embargo, durante su época de actividad generó reacciones como los RT y me gusta sobre las publicaciones.

Resultados de TwitterAudit:



Lo califica con un 99% e indica que existe un perfil falso como seguidor.

Binomio presidencial 2012-2015

A partir del año 2015 el uso de las redes sociales en el país giraron hacia las acciones y casos de corrupción sucintados en la administración de Otto Pérez Molina y Roxana Baldetti, siendo parte de hechos de malversación de fondos en el Estado y cabezas de diferentes actos delictivos. Esto provocó un revuelo de indignación ciudadana y tomas de decisiones de diferentes sectores del país. Siendo el año 2017 los casos se siguen tratando en los juzgados y por esa razón se mantienen vigentes en redes sociales.

No es de extrañarse que existan perfiles falsos que traten o refieran sobre estas dos figuras políticas, en el caso de este estudio se logró detectar tres perfiles falsos en relación a Roxana Baldetti y tres en referencia a Otto Pérez Molina.

Cuentas

Otto Pérez Molina:

- @OttoPerezMulona
- @OttoPerez_GT
- @Otto_PerezM

Roxana Baldetti

- @Roxanabalbote
- @roxanabaldetti
- @roxanabaldetti1

Del total de cuentas falsas encontradas se analizaron las cuatro más dinámicas en cuanto al manejo de contenido y publicaciones que hacen referencia a las dos figuras políticas.

- **@OttoPerezMulona**

Perfil con sentido sarcástico sobre Otto Pérez y otros políticos. Maneja un mensaje negativo y de rechazo. Por medio de un lenguaje informal y amigable con el humor negro guatemalteco construye el mensaje que comparte. En algunas ocasiones utiliza palabras soeces.

Replica publicaciones de otros perfiles y propios manejando en su mayoría la sátira u opiniones referentes a la situación actual en el marco político de Guatemala. La mayoría de publicaciones son memes en referencia a asuntos políticos actuales. Por otra parte, replica contenido de medios masivos y utiliza fotografías delatadoras o sarcásticas reforzadas con pequeñas frases.

Obtiene mayor reacción los tuits que enlazan a otras publicaciones o bien las publicaciones propias acompañadas de fotografías o memes humorísticos. Eventualmente interactúa con los usuarios y estos responden o comentan a las publicaciones.

Es un espacio de denuncias y expresiones de rechazo hacia la política que se maneja en la actualidad en Guatemala. Combina la sátira con la opinión. En cierta forma llega a influir pues en las reacciones se detecta dinamismo.

Resultados de TwitterAudit:



98% de calificación y reporta 11 perfiles falsos como seguidores de la cuenta.

- **@OttoPerez_GT**

Perfil que hace referencia con el binomio presidencial antes mencionados. Presenta un discurso en contra de ese mandato con fines sarcásticos. Por lo tanto el mensaje que se logró detectar es de rechazo a través de un lenguaje informal. Incluye humor negro con mensajes soeces.

Replica publicaciones de otros perfiles y propios manejando en su mayoría la sátira. La mayoría de publicaciones son memes en referencia al binomio presidencial. No registra mayor respuesta de los usuarios, sin embargo confronta y discute con el usuario que le responde alguna publicación. Induce a un ambiente tenso donde se refleja el choque de ideas. El uso de material multimedia por parte del perfil es esporádico.

Actualmente la cuenta se encuentra sin actividad, sin embargo se determinó que fue destinada para denunciar, burlarse y rechazar las acciones de Otto Pérez Molina. Replicó información y contenido sobre Roxana Baldetti y otros temas de interés. En ocasiones manejó discurso de odio y otras veces crea un ambiente de sátira.

En TwitterAudit recibe una calificación de 97% e indica que 3 seguidores son de cuentas falsas.



- **@Roxanabalbote**

Perfil con sentido sarcástico no solo de Baldetti sino referente a otros políticos. En su mayoría a Neto Bran. Por medio de un mensaje negativo manifiesta su rechazo ya sea por publicaciones propias o por el contenido que replica sobre publicaciones de otros perfiles con sentido humorístico y sarcástico en el marco político.

La mayoría de publicaciones son memes en referencia al Roxana u otros políticos. Comparte fotografía delatadoras o manipuladas reforzadas con frases de rechazo, odio o

sátira. Las publicaciones reciben más “Me gusta” que RT. No responde a los usuarios, pero estos sí le comentan siguiendo la misma línea del discurso que presenta.

Es un espacio donde el perfil por medio de la imagen de Roxana provoca un ambiente de sátira, pues esa es como su materia prima. No solo en referencia a los involucrados de los casos descubiertos en los últimos años sino que a otros personajes políticos como el caso de Neto Bran. Es una cuenta con bastante actividad que se toma el tiempo para armar bien el mensaje y así publicarlo. En este sentido puede provocarse en influyente.

TwitterAudit:



Del total de seguidores reporta 23 usuarios falsos, con una calificación de 90%.

- **@roxanabaldetti1**

En el caso de esta cuenta presenta poco sentido sarcástico pero alude estar en contra de Baldetti. Lo expresa en la descripción declarando odio hacia su persona. Su discurso base es el odio y rechazo hacia los involucrados en los casos recientemente sacados a la luz. Replica publicaciones de medios masivos o de otros perfiles afines al objetivo del perfil falso. En cada RT o tuit utiliza un lenguaje informal y cae en la utilización de insultos.

Replica mucho contenido y al mismo tiempo utiliza fotografía o memes acompañados por frases de odio o de sátira. Obtiene mayor reacción los tuits que enlazan a otras publicaciones de medios masivos. Los usuarios reportan bastante uso de la opción de RT y

poca utilidad de respuesta. Sin embargo, la cuenta falsa reporta respuestas eventuales hacia las publicaciones. La cuenta en la actualidad se encuentra en inactividad. Pero causó revuelo en el 2016 durante las sesiones de declaraciones por los casos de 2015.

Según los resultados de TwitterAudit



Lo califican con un 98% y reporta tres perfiles falsos en sus seguidores.

Este tipo de perfiles demuestran cómo crecen orgánicamente por el fin o temática que manejan. Todos los perfiles analizados son catalogados por TwitterAudit como efectivos y “reales”, sin embargo hay que aclarar que esto es por razones de agendas y comportamientos.

Para complementar el análisis de los perfiles falsos se realizaron entrevistas a expertos del tema y se logró definir el comportamiento, prácticas de interacción y comunicación que desarrollan, así también se determinó que existen dos tipos de capacidades de influencia.

Los comportamientos de la web van de la mano con la educación que se recibe o bien del conocimiento que se tenga. Cuando se habla de seguridad en la web se enfoca en el conocimiento que se tiene sobre los riesgos, desventajas, ventajas y beneficios que se pueden obtener cuando se interactúa o se actúan en ella.

- Luis Assardo: periodista y asesor informático

Indica que los límites en la web no existen sino hasta que el conocimiento ya no alcanza para seguir navegando o para manejar temas de seguridad. "Entre más conocimiento tenga mayor capacidad y más cosas podré hacer. Como la ley de la selva cada quién tiene sus capacidades pero quién conoce más de tecnología podrán hacer muchísimas más cosas sobre el tema y aprovecharse de quienes no saben".

Añade que por esta razón es importante implementar educación sobre la web, dar a conocer los riesgos que existen o lo que se puede lograr con ella, siempre y cuando se tomen precauciones. En la actualidad no hay un buen manejo, hay pocas personas capacitadas o que tengan el conocimiento y de estas muy pocas llegan a difundir, distribuir y restringir información o logran construir falsas percepciones o generar otro tipo de pensamiento humano.

Y no es solo educar sobre que se puede hacer con diferentes plataformas o herramientas, sino crear conciencia sobre esto. Tomando en cuenta que se requiere de una actualización constante conforme los avances tecnológicos. Existen ventajas y desventajas en la web pero no todas se conocen. "Robo de identidad, el acoso, cualquier tipo de agresión y el robo de información -contactos, número de tarjetas de créditos-", expone.

En la actualidad la mayoría de la humanidad tiene en sus manos una herramienta muy poderosa y depende de cada quién cómo utilizarla. En este sentido, explica: "En Internet hay una situación que puede ser ventaja y desventaja a la vez y es el anonimato. Ventaja porque supongamos que en algún lugar hay algún tipo de censura en cuanto un sistema de denuncias de cualquier tipo de abusos o violencia se maneja por vías anónimas. Pero hay gente que utiliza el anonimato para hacer daño. Entonces cualquier persona en vías anónimas puede estar haciendo daño que no hay manera de detectarlo, perseguirlo o procesarlo".

Acá en Guatemala no se ha accionado mayor cosa sobre la seguridad de los ciudadanos en la web. No hay formación de criterio y muchos actos que se comenten en el país por medio de redes sociales son delictivos y esto no se está regulando. No hay una ley 100% sobre la

regulación de delitos en Internet. "Un ejemplo es el artículo de la libre emisión del pensamiento, habla de difamación, calumnia e impugna pero no hay nada proveniente de algo que se viva en Internet. Si alguien roba una identidad, calumnia en internet no hay legalidad que respalde acusaciones o delitos y mucho menos que lo procesen. Es decir, estamos descubiertos en la parte formativa y en la parte legal", añade.

Por estas razones la identidad digital está en riesgo porque se expone de tal forma que puede ser vulnerable para muchos actos mal intencionados. Por su parte explica que se puede crear en menos de cinco minutos un perfil de una persona para suplantarlo y el resto de personas no formadas no sabrán quién es quién, no sabrán diferenciar y muchos se aprovechan de eso.

Respecto a los términos y condiciones de privacidad y seguridad responde que en el ciberespacio no existe la privacidad, hay ciertas restricciones pero no es suficiente porque al colgar una foto a Facebook con fuertes restricciones de privacidad, se está subiendo a la base de datos de esa red social y ellos como empresa les conviene porque los datos personales son rentables para analizar el comportamiento humano. "Cualquier empresa le conviene dejar el Internet libre, no educar a la gente y dejar que las personas se comporte como se comportan y así aprender que es lo que hace la gente y luego presentarle un servicio para y por lo que hace la gente", explica.

En Guatemala han existido varios casos y el más alarmante es sobre la pornografía infantil. Por lo que Assardo comenta: "...vemos a niños de 8 o 9 años que tienen una cuenta en Facebook y esta empresa precisamente tiene como edad permitida 13 años en adelante. Entonces nosotros mismos estamos exponiendo y vulnerando a los menores de edad por decirlo así, porque no tienen criterio adecuado, ni tienen una capacidad de discernimiento para detectar si una persona es buena o es mala. Por lo mismo, crean perfiles, se contactan con niños, les extraen información y con eso pueden hacer lo siguiente: les puede pedir fotografías, los pueden exponer... si viene un pederasta y manda una fotografía desnudo a un niño/niña, solo ahí ya está abusando de infante porque los niños no tendrían por qué estar viendo ese tipo de contenido".

En el marco del comportamiento de los perfiles falsos, Assardo responde que para detectar un perfil falso hay varias formas, pero para la creación de perfiles indica: "la censura, la manipulación de información y cualquier tipo de abusos en redes sociales, es necesario crear cuentas masivas, para eso necesito una máquina que es capaz de crear varios perfiles por minuto que puedan hacer lo que yo indique, eso cuesta aproximadamente \$ 40,000 por licencia mensual, es por eso que en Guatemala todavía se hace de manera manual. De manera manual yo tengo que crear correos, validar cuentas, abrir cuentas, meterme y buscar imágenes en internet y robarla".

Agrega, "verificar la imagen de perfil, al ingresarla en Google yo puedo comprobar si esa imagen ya existe... los comentarios se notan que no son pensados, son hechos a la carrera. Si uno agarra un tuit corto de este tipo de perfiles, en el caso de Twitter, lo meten en el mismo buscador de la plataforma, le va a parecer cuantas cuentas tienen el mismo tuit y ahí es donde uno se da cuenta cuantas cuentas tienen la misma publicación y en el mismo tiempo, eso es imposible por más instantáneo que sea el Internet".

Acerca del comportamiento inicial, estos perfiles empiezan a seguirse entre cuentas falsas y esto puede ayudar a detectar una cadena de este tipo de cuentas. Regularmente tienen una agenda específica, dan *likes* y compartir publicaciones al mismo tiempo, no tienen identidad propia, atacan comentarios de otros usuarios. "Son como un rebaño que alguien les dice a dónde dirigirse y ellos obedecen".

El origen de estos perfiles puede ser por empresas que manejan crisis o comunicación en internet. No existe una persona individual que pueda armar su propio equipo, puede tener un grupo pequeño pero si quiere hacerlo de manera masiva hay empresas que se dedican a eso. En el caso político, "subcontratan por seguridad y por costos, sale más barato y si llegan a detectar este tipo de movimientos el político se puede llegar a desligar porque no fue propiamente él el que efectuó el movimiento de perfiles".

Expone que Facebook ha tomado acciones sobre estos actos, pues creó restricciones que si alguien no las sabe y tiene intenciones de crear cuentas falsas, estas serán botadas por la misma plataforma porque no cumplen con los requisitos establecidos. "Al ponerle -Luis

Assardo- Facebook en milésimas de segundos puede detectar si ese nombre existe y si es real. Si en caso yo no le pongo un nombre real pues me pide otro tipo de validaciones como mi número de teléfono o un correo o algo singular. De una forma u otra van dificultando... En Twitter ya lo implementaron, solo que ellos agregaron que si de una misma ubicación por medio del IP se detecta dos cuentas creadas al mismo tiempo bloquea".

Este tipo de perfiles sirven para establecer agendas, hacer tendencias -influenciar-. "Pueden monitorear, acosar y atacar". En esta práctica existe otro factor más común y difícil de detectar, la censura de contenido. Un perfil puede establecer un tema pero atrás de eso hay cientos de perfiles que pueden ahogar la publicación con millones de publicaciones atacantes o contrarias a lo publicado. En el marco político funciona para implementar campañas negras.

Estos acontecimientos les afectan a las plataformas de redes sociales porque ellos mantienen una base de datos donde pueden analizar el comportamiento humano y eso venderlo a las empresas. Al existir demanda de perfiles falsos esa base de datos se ensucia pueden caer en falsas percepciones y estar lejos de la realidad.

"Hay empresas grandes que tienen un espacio de análisis y monitoreo, no con fines de violencia o ataques, simplemente porque necesitan estar enterados de que es lo que está ocurriendo. Casos de vigilancia, algo que normalmente hacen los gobiernos. Y en estos casos agarran grupos específicos: periodistas, propósitos, ciudadanos involucrados a espacios de oposición política o algo por el estilo", en respuesta sobre el uso de perfiles falsos por parte de sectores de poder. Mientras que en el marco político los utilizan para posicionar temas, balance de opiniones y campañas negras.

Para regular este tipo de acciones existen tres iniciativas: 4055, 5153 y la CSIRT-GT. Esta última, según Assardo la considera ilegal: "es ilegal y en esa hablan sobre la ciberdelincuencia o delitos cibernéticos. Lo que están haciendo con eso es empoderar a una entidad – Equipo de Respuesta de Incidentes de Seguridad Informática- (CSIRT-GT). El asunto con esto es que es una identidad del Ministerio de Defensa, obviamente es militar, pagado por ellos y estas iniciativas de ley proponen que esta identidad se convierta un tipo

CEA como en Estados Unidos, donde puedan intervenir en el Internet, sin necesidad de una solicitud judicial sino que si ellos detectan una situación amenazante hacia Guatemala se meten a cualquier perfil y empiezan a indagar sin tener restricciones y no hay quién lo regule a ellos".

Acerca de la comunicación que se establece en el perfil falso responde: "Sí llega afectar en cuestión de percepción, en posicionamiento de temas y si es con intención de atacar será capaz de inundar y censurar la información". El perfil utiliza un lenguaje específico respondiendo a la agenda que maneja y puede llegar a causar impacto de cierta manera. "...regularmente perfiles agresivos, hay otros que son para posicionar temas y estos no responden si uno les habla o responden muy tardíamente, aparecen mensajes en orquestas, masivos y al mismo tiempo. La mayoría solo se dedican a dar share o RT y darle *like*".

La efectividad de interacción es menor porque hay perfiles falsos creados por empresas que no tendrán la capacidad de estar atentos a responder, son demasiados para lograr una interacción alta. "Pero si yo hice dos o tres perfiles para atacar directamente a una persona obviamente voy a estar atento a esos perfiles y la respuesta es más inmediata y persiguen mantenerse anónimos".

Para poder lograr cambiar una idea se necesita un perfil potente y darse a conocer bien en las redes sociales, menciona el ejemplo del perfil de @DictaLord: "Él tenía 35,000 seguidores y como el pasaba publicando temas constantemente la gente tenía confianza en él. Capaz de posicionar temas de situaciones de desinformación o mala información o alguna difamación o calumnia, la gente lo creía. Pero si hablamos de una cuenta con tres o dos seguidores, no impacta en nada. Para eso están los net-centers".

Esto representa una amenaza para la ciberpolítica siendo capaces de crear rumores, publicarlos en los perfiles falsos y hacerle llegar la noticia masivamente, esto ocasiona que los medios de comunicación anden hablando sobre el tema.

Manifiesta que los perfiles falsos no solo pueden desviar la opinión pública sino que arruinar la reputación de alguien. "Estos linchamientos digitales pueden llegar a afectar a una persona haya hecho o no algo negativo.

Digamos en el caso reciente del Congreso o en el caso del Presidente, su reputación está a 0, ya pasó la etapa de linchamiento y llegó a la etapa donde las personas ya no soportan ver ni a diputados, ni al presidente".

Este tipo de perfiles pueden llegar a ser herramientas de poder para la ciberpolítica pero como complemento de otras herramientas. Hay que recordar que en Guatemala a pesar del nivel de conectividad que se tiene hacia el internet es alto, existen sectores que todavía no tienen ese tipo de acceso o ignoran la existencia o uso, por esta razón si un tema, suceso o acción que pase en las redes sociales, el impacto será diferente en las plataformas y en la vida real.

El sector político no debe de olvidar que pueden existir sectores que tengan los mismos mecanismos para contraatacar. Tienen menos posibilidades pero las hay. Según las capacidades y el financiamiento que se tenga podrán desarrollar este tipo de juegos.

"Cualquier organización o sector lo que quiere con estas prácticas es posicionar pensamientos y es parte de la naturaleza humana. Pero tampoco no van a invertir en recursos ni en eso, es bastante difícil que un sector social utilice estos métodos, a menos que tenga intenciones políticas".

En la pregunta: ¿Qué más se puede lograr con el uso de perfiles falsos en la ciberpolítica?, Assardo menciona:

- "En Estados Unidos llaman la destrucción de reputación como asesinato de carácter o de personalidad. Eso yo lo bauticé como sicariato digital, pensemos en los sicarios que son contratados para destruirle la vida o matar a alguien en la vida real, en Internet sucede lo mismo, obviamente no lo van a matar físicamente pero sí van a matar su reputación y cuando eso sucede difícilmente se puede levantar o recuperar. Aquí en Guatemala hay gente que lo hace".

- "El de Dictalord. Es un perfil que está privado actualmente y no se puede ver nada de lo que había antes, pero en la publicación que hizo Contrapoder sobre este perfil ahí sale toda la información".
- "Rodrigo Polo, es acusado por diferentes sectores de tener un ejército de perfiles para posicionar distintos temas. Además que él públicamente lo hace".
- "En el caso de las elecciones del 2011, yo trabajaba en el Periódico y en ese entonces era por correo que se posicionaban temas de manera anónima por medio de las famosas cadenas. Por medio de eso se podía monitorear e incidir, pero fue hasta en el 2015 que expertos asesoraron para llevar ese tipo de prácticas a las redes sociales aprovechando lo instantáneo que se puede publicar y hacer viral".

En la actualidad los políticos no utilizan de buena manera las redes sociales y para eso subcontratan empresas que los ayudan a crear campañas pero no logran provocar incidencia, sino que solo logran crear falsas percepciones. El político no entiende todavía cómo funcionan las redes sociales, ni está bien asesorado, esto provoca que las campañas en redes sociales no tengan mayor éxito.

Guatemala sí tiene potencial para realizar campañas en redes sociales y al mismo tiempo se puede llegar a las personas por ese medio, sin embargo requiere de mucha educación, no solo por parte de los ciudadanos sino de los políticos, porque en ambas partes hace falta criterio.

Las redes sociales son ahora una herramienta importante para la implementación de la comunicación política en la sociedad. En el caso de Estados Unidos sobre Barack Obama y Donald Trump, políticos que han implementado el uso de redes sociales para acercarse a las personas.

Es cuestión de establecer una estrategia clara y no solo ejecutarla sino que mantenerla. El intento de establecerlo en Guatemala durante el 2015 dejó muchas deficiencias según el ejemplo que da a conocer: "LIDER contrató campaña negra para hacerle a sus opositores, contrató para hacer su campaña para él y con una campaña de #NoTeToca lo botaron y él gastó millones y millones de dólares en eso. Otros candidatos pudieron capitalizar lo que la

gente pensaba pero no lo supieron hacer. Se negaban a abrir perfiles o los abrían y les decía a alguien más que lo manejara y ese es un gran error porque no aprovechan estar en contacto con la gente como primera línea y entender lo que la gente quiere".

Respecto a la pregunta: En el 2015 se generó el "rumor" de la implementación de estructuras informáticas encargadas de generar contenido político en redes sociales. ¿Considera que este es el nuevo juego del sector político?, responde:

"No es nuevo, porque el manejo propiamente de reputación digital o identidad digital existe hace rato. Antes lo hacían grandes empresas pero hoy está a la mano de todos hacerlo. Pero acá lo importante es la incidencia y saber hacerlo y eso es cuestión de conocimientos y saber bien lo que se está haciendo. Yo puedo tener muchos clics pero sin incidencia eso no me funciona".

Esto indica que en ese año parte del financiamiento de los partidos políticos era destinado para el manejo de redes sociales, sin embargo se convirtió en un juego sucio donde se manipulaba, generaba malas intenciones, desviación y manipulación de percepciones, y campañas negras entre candidatos. A pesar que la reputación e imagen de cada figura política estaba en juego no evitó que se convirtiera como estrategia central.

En la campaña de UNE en la cual participó Assardo, indica: "La campaña de la UNE fue el caso que a pesar de la estrategia global que se tenía en redes sociales la estrategia que se utilizó fue humanizar a la candidata. Yo puedo estar todo el tiempo trabajando en una idea pero si esta no es buena no va a servir de nada. Lo importante es saber que se quiere hacer".

El uso de *net-centers* en Guatemala no es ilegal pero sí es ilegítimo y eso lleva a la parte ética. "... es algo nocivos y como son anónimos y no están regulados se pueden prestar para hacer campañas negras, destruir reputación, acoso, monitoreo y vigilancia de manera clandestino. Llegar a hacer varias cosas negativas", explica.

- María Mercedes Zaghi: Ingeniera en Sistemas y experta en Seguridad Informática

La pornografía infantil es un caso muy alarmante en Guatemala pero es porque existe ignorancia en la sociedad sobre el uso de Internet. "Uno tiene que saber lo que está haciendo y protegerse de lo que hace, así como uno hace en la vida real. Yo no me voy a meter a un lugar que sé que hay muchos asaltos, tengo que resguardar mi vida, es lo mismo en la vida virtual. Lo que pasa con esto es que tenemos que tener más educación, entender y hacer" expresa.

Otro elemento que entra en juego es la libertad de la sociedad por eso es importante darle a conocer a la gente hasta donde se puede llegar en la web, sin un sentido de restricción, solo como precaución. "... es de regular y más que eso entender y comprender cómo se actúa, en el caso de los *fakes news* o perfiles falsos y de ahí advertirle a la gente que existe lo malo y resguardarse de eso. Educar para autorregular el uso de las redes sociales", agrega.

En cuanto a temas de seguridad en el ciberespacio, regulación y protección en Guatemala se cuenta con un Consejo Nacional de Seguridad, sin embargo este no agrega este tipo de temas por lo que el Ministerio de Gobernación a través del Viceministro de Tecnología, Luis Ruíz está trabajando para formar el Consejo Nacional de Ciberseguridad. Esta propuesta de ley ya se encuentra en el Congreso de la República, manejada por el diputado José Quintanilla. "Sobre todo para manejar temas de la vulnerabilidad de los niños, trata de personas y esos actos que se han ido manifestando en la actualidad", comenta Zaghi.

En el ámbito de la educación, la entrevistada habló sobre los proyectos educacionales que abordan el tema de la información y el manejo de la web: "nos acaban de aprobar un programa de Tecnología de Niños que ya es parte del pensum. Siempre hemos dado mucha presión en ese tema y creo que han hecho su mejor esfuerzo, pero hay que recordar que son más de 40,000 escuelas y eso es un reto, pero se ha trabajado en ello".

Agrega que la sociedad le da mucha confianza al Internet y al momento que un link llega al correo o red social, muchas personas lo abren sin hacer una previa investigación cuando no saben que existen herramientas o sitios web que orientan sobre el nivel de confianza de

distintos espacios cibernético y para tratar temas más importantes existe una ciberpolicía y no todos saben sobre su existencia.

Sobre la pregunta: ¿Cree que algunos sectores de poder se aprovecha de esta cierta vulnerabilidad de la web?, responde: "... hemos detectado personas que están tratando de influenciar a otras personas sin sustento y eso es parte de la auditoría social y que se está haciendo porque ahí volvemos a caer en los *fakes news* que eso es un fenómeno nuevo que hasta ahora conocemos y puedan ser que estén manipulando y más en elecciones".

Manifiesta que se ha trabajado para regular y mejorar la legislación para el control judicial de estos actos cibernéticos:

"Esto lo estamos viendo en la Comisión Nacional de Comercio Electrónico, ver que no haya falsedad sobre todo en el tema financiero. También el 2008 apoyé una ley sobre el tema de comercio electrónico de aceptar las transacciones electrónicas en Guatemala y por eso mismo estamos trabajando con el Ministerio de Gobernación la ley en contra de la Ciberdelincuencia porque se dejó parado desde el año 2008 para acá. El tema de privacidad está parado y por eso estamos trabajando mucho en la comisión para tratar estrategias de educación y establecer que se puede y que no se puede hacer. Esta mesa es la primera y la armamos para saber que otras leyes necesitamos en relación al tema, empezando con la ciberdelincuencia y la seguridad de transacciones.

De igual manera a pesar de leyes y regulación no se puede lograr controlar todo el ciberespacio, esto va avanzando todos los días. Por lo mismo es importante que todos los sectores involucrados estemos en pro al cambio, capacitarnos sobre esos cambios y estar informados.

En el sector judicial se está haciendo lo posible por tratar estos temas, pero es algo tardado porque la mayoría que lo conforman es de la generación pasada y no nacieron con la tecnología, por eso es importante capacitarlos para que se agilicen este tipo de casos.

Guatemala ya es un país tecnológico, hay potencial y talento en las personas, por eso es importante apoyarlos y empujarlos para que avancemos. Sin embargo, tenemos a un Congreso que desconoce del tema de tecnología por eso es la lentitud, es cuestión de empaparse del tema".

Respecto a la pregunta: A nivel política, ¿cree que utilizan los perfiles falsos a su favor?, responde: "Yo creo que sí, algunos con buena intención y otros con mala. Pero también depende de que nosotros seamos capaces de detectarlo, saber hacerlo, como te decía hacer un chequeo previo".

Por esta razón recomienda la necesidad de que los periodistas comprueben la información publicada por las redes sociales antes de difundirla como "noticia". Ahora no se sabe en qué momento pueden hackear la cuenta del Presidente de la República y lo publicado puede ser información falsa. No tener como primera fuente las redes sociales.

Experiencia de un político en el implemento de redes sociales

Se ahondó sobre las campañas políticas creadas para redes sociales en Guatemala. Para esto se sumó Jorge Marroquín, candidato a alcalde del municipio de Santa Catarina Pinula en las elecciones del año 2015.

- Jorge Marroquín:

Responde que para saber que si un político usa de buena manera las redes sociales "habría que definir que es buen uso pero igual creo que las redes sociales son el canal más directo que está actualmente de moda para transmitir cualquier información sobre su vida cotidiana. Y es el canal que han encontrado los políticos para poder manifestarse ante la sociedad. No es el buen uso sino la capacidad que se tiene para poder llegar transmitir un mensaje a través de las redes sociales".

Considera que Guatemala es un país donde el uso del celular y de las comunicaciones por vías de redes ha crecido bastante y ha superado el número de celulares comparado con el número de aparatos y actualmente se ve que el uso de datos es lo que realmente se está

cobrando porque es lo que más se tiene. Sí se está preparada y sí le da bastante uso a las redes.

"Las redes sociales han tomado una preponderancia bastante importante en la sociedad y prueba de eso las campañas de publicidad que han sido utilizadas también por los políticos ya que nos garantiza llegar a cierto sector, a cierta distancia y poder medir cuanta gente vio el mensaje, cuanta gente lo compartió, cuanta gente le dio like. De una u otra forma es el canal más importante".

En cuanto a la pregunta "¿Cuál es la dinámica de una campaña política en redes sociales?", responde: Una inversión poco costosa y que sí garantiza llegar al target o al electorado. Se puede medir cuanta gente y en que radio territorial llegan a percibir el mensaje ya que se garantiza el uso de la publicidad y así mismo las modalidades que actualmente ya se han implementado como las transmisiones en vivo que ayudan a publicar una actividad de manera instantánea.

Manifiesta que la red que más utilizaron en su campaña fue Facebook y pudieron calcular el alcance, siendo a su gusto la mejor opción para llevar a cabo una campaña política a comparación de otros medios más convencionales como vallas o volantes. Agrega que con este tipo de plataformas se pueden alcanzar más persona con un menor costo y en menor tiempo.

Respecto a la pregunta: En el 2015 se generó el "rumor" de la implementación de estructuras informáticas encargadas de generar contenido político en redes sociales. ¿Considera que este es el nuevo juego del sector político?, responde:

"Sí, el uso de redes se utilizó a nivel de todo los candidatos, fue muy importante y hasta cierto punto no me afectó el implemento de cuentas falsas pero sí creo que se manipuló cierta información, pero no hubo intervención directa en utilizar un perfil falso en cuanto a mí....

Pero sí hubo implementación de perfiles falsos como estrategias de campaña negra por lado de otros sectores. En ellos se copian fotografías, nombres de usuarios que

son sumamente parecidos y algunos no diferencian entre realidad y un uso de parodia de un perfil falso. Desinforman y eso es preocupante porque la política es imagen y al destruir la imagen es muy difícil volver a construirla y más a base de estos métodos.

Creo que el participar políticamente activo en unas elecciones es un ejercicio ciudadano y me deja mucho. Estoy consciente que es algo que realmente exige bastante tiempo, bastantes costos, así como la creación de un equipo bastante comprometido con el objetivo principal.

El uso de *net-centers* es algo lamentable para Guatemala, no le conviene que esto crezca porque esto provoca una polarización entre la sociedad a través del mal uso de la información y tocando temas personales sobre alguien. El anónimo expresa que es un montón de trucos, trampas, mentiras para el impulso de un producto o la destrucción de un producto”.

Experiencia de un "netcentero"

Este fenómeno nuevo es importante estudiarlo, no solo a nivel informático o tecnológico sino más allá de eso. Hay que recordar la capacidad de la web, más que eso puede llegar a modificar comportamientos humanos, generar nuevas formas de comunicación, manipulación y persuasión. Así como mecanismos políticos, económicos, mercadológicos entre otras cosas más.

Para determinar estas nuevas formas comunicacionales actuales primero hay que entender el comportamiento y de ahí analizar la persuasión o reacción que causan estas nuevas dinámicas de interacción en la red. En el caso de los perfiles falsos entender y comprender cómo actúan, qué herramientas usan, cómo reaccionan y cómo se forman.

Con el objetivo de ahondar sobre este tema se acudió a una persona que fue Jefe de Campaña de Otto Pérez Leal durante el período de elecciones en el 2015, por razones de confidencialidad no se presentan datos personales del entrevistado.

Expone que cada vez más se ha perfeccionado la creación de perfiles falsos. "A nosotros nos asesoró un grupo que fueron los encargados de redes sociales de Peña Nieto, se llama DC Estrategia y el que vino fue precisamente el estratega de la campaña de Peña Nieto, se llama Simón Coin... ellos ya habían logrado perfeccionar los perfiles falsos porque todavía en Guatemala están muy en pañales".

Normalmente los perfiles falsos cuando empiezan en redes como Facebook o Twitter se enlazan con otros perfiles falsos o a publicar y responder con el discurso que van manejar o el mensaje que quieren dar conocer. Segundo, siguen a las cuentas oficiales de medios de comunicación que ahondan temas políticos o páginas de los partidos políticos o de alguna figura política. Se convierten en vigilantes. En algunos casos pueden ser net-centers o en otros son personas reales escondiéndose a través de un perfil falso para exponer lo que no pueden hacer públicamente.

"Buscar la mayor parte de seguidores que puedan conseguir o seguir a la mayor cantidad de gente objetivo del perfil, si el objetivo es político es seguir a políticos, si el objetivo es comercial, perseguir gente con el mismo perfil. No se socializa directamente y si se hace tiene que ser entre perfiles falsos... pero eso es de conocerlo poco a poco".

El objetivo de los perfiles falsos es para influenciar y crear otras percepciones. "Se ha convertido en un negocio y están involucrados muchos sectores de poder porque esto se logra a través de un gran financiamiento, es imposible hacerlo de manera individual... tener a personas para que estén ocho horas sentadas, monitoreando y atacando... y eso hay que remunerarlo".

No se han visto acciones sobre esto por parte de Facebook o Twitter porque no solo es un negocio político, es un negocio mercadológico. Para fines publicitarios es conveniente pues los productos y servicios alcanzan a miles y miles de usuarios en la red, no importando si son verdaderos o falsos: "la mercadotecnia son números, cuánto es mi potencial de llegarle si yo anuncio en Facebook, no es lo mismo que decir cincuenta mil personas que sean los perfiles verdaderos, entonces para ellos son números".

A nivel político el entrevistado indica que es un juego que se practica mucho en Guatemala. Últimamente los perfiles falsos han servido para atacar, no para la construcción de imagen sobre algún tema o sobre alguien. "El problema acá de todo esto es que no hay regulación. Nosotros actuamos sin ningún problema, nos aprovechamos de eso... se ha intentado muchas veces generar leyes sobre esto pero no llega más que al tema del acoso. Nadie está interesado en esto porque son los mismos del gobierno que actúan bajo estos perfiles. No solo ellos, pero también forman parte de esta práctica".

Es un negocio rentable y que muchos lo utilizan para crear campañas contraste, las famosas "campañas negras". No hay que ir tan lejos y darse cuenta que los mismos del gobierno están involucrados en ese juego o entre pequeños grupos políticos como sucedió en el 2015.

Entendido el comportamiento se definen las dinámicas de comunicación, el lenguaje que manejan y cómo interactúan en las redes sociales. Según el entrevistado anónimo para poder establecer un lenguaje hay que saber para qué grupo va dirigido y cuál es el mensaje que se quiere dar a conocer. Es como vender un producto o una idea. "Hablar como mujer si es para mujeres, hablar como señoras si es para señoras".

Sin embargo considera que en Guatemala no existe organización en ese sentido, cualquiera crea un perfil falso y tira comentarios agresivos, sin sentido, ni criterio. Por lo mismo la interacción de un perfil falso y un perfil real no es tan efectiva porque el primero solo está para atacar. Hay ciertos casos en los que sí puede llegar a alcanzar cambios en percepciones: "es lo que hicimos para lograr aumentar porcentajes de votantes. Desprestigiar a un candidato a alcalde en específico para modificar la percepción que la gente ya tenía sobre él".

En cuanto al nivel de impacto el entrevistado señala que no confía en las estadísticas que se han hecho en Guatemala porque considera que el impacto se queda en donde se generó, en las redes sociales. Los perfiles falsos pueden llegar a cambiar percepciones, manipular e influir en la opinión pública pero incidir es difícil. La vida virtual con la vida real hay una gran brecha. "La persona que nos asesoró nos advirtió que con implementar los perfiles

falsos íbamos a ganar las elecciones, lo mucho que se puede lograr son cambio de percepciones acerca de los candidatos".

La comunicación que se establece en los perfiles falsos es capaz de modificar ideas, modificar pensamientos, cuestionar y mal informar.

Se ha mencionado varias veces que la ciberpolítica está expuesta a estas prácticas por parte de distintos sectores -políticos y sociales- que luchan por empoderarse e influir para generar cambios de percepción y opinión pública pero más allá de eso pueden llegar a ser capaces de cambiar o destruir la reputación de alguien, en este caso de un político, candidato o entidad pública.

Expresa que los perfiles falsos llegan a desprestigiar a una figura política y al ser expuesta masivamente esto provoca que los usuarios que están altamente conectados se la crean. Sin embargo esto trabaja bajo la lógica de masas y no en la lógica individual, por esa razón las redes sociales son complemento de todas las herramientas para crear una campaña política y no la principal. Muchos piensan lo contrario y es donde fallan y sufren pérdidas.

Sin embargo, actualmente le están apostando mucho a este tipo de prácticas. Grandes financiamientos se vienen en camino para desarrollar estructuras dedicadas a generar espacios de ataques cibernéticos sobre percepciones políticas, afirma el entrevistado anónimo. Apuesta que es un gran negocio para el sector político.

Acerca de la pregunta: ¿Se pueden sabotear a sectores políticos a través del uso de perfiles falsos?, responde que es poca la probabilidad que eso suceda, pero si se quiere sabotear alguna decisión política no basta solo con el uso de perfiles falsos en las redes sociales sino un conjunto de todos los medios masivos que existen hoy en día, como sucedió con Otto Pérez Molina.

En la pregunta: ¿Qué más se puede lograr con el uso de perfiles falsos en la ciberpolítica?, menciona:

- "Primero hay que entender que el uso de perfiles falsos no es la única tarea que hay que hacer, sino que es una de todas. Porque si se mide el grupo objetivo con el que se quiere trabajar sobre las capacidades de conectividad, analfabetismo, patrón electoral, etc., se van contrarrestando las posibilidades de la efectividad de las redes sociales".
- "Por ejemplo Mixco que fue el territorio donde yo trabajaba, allí terminamos descubriendo que el 65%, 70% de la población no tenía acceso a teléfonos inteligentes por lo tanto no tenía acceso a Twitter ni a Facebook y de ese 65% el 80% eran votantes de las elecciones. Quiere decir que solo el 20% de la población de Mixco tenía acceso a redes sociales, entonces nosotros estamos dirigiéndonos a 20% de la población gastando un montón de recursos".

El político actual no sabe utilizar las redes sociales: "está perdido, creo que no entienden todavía, es por la vanidad, al político el problema no se le puede decir no porque además es el que paga entonces se -paniquea- y hay que hacer lo que ellos digan sencillamente.

Considera que existieron excelentes trabajos en algunos *call center* de partidos políticos. "El de la UNE estuvo trabajando muy bien. El de Baldizón era terrible no sabía ni qué hacer, no tenían estrategias. El problema no solo fue el *call center* o el *net-center*, sino la estrategia en general quien la trabajó no sabía lo que estaba haciendo.

Con orgullo lo puedo decir que en Mixco lo trabajamos muy bien, las circunstancias eran otras y esa es la prueba, las mejores redes sociales las manejamos nosotros y no ganamos por qué, porque el asunto político prensa, televisión y radio eran distinto y muy negativo a pesar que ganamos en redes sociales en cuanto calidad, mensaje, proyección grupos sociales a los que llegamos y la cantidad de votantes que logramos jalar pero no pudimos con los medio masivo".

Respecto a la pregunta: En el 2015 se generó el "rumor" de la implementación de estructuras informáticas encargadas de generar contenido político en redes sociales. ¿Considera que este es el nuevo juego del sector político?, responde:

"No es tan nuevo, ya viene desde hace algunos años, lo que pasa es que no lo habían volteado a ver sino hasta la campaña anterior cuando para variar los gringos nos dieron una lección de mercadotecnia porque realmente quienes manejaron toda la campaña alrededor en contra de Otto Pérez y Roxana Baldetti fueron los gringos. Incluso la generación de información y contenidos venía hasta de EEUU, ósea allá le pusieron sus centavitos los mismos gringos y ellos fueron quienes generaron toda esta estrategia. Quienes estaban financiando algunos de los net-centers que estaban dedicados exclusivamente para atacar a Otto Pérez y Roxana Baldetti eran USAID".

El implemento de un *net-center* para una campaña política conlleva más inversión, más tiempo y organización. Según la experiencia del entrevistado anónimo, comparte:

"las instituciones oficiales ya demostraron que son una fuente de dinero para contratar netcenteros... Yo tuve la experiencia de ver como desde una farmacéutica fueron contratados 5 personas. Estos netcenteros pueden tener contratos desde un 029 sin prestaciones pero bien pagado, sueldos de 12,000, 14,000 y así andaban los 18 netcenteros.

Una empresa privada no va a pagar eso, paga del sueldo mínimo en adelante, 3,500, 4,000. Otros –negocean- colaboradores, -este trabaja para mí pero te lo voy a prestar-. Reclutamiento a este tipo de cosas hay cuanta cantidad inimaginable.

En el equipo había 12 personas de manera formal, pero como colaboradores teníamos como 200, es difícil manejarlo porque son indisciplinados cuando solo están por colaborar. No se les puede exigir mucho. Les dábamos instrucciones por día, el mensaje que se quería dar a conocer, se planteaban metas diarias sobre impacto y alcance. Quiere decir que hay muchas dinámicas que se alimenta un net-center por lo mismo.

Es fácil, es barato y muy fácilmente se pueden encontrar colaboradores para replicar la información que se quiere posicionar, lo difícil es mantenerlo, procurar no cometer errores. En el caso nuestro sucedió que colocamos una foto que no era

nuestra y se convirtió en un escándalo porque salió la dueña de la foto a decirnos que éramos unos piratas.

Teníamos una base de datos como inventario de todos los perfiles creados y luego esta información fue eliminada por seguridad de todos”.

En análisis a todo esto se pueden detectar que los perfiles falsos encontrados son hechos de manera manual y por personas/usuarios que se esconden a través de la imagen de alguien más para poder realizar un escape de opinión, pensamiento o sentimiento. Por esta razón son fáciles de detectar y al mismo tiempo percibir que la aceptación de los seguidores se desarrolla por el contenido y temática que manejan.

El lenguaje es muy fácil de digerir, pues presentan dinámicas de comunicación comunes y corrientes que son amigables para la capacidad receptiva de cualquier persona que navega en internet.

Sin embargo, crean un espacio de mala información, discriminación y ataques que en cierta forma puede modificar las percepciones que se tiene acerca de la figura o personaje que presentan. Si no se tiene la educación necesaria y el uso adecuado es fácil caer en pensamientos cargados de odio, adoptarlo y formarlo parte de su comportamiento, criterio y opinión.

La capacidad de los perfiles de este estudio sobre la reputación de la imagen de las figuras política es mínima a comparación de otras formas de ejecutar como bien lo mencionaron los expertos entrevistados. Sin embargo, son capaces de ir alimentando con el tiempo un discurso de desprestigio, rechazo e información manipulada y el mejor ejemplo es el caso de @DictaLord, un usuario "común y corriente" que poco a poco fue introduciéndose en el Time Line de muchos usuarios en Twitter.

Es decir, que por el momento estos pueden verse débiles pero con el tiempo, entre más personas conozcan de ellos y se dejen llevar por las emociones que pueden llegar a causar, pueda que se esté conociendo futuros perfiles falsos fuertes. Por el momento se mantienen al tanto de las acciones de las figuras política y al tener antecedentes durante las elecciones

de 2015 es probable que en estos cuatro años los utilicen como preparación, capacitación, monitoreo o vigilancia y de esta forma mejorar sus ejecuciones para las próximas elecciones u otros eventos relevantes en la política.

V. Discusión de resultados

En base a los perfiles analizados y el punto de vista de cuatro expertos sobre el tema se desarrolla una discusión de todos los resultados confrontadas con términos y explicaciones anteriormente presentadas. Es necesario mencionar nuevamente que las cuentas analizadas son creadas con un fin de desvío de opiniones, polarización y ausencia de percepciones.

Como menciona Redondo (2016) sobre los usuarios falsos que pueden llegar a existir en la web, en el caso de los perfiles analizados son determinados como falsos ya que utilizan fotografías, imágenes, discursos de odio, de rechazo, de ataques o bien evangelizadores en referencia a las figuras políticas.

Vale la pena recordar que estos en la red pueden desarrollar comunidades a través del conjunto de nodos, sin importar el tipo de comportamiento, si es bueno o malo. La dinámica es la misma, los fines, los valores y característica son diferentes.

Esto mismo lo explica Sanz (2003) sobre el Análisis de la Redes Sociales <<ARS>> que no solo de interacción se trata sino de un espacio que es capaz de causar impacto en el comportamiento de los actores formando estructuras de poder.

Es decir que la capacidad de un perfil falso puede ser la misma capacidad que tiene una cuenta de una figura pública relevante. El mensaje o discurso son clave para que esto suceda, sin embargo existen tanta tácticas tecnológicas que no es imposible tener mayor alcance de una manera “bajo de agua”.

Como perfiles falsos más influyentes de todos los analizados se puede determinar que la cuenta referente a Jimmy Morales: @jimmymoriesgt, referente a Álvaro Arzú:

@Arzu_Tonatiuh / @Arzu_Alvarito, en referente a Patricia de Arzú: @LaDonaPatydArzu y en referente a Otto Pérez Molina: @OttoPerezMulona son los más afines a la explicación de Sanz. Las cuatro cuentas son las que tienen más seguidores, sin mayor movimiento e interacción.

Mientras Castells (2008) menciona que la comunicación socializada tiene la capacidad de influir en la opinión de las personas y esto se logra a través de los medios de masas. En este caso las redes sociales representan esa comunicación masiva y en el caso de de estos perfiles falsos analizados, la mayoría trabaja bajo esa la lógica.

Ejemplos de esto se pueden mencionar las cuentas referentes a Zury Ríos: @ZuryGuate, Neto Bran: @MixcoBran y Roxana Baldetti: @Roxanabalbote que lanzan mensajes de odio, halagos o insultos y los usuarios responden a esa misma línea.

Con esto es importante resaltar que el poder está en la red y el juego de poder puede estar en manos de cualquiera que tenga intenciones de influenciar o causar movimiento o algún comportamiento determinado. Muy bien lo menciona Castells sobre su concepto de: comunicación es poder. Si bien en la actualidad el uso de la tecnología, comunicarse por medio de diferentes tipos de herramientas tecnológicas hace que muchos lleguen a obtener poder.

Un perfil falso sobre cualquier temática, en este caso sobre una figura política provoca que llegue al poder o capacidad de causar confusiones, cambiar percepciones, engaños, rechazo, ilusiones o también que exista mala información acerca de un tema en específico.

La mayoría de perfiles analizados tiene como principal materia prima la burla y por esa razón están a la orden del día para fijarse sobre cualquier acción, expresión o publicación de la figura que hacen referencia. Capaces de manipular o tergiversar cualquier contenido para conseguir usuarios. El sentido sarcástico y humorístico engancha fácilmente con los usuarios, en especial en Guatemala este tipo de perfiles se han convertido como un escape y llegan a ser entretenidos con el contenido que manejan.

Sin embargo, hay otros que pueden llegar a provocar un ambiente tenso, este es el caso de varios de los perfiles. El referente a Iván Velázquez: @BobGramajo y en referente a Otto Pérez Molina: @OttoPerez_GT, son dos cuentas que construyen un ambiente de confrontación de ideas y ataques a diferentes publicaciones. Se comunican con un sentido masivo, obtiene poder e influyen para que los usuarios actúen de la misma forma.

Se ha mencionado que las plataformas sociales como Facebook o Twitter son herramientas informáticas y comunicacionales con una alta gama de acciones y reacciones, pero más que eso son canales en los cuales se pueden generar percepciones. Esto para la comunicación política puede ser ventaja y al mismo tiempo desventaja, porque se puede estar creando estrategias de campañas para redes sociales pero por el otro lado puede estar pasando exactamente lo mismo pero con objetivos negativos y mal intencionados.

Así menciona Túñez (2008) sobre el caso de Barack Obama sobre el éxito que reflejó la estrategia que llevó a cabo en las redes sociales. Caso contrario que existió en Guatemala durante la época de campañas electorales de 2015 y hasta la fecha con el manejo de redes sociales de Jimmy Morales, pues de todas las figuras políticas presentadas en esta investigación, es la que tiene más perfiles falsos.

Un ataque cibernético puede venir de cualquier lado, desde el mismo político hasta sus contrincantes u opositores. En este sentido hay que tomar en cuenta que el juego y manejo de perfiles falsos funciona para desviar, persuadir o destruir reputaciones, sin embargo, en el caso de Guatemala estos actos en la actualidad no tienen mayor relevancia por motivos de analfabetismo, conectividad al internet y accesos a aparatos tecnológicos, la posibilidades de impactar solo por redes sociales todavía corta.

En el caso de Zaghi y Assardo ambos coinciden que la pornografía infantil es el caso más grave que se ha manifestado en la web a nivel nacional. Han estado en distintas investigaciones donde logran mapear a pederastas y otro tipo de organizaciones delincuenciales.

Respecto a los perfiles falsos utilizados por personas comunes y corrientes, las cuatro personas entrevistadas, concuerdan que cualquiera tiene la capacidad de efectuarlos siempre y cuando tenga el conocimiento. Unos estarán mejor estructurados que otros, eso depende de la agenda y nivel tecnológico que manejen.

Por esta razón no es de extrañarse ver campañas o actos políticos realizadas de manera convencional a pesar de ser un país avanzado en tecnología. Los niveles de falta de acceso

tecnológico o ignorancia sobre el uso de la tecnología son dos factores que retan a Guatemala para ser reducidos. A pesar de que esto lo ven como conveniencia propia para muchos sectores de poder, al mismo tiempo se convierte en una desventaja si se tienen intenciones de ejecutar métodos tecnológicos para empoderarse aún más.

En el caso de los perfiles analizados en este estudio denota que los que manejan la parodia o sátira en el contenido que publican, utilizan un lenguaje ausente de semántica formal y esto mismo ayuda a que sea legible para cualquier persona que recibe el mensaje sin importar el nivel socioeconómico y educativo.

Es decir, que los perfiles falsos pueden ser aceptados con facilidad sin tener una verificación previa de la veracidad de usuario o sin saber diferenciar entre un perfil falso y oficial por la falta de conocimiento que se manifiesta actualmente. En otros casos, existe la posibilidad que muchos usuarios sigan a este tipo de perfiles por motivos de ocio y entretenimiento, pues en Guatemala la reputación de la política está en los suelos y esto alimenta aún más la percepción que se tiene.

Para el entrevistado anónimo los perfiles falsos son complementos y no una herramienta poderosa, mientras tanto Assardo y Marroquín manifiestan lo contrario al presentar ciertos dominios tecnológicos se pueden llegar a grandes masas y eso causar impacto. En el caso de Zaghi, expresa que depende el tiempo para sostener la mentira que se maneja en esos perfiles.

Por otro lado, tanto Assardo como el entrevistado anónimo y Zaghi explican que lo único que logran las redes sociales es la creación de percepciones sin causar incidencia y en el caso de los perfiles falsos provocan falsas percepciones y de igual manera sin causar incidencia.

Para lograr algún tipo de incidencia en la sociedad por medio de las redes sociales, es necesario que exista un sentir, una percepción común o un evento masivo. Tal es el caso del binomio presidencial de Otto Pérez Molina y Roxana Baldetti que se conectó el sentir de

intolerancia con la percepción de redes sociales, esto provocó la gran afluencia en la Plaza Central.

Los acontecimientos presentados en este estudio manifiestan que es necesaria la regulación sobre el uso de las redes sociales y el internet para y por el beneficio de todos. Es conveniente tanto para los sectores de poder como para la misma sociedad en sí. Esto ayudará a que se inicien capacitaciones sociales sobre el buen manejo, precauciones y las ventajas/desventajas del internet.

En cuanto a Zaghi considera que sí se ha trabajado para regular y controlar los actos delincuenciales en la web en Guatemala, mientras Assardo manifiesta que solo se han presentado iniciativas de ley ausentes de criterio y para el entrevistado anónimo no se ha hecho mayor cosa más presentar una ley sobre el cibercrimen. Sin embargo, los entrevistados concuerdan que es un trabajo difícil y lento en presentar resultados pues la educación sobre el uso y manejo de la web está por los suelos.

Siempre en el mal manejo de la web Zaghi, Assardo y el entrevistado anónimo consideran que los políticos no tienen un buen manejo en sus redes sociales y se dejan llevar fácilmente con propuestas publicitarias de distintas empresas para posicionarlos en la mente de las personas, sin embargo olvidan que ellos mismo necesitan del conocimiento para obtener un buen uso y alcance con las personas. Es necesaria la humanización de las figuras políticas, pues la reputación que se tiene en la mayoría de casos es mala.

Por otro lado, la libertad de expresión está en juego y en este sentido es necesario recordar que la utilización de la tecnología puede ayudar a alcanzar ciertas cosas que la "vida real" es imposible. Es cuestión de que se practique transparentemente y de manera auténtica sin acudir a juegos sucios que solo han dejado falsas percepciones que cada vez más separan a la sociedad con la realidad de las cosas.

Muy bien lo mencionan Temperini y Macedo (2015) que la creación y utilización de un perfil falso no contradice ninguna normativa vigente, sino que podría ser considerado como

una manifestación de la libertad de expresión y a modo general, representando una de las libertades más importantes que se pueden encontrar en Internet.

Asimismo Giones y Serrat (2010) recomiendan que hay que estar al tanto de lo que hablan las personas, en que sitios y de la manera en la que se desenvuelven en la red. Solo de esta forma se podrá conocer las intenciones de la opinión que difunden.

Analizar, comprender y educarse son acciones claves para lograr ser una sociedad netamente tecnológica. Desde gobiernos hasta ciudadanos, desde instituciones privadas hasta instituciones gubernamentales, desde adultos hasta infantes. Generar autoconciencia y autorregulación sobre la tecnología.

VI. Conclusiones

Luego de realizar el análisis del estudio se pudo llegar a las siguientes conclusiones:

- Sobre lo expuesto por los entrevistados y los hallazgos de los perfiles analizados se pueden evidenciar varios usos que manejan en este tipo de cuentas falsas. La suplantación de identidad, manipulación, creación de falsas percepciones, ataques a usuarios, denuncias sociales y descargas de odio/rechazo, son los usos más comunes que se pueden detectar.
- La mayoría de perfiles falsos manejan una línea de sátira y burla en referencia a las figuras políticas. Los discursos humorísticos se basan en discriminar, ofender e insultar a la entidad pública. Sin mayor criterio, lanzan burlas o contenido sarcástico sobre algún político. Sin dudarlo dos veces denuncian sobre hechos en su mayoría de veces sin fundamentos o verificación de veracidad. Esto provoca falsas percepciones o rumores en las personas que están expuestas a este tipo de contenido.
- Los mensajes que más se utilizan son el rechazo, el odio, la burla. En otros expresan halagos y apoyo. El mensaje depende del fin del perfil falso y del contenido que quiere dar a conocer. De los perfiles analizados son pocos los que logran mantener una misma línea en su agenda, en el resto se logra detectar que lanzan contenido que tengan a la mano con tal de que siempre afecte al personaje al cual está haciendo referencia. Por esta razón es difícil encontrar su camino a seguir.
- Respecto a las dinámicas de comunicación desarrolladas en los perfiles falsos analizados se puede mencionar que utilizan como primordial vía la escritura de tuits sin ningún material o herramienta multimedia. Las fotografías, memes, vídeos, enlaces a distintos sitios de internet son utilizados como complemento.
- La mayoría de perfiles enlazan a artículos de opinión o de contenido anónimo que narran algún caso en específico para lograr poner en duda la reputación del político otras veces resaltan publicaciones hechas por medios independientes o contra-sistema sobre algún político para sobresaltar las acusaciones o descubrimientos publicadas por estas agrupaciones.

- Los perfiles falsos desarrollan la comunicación a través de contenido multimedia muchas veces manipulado, en el caso de las fotografías y vídeos sobre las actividades políticas son acompañadas de textos que presentan una historia diferente a la publicación original que se realizó en las cuentas oficiales de las figuras o entidades políticas.
- En cuanto a las dinámicas de interacción, los administradores o autores de los perfiles falsos responden esporádicamente a los comentarios que reciben sus publicaciones. Las herramientas de reacción más utilizadas son las opciones de "Me gusta" y RT -retweet-.
- A través de los resultados de la aplicación de TwitterAudit se concluye que los perfiles falsos encontrados son creados por personas comunes y corrientes, sin alta intervención de aparatos tecnológicos como los que utilizan los net-centers. En el caso de los perfiles falsos manuales en su mayoría crecen orgánicamente al darse a conocer dentro de la plataforma Twitter y no suelen ser tan acosadores como en el caso de los perfiles creados por alguna agencia de información o publicidad.
- La reputación de las figuras políticas está en juego sobre estos actos, al ser influyente un perfil falso puede crear una falsa percepción o duda sobre su reputación o sobre la imagen sin verificar la veracidad de la información que se presenta. En este caso los políticos pueden estar al tanto sobre estos eventos pero no hacen mayor cosa más que quedarse en el mismo lugar. La falta de conocimiento por parte de los políticos hace que no existe una regulación o denuncia sobre estas cuentas que se hacen pasar por ellos de forma mal intencionada.

VII. Recomendaciones

- A. A los políticos actuales se les recomienda asesorarse con personas capaces de manejar las redes sociales o herramientas tecnológicas para que construyan una estrecha relación entre la sociedad y su persona. Manejar las cuentas de redes sociales por ellos mismo, sin tener subalternos digitales. Esto crea un ambiente de confianza, transparencia y autenticidad en la imagen del político.

- B. Los agentes de comunicación política tomar en cuenta que las crisis pueden nacer al ser expuestos a los ataques de perfiles falsos referentes a los políticos con los que trabajan o asesoran. Tener una guía de manejo de crisis para estos casos digitales y virtuales.

- C. Para los medios de comunicación se recomienda no dejarse llevar por las publicaciones de información importante sobre las figuras políticas en redes sociales hasta no ser comprobada y verificada. Sin previa investigación no proceder a publicar noticias en base a publicaciones en internet, pues no es conveniente tomarlo como primera fuente o fuente accesible.

- D. Se recomienda a la facultad de Humanidades abordar temas teóricos en la carrera de Ciencias de la Comunicación acerca de la ejecución, actuación y el quehacer de las manipulaciones que se pueden llegar a manifestar en internet y redes sociales. Saber entender desde la comunicación y análisis sobre el tema.

- E. A los estudiantes se les recomienda realizar estudios que aborden y ahonden sobre las percepciones que reciben los discursos que manejan los perfiles falsos para medir el nivel de impacto y persuasión.

Bibliografía

- Arribas, M. (2004). Diseño y validación de cuestionarios. *Matronas profesión*, 5(17), 23-29. Recuperado de: http://ebevidencia.com/wp-content/uploads/2014/07/validacion_cuestionarios.pdf
- Assardo, L. (2016). Sicarios digitales. Guatemala: BitViu, revista urbana. Recuperado de: <http://www.bitviu.com/2016/09/sicarios-digitales/>
- Assardo, L. (2016). ¿Cómo reconocer un #perfilfalso?. Guatemala: BitViu, revista urbana. Recuperado de: <http://www.bitviu.com/2016/09/como-reconocer-un-perfilfalso/>
- Assardo, L. (s.f). Seguridad Digital.
- Ayala, S. (2013). Internet y participación política: el caso del partido pirata alemán (Tesis de grado). Universidad Nacional Autónoma de México, México. Recuperado de: <http://132.248.9.195/ptd2014/febrero/305500030/Index.html>
- Bravo, A. (2003). Cibercrimen. *Direito e Democracia*, 4(1). P. 119- 143. Recuperado de: <http://www.periodicos.ulbra.br/index.php/direito/article/view/2449>
- Burch S., León O., Tamayo E. (2001). *Movimientos sociales en la red*. Quito, Ecuador: Agencia Latinoamericana de Información.
- Caldevilla, D. (2009). Democracia 2.0: La política se introduce en las redes sociales. España: Pensar la Publicidad. Recuperado de: <http://revistas.ucm.es/index.php/PEPU/article/view/PEPU0909220031A/152> 18
- Caldevilla, D. (2010). Las Redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual. España: Departamento de Comunicación Audiovisual y Publicidad 2 -CAP2. Facultad de Ciencias de la Información de la UCM. Recuperado de: <http://revistas.ucm.es/index.php/DCIN/article/view/DCIN1010110045A/186> 56

- Campos, F. (2008). Las redes sociales trastocan los modelos de los medios de comunicación tradicionales. Tenerife, Canarias; España: *Revista Latina de Comunicación Social*, 63, páginas 287 a 293. Recuperado de: http://www.revistalatinacs.org/_2008/23_34_Santiago/Francisco_Campos.html
- Cano, L. (s.f). Margen de actuación de Facebook y Twitter para censurar, políticas de privacidad y derechos del usuario como límite de la libertad de expresión. Valencia, España: Universidad de Valencia. Recuperado de: http://s3.amazonaws.com/academia.edu.documents/42708474/Margen_de_actuacion_de_Facebook_y_Twitter_para_censurar._Políticas_de_privacidad_y_derechos_del_usuario.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1490686086&Signature=iZstxFAZUznaRLGEQ9W4K6tXMaE%3D&response-content-disposition=inline%3B%20filename%3DMargen_de_actuacion_de_Facebook_y_Twitter.pdf
- Carías, I. (2015). Uso de Facebook como red social de los partidos políticos en campañas electoral 2015 (Tesis de grado). Universidad de San Carlos de Guatemala, Guatemala. Recuperado de: http://biblioteca.usac.edu.gt/tesis/16/16_1362.pdf
- Castells, M. (2001). Internet, libertad y sociedad: una perspectiva analítica. *Lección inaugural del curso académico, 2002*, 13-15. Recuperado de: http://red.pucp.edu.pe/wp-content/uploads/biblioteca/Manuel_Castells_-_Internet_libertad.pdf
- Castells, M. (2008). *Comunicación, poder y contrapoder en la sociedad red (I). Los medios y la política*. Telos, 74, 13-24.
- Castells, M. (2014). *Comunicación y poder*. Madrid, España: Alianza Editorial, S.A.
- Catells, M. (2012). *Redes de indignación y esperanza*. España: Alianza Editorial
- Chatfield, T. (2011). *50 cosas que hay que saber sobre el mundo digital*. Barcelona, España: Ariel con sello de editorial Planeta, S.A.
- Criado, J. y Rojas, (eds) (2013). *Las redes sociales digitales en la gestión y las políticas públicas*. Barcelona: Escolar de Administración Pública de Catalunya. Recuperado de: http://americo.usal.es/iberoame/sites/default/files/criado_redes_sociales_digitales.pdf

- De Grácia, C. (2013). Campanas electorales transparentes: figuras públicas — ¿hasta dónde los candidatos pueden mantener su privacidad?-. Foro: Derecho a la Privacidad vs. Derecho a Información de Organizaciones Políticas y Candidatos. Quito, Ecuador: Instituto de Investigación para la Justicia. Recuperado de: <http://www.iijusticia.org/docs/figuraspublicas.pdf>
- Del Río, O. (2011). El proceso de Investigación: etapas y planificación de la investigación. Vilches (coord.). La investigación en comunicación. Madrid, España: Gedisa.
- Edwards, P. y Edwards, S. (2001) Hacer negocios en el ciberespacio (Patrick Ducher, trad.). Barcelona: Ediciones Paidós Ibérica, S.A (Obra original publicada en 1998). Recuperado de: https://books.google.es/books?id=N5kMBBjCkYYC&pg=PA40&dq=lo+malo+del+ciberespacio&hl=es&sa=X&ved=0ahUKEwiq39jVj_3SAhXG7yYKHeIpDm0Q6AEIPjAG#v=onepage&q=lo%20malo%20del%20ciberespacio&f=false
- Elizondo, M. (s.f). Las personas políticamente expuestas y el blindaje de las elecciones. México: UNAM. Recuperado de: <https://revistas-colaboracion.juridicas.unam.mx/index.php/quid-iuris/article/view/17346/15555>
- Enríquez, X. (2016). Por qué escribimos de DictaLord, net centers y perfiles falsos. Guatemala: Revista ContraPoder. Recuperado de: <http://contrapoder.com.gt/2016/07/08/por-que-escribimos-de-dictalord-net-centers-y-perfiles-falsos/>
- Fernández, C. (2011). Privacidad y Facebook: estudio sobre los datos personales en las redes sociales online. España: Universidad de Salamanca. Recuperado de: https://gredos.usal.es/jspui/bitstream/10366/116281/1/TFM_Fern%C3%A1ndezMor%C3%A1n_Carlos_PrivacidadyFacebook.pdf
- Finoll, V. (2014). El trol de Internet: estrategias de los usuarios para controlar el diálogo en los medios digitales durante el juicio de Francisco Camps. Valencia, España: Dígitos, revista de comunicación digital. Recuperado de: <http://roderic.uv.es/bitstream/handle/10550/43949/102690.pdf?sequence=1&isAllo=1&isAllowed=y>

- Flores Mamani, F. D. (2014). ¿Qué es TOR?. *Revista de Información, Tecnología y Sociedad*, 1. Recuperado de: http://www.revistasbolivianas.org.bo/pdf/rits/n9/n9_a02.pdf
- Flores, J. (2009). Nuevos modelos de comunicación, perfiles y tendencias de las redes sociales. Madrid, España: Revista Científica de Educomunicación. Recuperado de: <http://rabida.uhu.es/dspace/bitstream/handle/10272/2843/b15573680.pdf?sequence=1>
- Fundación Telefónica (2013). Identidad Digital: El nuevo usuario en el mundo digital. Madrid, España: Ariel. Recuperado de: http://boletines.prisadigital.com/identidad_digital.pdf
- Gaitán y Piñuel (1998). Técnicas de investigación en comunicación social. Madrid, España: Editorial Síntesis.
- García, T., Yezers'ka, L., Rost, A., Calderín, M., Edo, C., Rojano, M., Said, E.,... Corredoira, L. (2011). Uso de Twitter y Facebook por los medios iberoamericano. (s.l): El profesional de la información. Recuperado de: http://s3.amazonaws.com/academia.edu.documents/34063605/Garcia_et_al_2011.El_Profesional_de_la_Info.pdf?AWSAccessKeyId=AKIAIWOWY YGZ2Y53UL3A&Expires=1490676308&Signature=N0shgbYzozi26YETPc WY7gZ9n18%3D&response-content disposition=inline%3B%20filename%3DUSO_DE_TWITTER_Y_FACEBOOK_K_POR_LOS_MEDIOS.pdf
- Giones Valls, A., & Serrat Brustenga, M. (2010). La gestión de la identidad digital: una nueva habilidad informacional y digital. Recuperado de: <http://www.tabuladecimal.info:8080/xmlui/bitstream/handle/123456789/206/giones2%5b2%5d.htm?sequence=2&isAllowed=y>
- González - Manzano, González - Tablas, Fuentes y Ribagorda (2013). Seguridad en Redes Sociales: problemas, tendencias y retos futuros. Madrid: Universidad Carlos III de Madrid. Recuperado de: http://orff.uc3m.es/bitstream/handle/10016/18169/Seguridad%20en%20Redes%20Sociales_problemas%20tendencias%20y%20retos%20futuros.pdf?sequence=1&isAllowed=y
- Gordo, Á., Sádaba I. (2008). Cultura digital y movimientos sociales. Madrid, España: Catarata.
- Hernández, Fernández y Baptista (2010). Metodología de la investigación. Ciudad de México, México: Mc Graw Hill.

- Igarza, R. (2010). Nuevas formas de consumo cultural: Por qué las redes sociales están ganando la batalla de las audiencias. Sao Paulo, Brasil: Dossié. Recuperado de: http://s3.amazonaws.com/academia.edu.documents/43453548/205-207-1PB.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1490526510&Signature=5zlDRhinDD2F2caUsbAB1lczNxw%3D&response-contentdisposition=inline%3B%20filename%3DNuevas_formas_de_consumo_cultural_Por_qu.pdf
- iLifeBelt (2016). Sexto Estudio de Redes Sociales de Centroamérica y el Caribe 2016. Dirigido por Jose Kont. Guatemala: iLifeBelt. Recuperado de: <http://ilifebelt.com/6to-estudio-anual-ilifebelt-redes-sociales-centroamerica-caribe-2016/2016/08/>
- Internet World Stats (2017). Estadísticas de uso de Internet. Recuperado de: <http://www.internetworldstats.com/stats2.htm>
- IV Congreso uruguayo de Ciencia Política (2012). El rol de las redes sociales en la participación política de los jóvenes en Uruguay. Montevideo, Uruguay.
- Jarvis, J. (2015). El fin de los medios de comunicación de masas: ¿cómo serán las noticias del futuro?. Nueva York, Estados Unidos: Paidós.
- Johnson, N. (1996). Democracia, censura e internet:: una visión desde el norte. Estados Unidos: Universidad de Iowa. Recuperado de: <https://repositorio.uc.cl/bitstream/handle/11534/7664/000178464.pdf?sequence=1&isAllowed=y>
- Kollock, P. y Smith, M. (2003). Comunidades en el ciberespacio (Ruíz, J., trad.). Barcelona: Editorial UOC. (Obra original publicada en 1999). Recuperado de: https://books.google.es/books?hl=es&lr=&id=2ThcN96FIEUC&oi=fnd&pg=PA17&dq=Kollock,+2003&ots=_YJiJuM_&sig=HPArcJ2YzOEGnisV1YIbLolR4m0#v=onepage&q=Kollock%2C%202003&f=false
- Lessig, L. (2014). Las leyes del ciberespacio. *THĒMIS-Revista de Derecho*, (44), 171-179. Recuperado de: <http://www.revistas.pucp.edu.pe/index.php/themis/article/view/10069/10504>
- Lozares Colina, C. (1996). La teoría de redes sociales. *Papers: revista de sociologia*, (48), 103-126. Recuperado de: <https://ddd.uab.cat/pub/papers/02102862n48/02102862n48p103.pdf>
- MacAdam, D., MacCarthy, J., Zald, M. (1999). Movimientos sociales: perspectivas comparadas. Madrid, España: Istmo.

- Magariño, A. (2015). La política de los jóvenes en Facebook en la Ciudad de Guatemala en el movimiento #RenunciaYa (Tesis de grado). Universidad de San Carlos de Guatemala, Guatemala. Recuperado de: http://biblioteca.usac.edu.gt/tesis/16/16_1369.pdf
- Martínez, M. (2015). Experiencia de comunicación política durante la campaña de un candidato a diputado, por el Partido Patriota, en el departamento de Jutiapa (Tesis de grado). Universidad de San Carlos de Guatemala, Guatemala. Recuperado de: http://www.repositorio.usac.edu.gt/4367/1/16_1233.pdf
- Mateus (2010). Jóvenes y Política 2.0: ¿Del desencanto real al oportunismo virtual?. Lima, Perú: Universidad de Lima. Recuperado de: <http://revistas.ulima.edu.pe/index.php/contratexto/article/view/197/226>
- Meneses, M. (2012). Redes y medios en el proceso electoral 2012: Mismas prácticas, herramientas distintas. México: Revista Mexicana de Comunicación. Recuperado de: <http://mexicanadecomunicacion.com.mx/rmc/?s=Redes+y+medios+en+el+proceso+electoral+2012%3A+Mismas+pr%C3%A1cticas%2C+herramientas+distintas>
- Miró, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Recuperado de: <http://www.marcialpons.es/static/pdf/9788415664185.pdf>
- Montoya, J. (2013). Redes sociales virtuales y sus efectos en la campaña política presidencial en Colombia para el periodo 2010 (Tesis de grado). Pontificia Universidad Javeriana, Colombia. Recuperado de: <https://repository.javeriana.edu.co/bitstream/handle/10554/15236/MontoyaVergelJuanPablo2013.pdf?sequence=1&isAllowed=y>
- Nicolás, M., Grandío, M. (coords.) (2012). Estrategias de comunicación en redes sociales: usuarios, aplicaciones y contenidos. Barcelona, España: Gedisa.
- Oficina de Seguridad del Internauta (s,f). En Internet cuida tu privacidad. España: Instituto Nacional de Ciberseguridad del Gobierno de España. Recuperado de: <https://www.osi.es/es/tu-informacion-personal>
- Ossorio (s.f.). Diccionario de Ciencias Jurídicas Políticas y Sociales. Guatemala: Datascan, S.A. Recuperado de: https://conf.unog.ch/tradfrweb/Traduction/Traduction_docs%20generaux/Diccionario%20de%20Ciencias%20Juridicas%20Politicas%20y%20Sociales%20-%20Manuel%20Ossorio.pdf

- Pérez, M. (2012). Uso de redes sociales en campaña electorales (Tesis de grado). Pontificia Universidad Católica del Perú, Perú. Recuperado de: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/1718>
- Piscitelli, A., Adaime, I., Binder, I. (2010). El Proyecto Facebook y la posuniversidad: sistemas operativos sociales y entornos abiertos de aprendizaje. Buenos Aires, Argentina: Ariel, S.A.
- Ponce, V., & Maldonado, A. (2016). Redes Sociales: Definición. Recuperado en: <http://recursostic.educacion.es//observatorio/web/ca/internet/web-redes-sociales?start=1> 20//1043-
- Ramírez, J. (2015). Las redes sociales y su impacto en la agenda mediática (el Periódico y Prensa Libre) (Tesis de grado). Universidad Rafael Landívar, Guatemala. Recuperado de: <http://recursosbiblio.url.edu.gt/tesiseortiz/2015/05/01/Ramirez-Jose.pdf>
- Ramonet (2003). La tiranía de la comunicación. Barcelona, España: Debate.
- Ramonet, I. (1998). *La tiranía de la comunicación*. Madrid, España: Debate, S.A.
- Ramos-Serrano, M. (2007). Comunicación viral y creatividad. Valencia, España: *Revista Creatividad y Sociedad*, 11, 202-226. Recuperado de: <https://idus.us.es/xmlui/bitstream/handle/11441/26579/%C2%BF%C2%BFCreatividad%20y%20Sociedad.%20Comunicacion%20viral%20y%20creatividad.pdf?sequence=1&isAllowed=y>
- Redondo, S. (2016). Sobre perfiles falsos en redes sociales. Entre Paréntesis. Recuperado de: <http://entreparesis.org/perfiles-falsos-redes-sociales/>
- Reyes, L. (2017). Movilización ciudadana y redes sociales: descripción de la emergencia de nuevos líderes de opinión en 2015 (Tesis de grado). Universidad Rafael Landívar, Guatemala. Recuperado de: <http://biblio4.url.edu.gt/Tesis/V20/jcem/Tesis/2017/05/01/Reyes-Libny.pdf>
- Ribas, J. (1998). La Sociedad Digital: Riesgos y Oportunidades, publicado en *Informática y Derecho*. Mérida: Universidad Nacional de Educación a Distancia.

- Rodríguez, C. (2016). Los partidos políticos guatemaltecos Líder y UNE, y su agenda mediática de oposición en redes sociales durante los años 2012- 2013 (Tesis de grado). Universidad Rafael Landívar, Guatemala. Recuperado de: <http://biblio4.url.edu.gt/Tesis/V20/jcem/Tesis/2016/04/26/Rodriguez-Carlos.pdf>
- Rodríguez, J. (2011). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación (Tesis de grado). Colombia: Universidad CES. Recuperado de: <http://bdigital.ces.edu.co:8080/repositorio/handle/10946/1334>
- Rodriguez, P. (2001). Feos, sucios y malos. La imagen de los hackers en los medios de comunicación. IV Congreso Chileno de Antropología. Departamento de Antropología de la Universidad de Chile, Santiago de Chile. Recuperado de: <https://www.aacademica.org/pablo.gustavo.rodriguez/23>
- Sánchez Medero, G. (2012). Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del S. XXI. Venezuela: *Revista Cenipec*, (31), 239-267. Recuperado de: <http://www.saber.ula.ve/bitstream/123456789/36770/1/articulo9.pdf>
- Sanz, L. (2003). Análisis de Redes Sociales: o como representar las estructuras sociales subyacentes. Madrid, España: Asociación para el Avance de la Ciencia y la Tecnología en España (AACTE). Recuperado de: <http://ipp.csic.es/sites/default/files/content/workpaper/2003/dt-0307.pdf>
- Schlosberg, J. (2017). El complejo mediático-tecnológico- militar-industrial. Transnational Institute y Fuhem Ecosocial. Recuperado de: <https://www.fuhem.es/media/ecosocial/file/Estado-del-poder-2017/7.Complejo-Estado-del-poder2017.pdf>
- Siles, V. (2014). ¿Cuántos ataques se generan en Centroamérica?. *Revista It Now*. Recuperado de: <https://revistaitnow.com/cuantos-ataques-se-generan-en-centroamerica/>
- Téllez, J. (1998). *La Sociedad Digital: Riesgos y Oportunidades*, publicado en *Informática y Derecho*. Mérida: Universidad Nacional de Educación a Distancia.
- Temperini y Macedo (2015). La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen. Rosario, Argentina: Simposio Argentino de Informática y Derecho. Recuperado de:

http://sedici.unlp.edu.ar/bitstream/handle/10915/55608/Documento_completo.pdf-PDFA.pdf?sequence=1

- Toral, A. (2013). Las redes Sociales un complemento en campañas electorales (Tesis de grado). Ecuador: Universidad del Azuay. Recuperado de: <http://dspace.uazuay.edu.ec/handle/datos/3330>
- Trejo, C. E. A., Chimbo, K. M. O., & Cisneros, J. C. (2016). Los medios de comunicación y la estafa electrónica: Nueva forma de delito (Ecuador). *In Crescendo Derecho y Ciencia Política*, 3(1), 78-92. Recuperado de: <http://revistas.uladech.edu.pe/index.php/increscendo-derecho/article/view/1171/952>
- Túñez, M. y Sixto, J. (2011): "Redes sociales, política y Compromiso 2.0: La comunicación de los diputados españoles en Facebook", en Revista Latina de Comunicación Social, 66. La Laguna (Tenerife): Universidad de La Laguna, páginas 210 a 246. Recuperado de: <http://www.cuadernosartesanos.org/2016/p8.pdf#page=85>
- Valladolid, C. (2009). Seguridad informática. España: Junta de Castilla y León. Recuperado de: <http://cloud.crfptic.es:9080/jspui/bitstream/recursos/46/1/seguridad.pdf>
- Vega, M. (2010). Uso e impacto de las Tics en la campaña presidencial de 2010 en Colombia (Tesis de grado). Pontificia Universidad Javeriana, Colombia. Recuperado de: <https://repository.javeriana.edu.co/bitstream/handle/10554/7734/tesis395.pdf?sequence=1&isAllowed=y>
- Wallace, P. (2001). La Psicología de Internet. Barcelona, España: Editorial Paidós
- Zallo, R. (2011). Estructuras de la comunicación y de la cultura: Políticas para la era digital. Barcelona, España: Gedisa.

Anexos

Anexo I

IDENTIFICADOR DE PERFIL FALSO										
Usuario	Personaje político	¿Cuenta con fotografía?	¿Cuenta con descripción?	No. de "siguiendo"	No. de seguidores	No. de tuits	Fecha de creación	¿Sigue en actividad?	Ubicación	Observaciones

Anexo II

ANÁLISIS DE PERFILES FALSOS			
Personaje Político			
Usuario			
Cargo			
1. Según su fin		Observaciones	
a. Sátira			
b. A favor			
c. En contra			
2. Según su mensaje		Calificación	Observaciones
a. Discriminación		Positivo	
b. Odio			
c. Apoyo/halagos		Negativo	
d. Rechazo			
e. Alentador		Lenguaje	
		Coloquial	

		Político	
		Soez	
3. Según dinámicas de comunicación		Observaciones	
a. Texto			
b. Vídeo			
c. Meme			
d. Fotografía			
e. Enlaces a medios			
f. Gif			
4. Según interacción		Observaciones	
¿Los tuits acompañados por fotografías, memes, videos, gif o enlaces reciben mayor aceptación?			
¿Qué reacción de interacción es más utilizada en ese perfil?			
¿La respuesta del perfil falso hacia sus "seguidores" es alta?			

¿La respuesta de los "seguidores" es dinámica? (texto con videos, gif o memes)	
¿Se considera influyente hacia los usuarios?	

Anexo III

Preguntas guía

Entrevista semiestructurada

Esta guía de preguntas será utilizada para desarrollar las entrevistas con los tres especialistas establecidos. Las preguntas serán modificadas según la profesión de cada entrevistado y según el área que ejercen o conocen en base a su experiencia. La entrevista se enfocará en cubrir tres principales temas: seguridad en la web, dinámicas de comunicación de los perfiles falsos y un candidato en redes sociales.

a) Seguridad en la web

1. El implemento de las TIC's en nuestra vida diaria tiene sus ventajas y desventajas. ¿A ciencia cierta hasta donde es capaz de llegar el usuario en la web?
2. ¿El ser humano está capacitado para tener en sus manos el mundo digital?
3. ¿Cree que hay conocimiento y manejo correcto de la web?
4. ¿Es necesario implementar cierta educación web en los centros educativos?
5. Si se habla de las desventajas de la web, la inseguridad que esta conlleva puede ser muy peligrosa para el usuario, ¿cuáles son las más grandes amenazas para la seguridad del ciberespacio?
6. ¿Qué se está haciendo para mejorar la seguridad en la web?
7. ¿Quiénes son los actores o "malhechores" en la web?
8. Las redes sociales han sido un espacio demasiado abierto, ¿hasta dónde llega la privacidad?
9. ¿Se cumplen con los términos y condiciones de privacidad y seguridad por parte de las plataformas de redes sociales?
10. ¿La identidad digital está riesgo?
11. Uno como usuario común y corriente, ¿qué debería tomar en cuenta para su seguridad?
12. ¿Algún caso en Guatemala relevante sobre amenazas de seguridad en la web?

13. ¿Cree que algunos sectores de poder se aprovecha de esta cierta vulnerabilidad de la web?

b) Dinámicas de comportamiento de los perfiles falsos

14. Una de las vulnerabilidades en las redes sociales son los perfiles falsos, ¿cómo se identifican este tipo de perfiles?

15. ¿Cuál es el comportamiento particular de un perfil falso?

16. ¿Cuál es el origen de los perfiles falsos?

17. ¿Qué han hecho las plataformas de redes sociales para combatir los perfiles falsos?

18. Entre Facebook y Twitter, ¿cuál es la plataforma más segura?

19. ¿Para qué fines se crean normalmente los perfiles falsos?

20. ¿Cree que existan sectores de poder que utilicen los perfiles falsos como herramienta para su empoderamiento en usuarios?

21. A nivel comercial y publicitario, ¿los perfiles falsos son un negocio?

22. ¿Cree que este puede ser otro negocio para las empresas de Facebook, Twitter?

23. A nivel política, ¿cree que utilizan los perfiles falsos a su favor?

24. Según las leyes internacionales esto es penado, ¿cree que hay regulación en este sentido?

25. ¿En Guatemala se trabaja por regular estos tipos de actos en la web?

c) Dinámicas de comunicación de los perfiles falsos

26. ¿Cuál es el lenguaje que utilizan los perfiles falsos?

27. ¿El contenido publicado tiene intenciones de agresión?

28. ¿Cree que la interacción entre el usuario falso y el usuario "real" es efectiva?

29. ¿El contenido causa impacto en los usuarios?

30. ¿Pueden llegar a ser capaces de influir en la opinión pública?

31. ¿La comunicación establecida llega a persuadir o impactar al pensamiento humano?

32. ¿El poder de un perfil falso depende de cómo se implementa la comunicación?

33. ¿Los perfiles falsos pueden considerarse una estrategia de comunicación para efectos de persuasión?

d) Los perfiles falsos en la ciberpolítica

34. ¿En qué le puede afectar los perfiles falsos a la política implementada en la red?

35. ¿Existen amenazas relevantes para la ciberpolítica?

36. ¿Los perfiles falsos pueden lograr desviar la opinión sobre el sector político?

37. ¿El uso de perfiles falsos pueden llegar a destruir la reputación de una figura política?

38. ¿Los perfiles falsos pueden considerarse un herramienta de poder para la ciberpolítica?

39. Si en la política se utilizan los perfiles falsos, ¿esta actividad se podría considerar un gran negocio para este sector?

40. ¿Representa una amenaza si los perfiles falsos tienen origen de grupos sociales?

41. ¿Se puede sabotear a sectores políticos a través del uso de perfiles falsos?

42. ¿Qué más se puede llegar a lograr con los perfiles falsos en la ciberpolítica?

43. Un caso relevante en Guatemala sobre este tema

e) Una campaña política en redes sociales

44. Los políticos en Guatemala, ¿le dan un buen uso a las redes sociales para introducirse en la sociedad?

45. ¿Guatemala está preparada para ver y conocer campañas políticas por medio de redes sociales?

46. ¿Las redes sociales es el nuevo reto para la comunicación política?

47. ¿Cuál es la dinámica de una campaña política en redes sociales?

48. ¿Las prácticas comunicacionales se han establecido de buena manera en las campañas virtuales que se dieron a conocer en las elecciones del 2015 en Guatemala?

49. En el 2015 se generó el "rumor" de la implementación de estructuras informáticas encargadas de generar contenido político en redes sociales. ¿Considera que este es el nuevo juego del sector político?
50. En su contraparte, ¿pueden llegar a existir sectores sociales capaces de implementar estas mismas estrategias?
51. ¿Considera un truco o trampa el uso de net-centers para generar impacto en la sociedad?
52. Se tiene el conocimiento que las prácticas tradicionales en las campañas políticas ya están muy explotadas. ¿Esto quiere decir que no es extraño detectar "trucos" virtuales para poder colocarse en redes sociales?
53. ¿Qué equipo se necesita para implementar una campaña política con éxito en redes sociales?
54. ¿Considera a las redes sociales una herramienta de poder para la política actual?