



CAEN
ESCUELA DE POSGRADO

LA DESINFORMACIÓN, FAKE NEWS Y SUS IMPLICANCIAS EN EL ENTORNO INTERNACIONAL

Expositor:

José Marangunich R.

Doctor en Desarrollo y Seguridad Estratégica

Lic. Derecho y Ciencias Políticas

Master of Business Administration

Especialista en Crimen Cibernético

Lima, Abril 2021





Contenido

- 01 Fenómeno FAKE NEWS
- 02 Orígenes de las FAKE NEWS
- 03 ¿Por qué se dio y continúa en el 2021? ¿Qué busca?
- 04 Impacto de las FAKE NEWS en distintos escenarios
- 05 FAKE NEWS y buscadores (Google, Yahoo, Bing, otros)
- 06 Las FAKE NEWS y los casos Wanna Cry y Estonia
- 07 Las Fake News y la Ciberseguridad
- 08 Comentarios Finales



1

FENÓMENO FAKE NEWS



Enmanuel Kant teorizó que el ser humano no puede conocer las 'cosas-en-sí-mismas', sino solamente las cosas tal como las experimenta en su mente”



PSICOLOGÍA DE LAS “FAKE NEWS”

La neurociencia explica cómo de predispostos estamos a aceptar informaciones falsas según nuestra ideología, el estado emocional, el entorno.

En situaciones de tensión y preocupación como las actuales las personas somos más susceptibles, le damos credibilidad a ciertas noticias que no son reales porque sesgamos mucho nuestro procesamiento de la información.

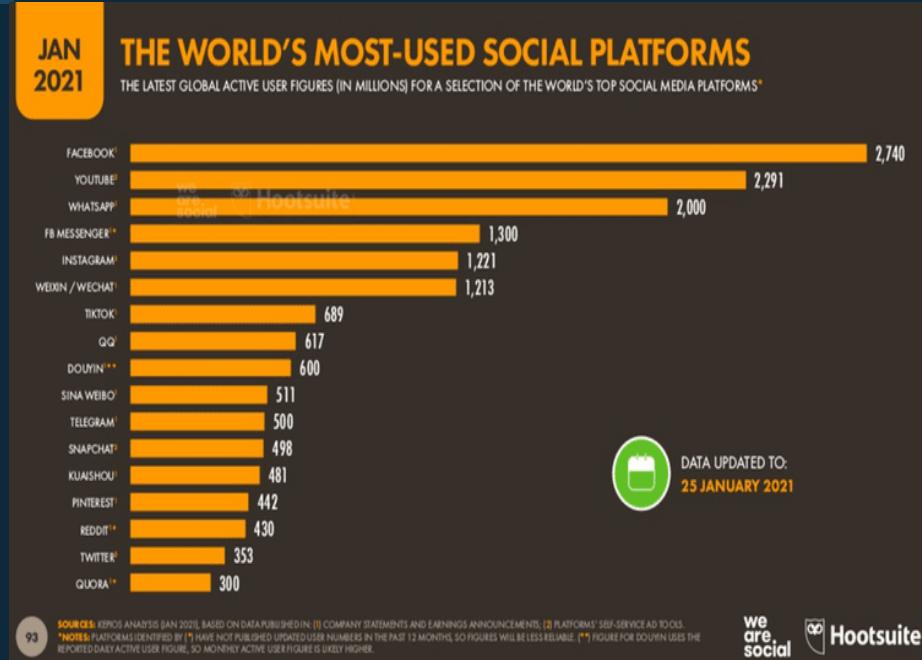
Rafael San Román-Psicólogo ifeel

“Tenemos tendencia a dar por buenas las cosas que coinciden con lo que creemos, con nuestras ideas preconcebidas, de modo que si llega una información que va en la misma línea que tus esquemas mentales es más fácil que la integres”.

Beatriz Fagundo
Doctora en Neurociencia Cognitiva



REDES SOCIALES CON MAS USUARIOS EN EL MUNDO



Los nuevos modelos de comunicación han transformado la manera de transmitir las noticias. Gracias a internet, el acceso a la información es más rápida.

Al día se realizan más de 6 mil millones de búsquedas en Google. Facebook tiene 2.700 millones de usuarios activos e Instagram tiene 1 mil millones de usuarios. Esta necesidad de estar informados a cada instante ha provocado el auge de las conocidas 'fake news'.

Los nuevos usuarios digitales

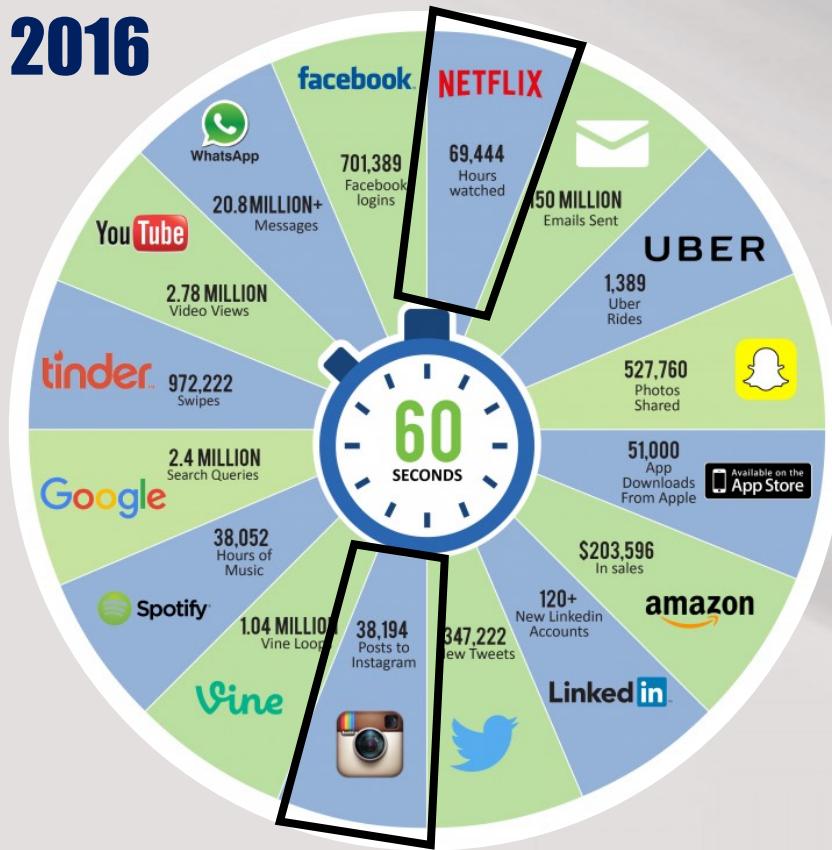


Fuente: KPMG, El nivel de madurez digital, abr. 2017

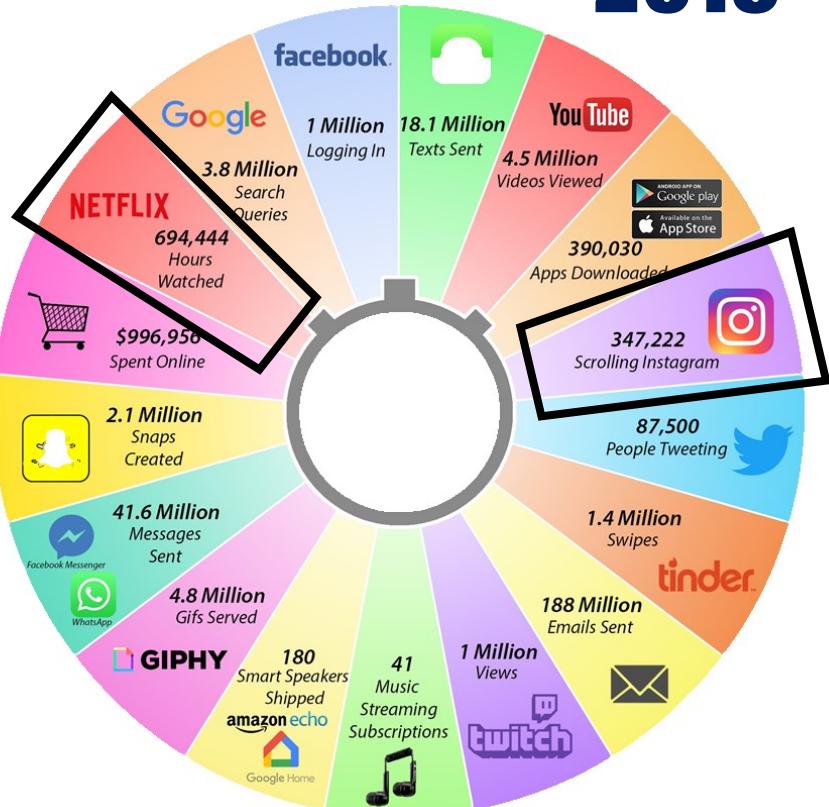
II. Futuro: ¿Época de cambio o cambio de época?

Internet en un minuto y su crecimiento exponencial

2016



2019



LA AMENAZA DE LAS “FAKE NEWS”

- ◊ La preocupación por la desinformación y la difusión de noticias falsas en Internet y en especial en redes sociales va en aumento.
- ◊ El 56,4% de los usuarios de Internet de todo el mundo manifiesta preocupación por no saber qué es cierto y qué no en el ámbito de las noticias en la Red.
- ◊ De los países analizados, el que más preocupación muestra por las noticias falsas o “fake news” y la desinformación es Brasil (84%), mientras que los Países Bajos (32,3%) es el menos preocupado.

¿Cuánto nos preocupan las "fake news"?

Adultos preocupados por la veracidad de las noticias en Internet, en países seleccionados



Datos de enero de 2021.

Fuente: Digital 2021 Global Overview Report



LAS FAKE NEWS Y LA DESINFORMACIÓN



Entender que es la desinformación nos permitirá comprender mejor las fake news, y se define como:

- ◊ Brindar información errónea que en la mayoría de casos se hace de manera intencionada
- ◊ Efecto de desinformar
- ◊ Carecer de información

El término anglosajón de fake news hace referencia en español a noticias falsas. Este término se utilizada para describir las noticias erróneas o que carecen de verdad y que al momento de divulgarse **provocan una ola de desinformación.**



2

ORÍGENES DE LAS FAKE NEWS

FAKE NEWS A TRAVÉS DE LA HISTORIA

Las FAKE NEWS siempre han existido, incluso se considera que la serpiente “narrada en el Libro del Génesis es la artífice de la primera FAKE NEWS, al engañar a Eva, mezclando verdad y mentira, con un objetivo claro. Pocas veces las consecuencias han sido tan drásticas y desastrosas.” (Burgueño, 2020)



Mentiras de la serpiente, primeras «fake news»: Papa Francisco



MARIA ANTONIETA GUILLOTINADA

También se considera que la revolución francesa usó en su favor las FAKE NEWS, pues gracias a estas se dirigió el camino de María Antonieta hacia su muerte en la guillotina. Esas falsedades que se le atribuía originaron que la archiduquesa de Austria fuera vista como frívola y despilfarradora, además de acusársele de “conspirar contra Francia y promover todo tipo de intrigas.

FAKE NEWS A TRAVÉS DE LA HISTORIA

Actualmente con el desarrollo de tecnología tan avanzada, las FAKE NEWS han ampliado sus márgenes de difusión, pues ahora con el Internet pueden llegar a cualquier parte del planeta.

“La universalización de las herramientas de difusión, su facilidad de uso y su carácter gratuito multiplican la capacidad de divulgación de este tipo de informaciones.”
(Burgueño, 2020)

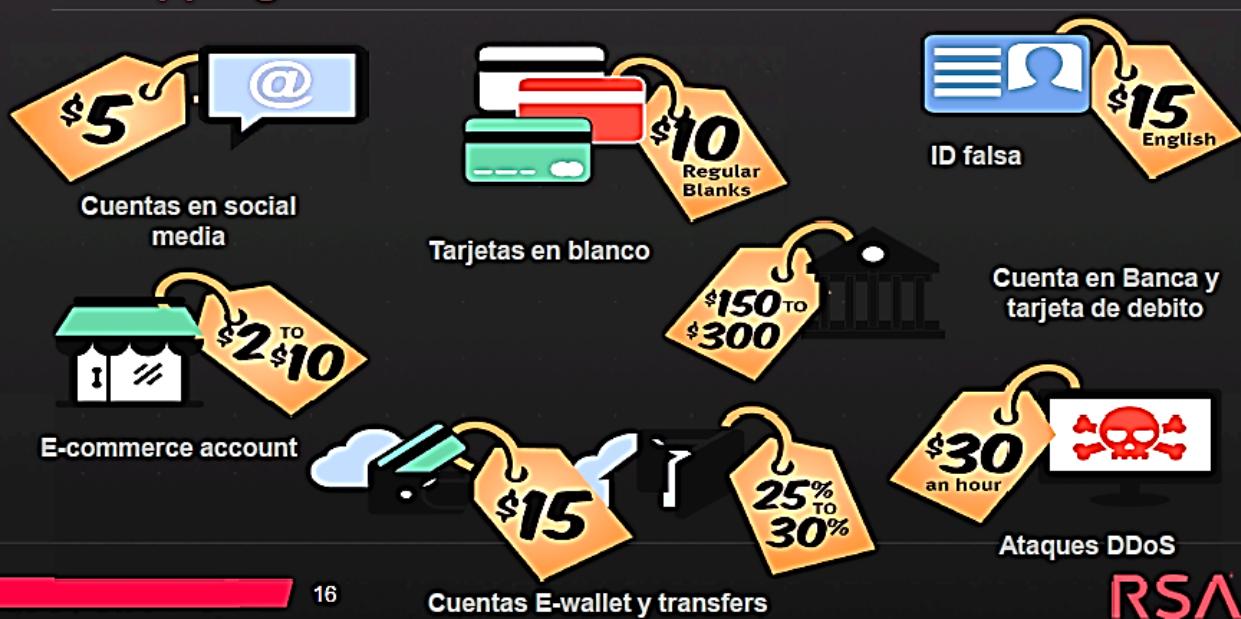
En las redes sociales y en Internet, el compartir y difundir información es tan fácil, pues solo es necesario dar un clic. Generando de esta forma potenciar la difusión de contenido engañoso y de información errada. “Así se genera un circuito vicioso, y una noticia falsa se replica miles de veces en cuestión de segundos.” (IFJ, 2020)



III. Industria Bancaria

Amenazas cibernéticas

Shopping list de la Ciberdelincuencia



TIPOS DE FAKE NEWS



Sátira o parodia

Este tipo de fake news no pretende causar daño por posiblemente engañar



Conexión falsa

Este se da cuando los titulares, imágenes o leyendas no confirman el contenido.



Contenido engañoso

Es intencionado con el fin de desestimar, actualmente se usa en los campos de la política, el entretenimiento y el deporte.



Contexto falso

Este tipo de fake news se da cuando el contenido genuino se difunde con información de contexto falso



TIPOS DE FAKE NEWS



Contenido impostor

Es aquél que se da cuando se suplantan fuentes genuinas.



Contenido manipulado

Es aquella fake news con información o imágenes genuinas que se manipulan para engañar.



Contenido fabricado

Contenido nuevo que es predominantemente falso, diseñado para engañar o perjudicar.



3

¿POR QUÉ SE DIO Y
CONTINÚA EN EL 2021?
¿QUÉ BUSCA?

	1945	1960	1980	1995	
Producto más usado	Veteranos (Tradicionalistas)	Baby Boomers	Generación X	Generación Y (Millenials)	Generación Z (Generación Internet)
Medios de comunicación	 	 	 	 	 
Preferencia de comunicación	Cara a Cara	Cara a Cara preferentemente / Por teléfono o Por correo si es necesario	Mensaje de Texto o Por Email	Online y Móvil (Mensaje de Texto)	Facetime
Porcentaje en USA / HISPANOS	9 % 8% Hispanos	24% 11% Hispanos	20% 18% Hispanos	22% 21% Hispanos	26% 22% Hispanos
Actitud hacia la tecnología	Análogos	Análogos	Inmigrantes Digitales	Nativos Digitales	Nativos Digitales
Actitud hacia la carrera	En gran parte desconectados	Primeros adaptadores de las TI	Transición hacia la era digital	Dependiente de las TI	Totalmente dependientes de las TI
	Los trabajos son para toda la vida	Organizacional: Las carreras son definidas por los empleadores	Fiel a la carrera, no necesariamente al empleador	Empresarios digitales: trabajan con las organizaciones, no para ellas	Se mueven sin problemas entre organizaciones y negocios emergentes

Las tecnologías más relevantes en la actualidad

Las que están más extendidas, más implementadas y con mayor demanda en profesionales y en servicios relacionados



Big Data



Cloud & Virtualización



Ciberseguridad



Lenguajes de
programación
relacionados
con Big Data



Tecnologías
de APIs y
Microservicios



IoT

@icemd



Realidad Virtual
& Aumentada

Las tecnologías más disruptivas y de mayor impacto en la actualidad

Las que independientemente de su relevancia están impactando más desde estos puntos de vista

Cliente:

Impacto en la forma de gestionar la información del cliente, y en la que nos comunicamos, relacionamos, vendemos y atendemos a nuestros clientes.

Procesos:

Impacto en la optimización y eficiencia de procesos de toda la cadena de valor de la empresa.

Modelos de negocio:

Impacto en la aparición y en el desarrollo de nuevos modelos de negocio y transformación de industrias, sectores y actividades.



Inteligencia
Artificial y Cognitiva



Deep Learning,
Chatbots y Asistentes
Virtuales



Image Recognition,
Text analytics,
Voice recognition



Industria 4.0



MOM: Manufacturing
Operations
Management Software



Fabricación
Aditiva 3D



Blockchain



Wearable
Technology

Las tecnologías de tendencias que aparecerán o se desarrollará mucho más su importancia en los últimos años



Robótica de
Servicios



Vehículo
Autónomo



Inteligencia
Artificial



Realidad
Virtual/Ampliada



Blockchain



Impresión 3D



Nanotecnología



Biotecnología (ADN,
medicina preventiva,
cyborgs)



Huellas
Digitales



Conexión
máquina/humano



Convivencia de la
logística física y digital



Smart cities

III. Industria Bancaria

Reflexiones



III. Industria Bancaria

Reflexiones



Elon Musk: cofundador de PayPal, Tesla Motors, SpaceX, Hyperloop, SolarCity, The Boring Company y OpenAI



4

IMPACTO DE LAS FAKE NEWS EN DISTINTOS ESCENARIOS

EJEMPLOS DE FAKE NEWS

Pope Francis Shocks World, Endorses Donald Trump for President, Releases Statement

TOPICS: Pope Francis Endorses Donald Trump



Noticia falsa que asegura que El Papa Francisco apoyó a Trump. No es verdad
(Independent.co.uk)

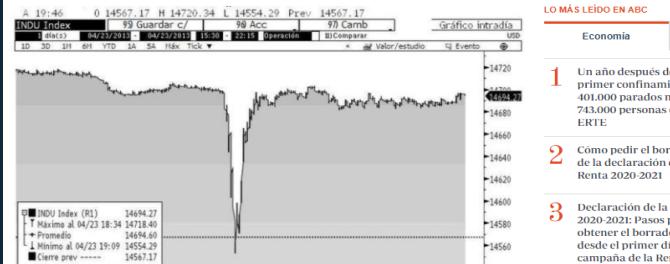
4:39 12 marzo 2021
5 mitos sobre las vacunas contra la covid-19



La propagación de afirmaciones erróneas o falsas sobre las vacunas del covid amenaza con entorpecer los programas de vacunación que se han iniciado en todo el mundo.

Wall Street se desploma por la noticia de un falso atentado sobre Obama

- Un tuit en la cuenta de Associated Press sobre un supuesto ataque a la Casa Blanca provocó una caída de casi 1 Bolsa de Nueva York en apenas unos segundos



Un video falso muestra cómo Corea del Norte vence a sus rivales en Brasil 2014

Por CNNEspañol Sí
14:09 ET (18:09 GMT) 13 Julio, 2014





Según un estudio del Instituto Tecnológico de Massachusetts (MIT) las noticias falsas tienen hasta un 70% más de posibilidades de ser retuiteadas que las verdaderas. Esto se debe, en gran medida, a que este tipo de información utiliza las interacciones en las redes sociales y los algoritmos para alcanzar sectores ideológicos concretos.

FAKE NEWS EN DISTINTOS ESCENARIOS



Acontecimientos políticos, cambio climático, avances científicos o movimientos sociales. Ningún campo informativo parece estar a salvo, imágenes retocadas y datos no contrastados que se viralizan causando el pánico general.

Ante la era de las FAKE NEWS, expertos de diversas instituciones ponen en marcha mecanismos para hacerles frente, siendo la Inteligencia Artificial uno de los más potentes.

Fuente: UCM: "Las fake news siempre han existido, pero hoy en día se han visto catapultadas por las redes sociales"



FAKE NEWS EN LA POLÍTICA

Washington Post slammed for fabricating quotes to frame former President Donald Trump



Democrats had cited the fabricated quotes in their impeachment documents – but Trump was later acquitted. (Screen shot)

Short Url <https://arab.news/cvhqw>

Las fake news a lo largo de su proceso histórico nos han mostrado que tienen un potencial poder para lograr movilizar masas de acuerdo a determinados intereses y respaldar medidas o actos complejos como por ejemplo, las guerras.

Con respecto al campo de la política, cuando se menciona unas FAKE NEWS casi todo el mundo lo relaciona con el presidente número 45 de los Estados Unidos, Donald Trump.

FAKE NEWS EN LA POLÍTICA

La ciudad europea que hizo una fortuna a base de crear noticias falsas sobre las elecciones de Estados Unidos

Emma Jane Kirby
BBC News

6 diciembre 2016



En Veles, una pequeña ciudad de Macedonia, muchos jóvenes se están enriqueciendo con un negocio que despierta polémicas.

Las elecciones presidenciales 2016, son un gran ejemplo (más actualizado) para explicar la influencia de la FAKE NEWS en el mundo de la política.

Donald Trump obtuvo el cargo de presidente número 45 de los Estados Unidos, su victoria en las elecciones presidenciales de 2016 “fue posible gracias al tratamiento de manipulación de verdad. Según la web Politi Fact el 70% de las declaraciones electorales de Trump eran bastante falsas, falsas o grandes mentiras.” (IFJ, 2020)

Fuente: Goberna: Fake news y el peligro de la desinformación.

BBC: La ciudad europea que hizo una fortuna a base de crear noticias falsas sobre las elecciones de Estados Unidos



FAKE NEWS EN LA SALUD



La Revista Estadounidense de Medicina e Higiene Tropical señala que al menos 800 personas habrían perdido la vida como resultado de la desinformación sobre la COVID-19 en los primeros meses de 2020, y otras 5.800 habrían acabado ingresadas en el hospital, según recoge la revista MIT Technology Review, como consecuencia de ingerir metanol y otros productos de limpieza como antídoto frente al virus.

la OMS ha analizado el origen de muchos consejos incorrectos que han circulado por la red acerca de la enfermedad y concluye que, aunque muchos no se comparten con intención maliciosa, pueden ser igualmente peligrosos para la salud.

FAKE NEWS LAS MAS COMENTADAS



Falso atentado contra Obama

La agencia de noticias publicó un urgente en su cuenta sobre explosiones en la Casa Blanca Wall Street llegó a caer un 1% durante unos minutos.



La niña de Kuwait y la invasión de Irak

Nayirah, denunciaba las atrocidades cometidas por los invasores iraquíes en su país. Relató un brutal testimonio que inclinó la balanza de la opinión pública estadounidense a favor de la guerra de Irak.



Muerte de Kim Jong

Rumores publicados por medios internacionales aumentaron tras la operación a la que fue sometido.

Fuente: BBC: 3 noticias falsas que propiciaron guerras y conflictos alrededor del mundo.
EL País: Un pirata publica un falso atentado contra Obama en el Twitter de AP.
EL Tiempo: Cobran fuerza versiones sobre muerte o estado de coma de Kim Jong Un.





5

FAKE NEWS Y BUSCADORES (GOOGLE, YAHOO, BING, FB, OTROS)

FAKE NEWS Y BUSCADORES

Google dará más información sobre una página web a los usuarios para facilitar su verificación y combatir las FAKE NEWS.

Algunos usuarios ya podrán observar que los resultados de Google muestran un ícono de menú, con el que pueden saber más sobre el resultado para tener una decisión informada sobre visitar o no la página.

Microsoft estrenó en el 2017 su etiqueta “Fast Check” en los resultados de búsquedas de Bing, su buscador de Internet, para señalar sitios web de noticias o que contengan artículos con información importante, siempre que se haya determinado que contengan información de verificación de hechos.



¿CÓMO SE VIRALIZAN?

- ◊ Por medio de la comunidad virtual que no cuenta con herramientas para reconocer FAKE NEWS y comparte información sin tener claridad sobre la veracidad de la información, motivados solo por sus emociones.
- ◊ En cadenas de WhatsApp, audios, videos e imágenes sin fuentes claras o que corresponden a otros hechos que buscan generar impacto emocional y así garantizar la difusión masiva.
- ◊ En redes sociales como Facebook es común la viralización de notas de portales dedicados a las 'FAKE NEWS' y en Twitter se hacen populares trinos de cuentas falsas o imágenes de supuestos mensajes que nunca existieron.
- ◊ Adicionalmente, por el envío de correos electrónicos de usuarios desconocidos o mensajes de texto contribuyen en dicha viralización.



¿Hoy, de quién son los datos?

Términos y Condiciones

- Extensos
- Difíciles de comprender
- Cláusulas que afectan la privacidad y derechos del usuario



¿Qué hacer con los Términos y Condiciones?

- Todas las personas debemos ser conscientes de los servicios a los que nos suscribimos.
- Es recomendable leer los términos y condiciones y políticas de privacidad de todos los servicios para entender que podemos esperar de los servicios y que información recopilan.
- Existen iniciativas para poder descifrar términos y condiciones muy extensas y entender aspectos clave, tal como: *Terms of Service; Didn't Read* tosdr.org

Google Class C

-  This service may collect, use, and share location data
 -  The service can read your private messages
 -  You agree to defend, indemnify, and hold the service harmless in case of a claim related to your use of the service
 -  This service tracks you on other websites
 -  Limited copyright license to operate and improve all Google Services
- [More details](#)

YouTube

Class D

-  Terms may be changed any time at their discretion, without notice to the user
-  Processes a personal information (email, id but also device info, location)
-  Users should revisit the terms periodically, although in case of material changes, the service will notify
-  If you are the target of a copyright claim, your content may be removed
-  The service is not responsible for linked or (clearly) quoted content from third-party content providers

[More details](#)

Facebook

Class E

-  Your identity is used in ads that are shown to other users
-  App required for this service requires broad device permissions
-  This service tracks you on other websites
-  This service tracks you on other websites
-  The service may use tracking pixels, web beacons, browser fingerprinting, and/or device fingerprinting on users.

[More details](#)

Wikipedia

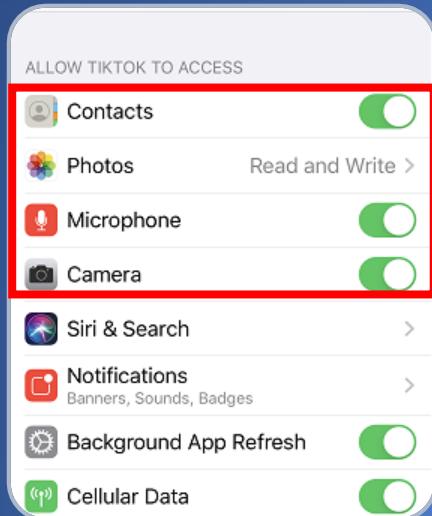
Class B

-  You publish your contributions under free licenses
-  The service will resist legal requests for user information where reasonably possible
-  The service can delete your account without prior notice and without a reason
-  There is a date of the last update of the terms
-  No need to register

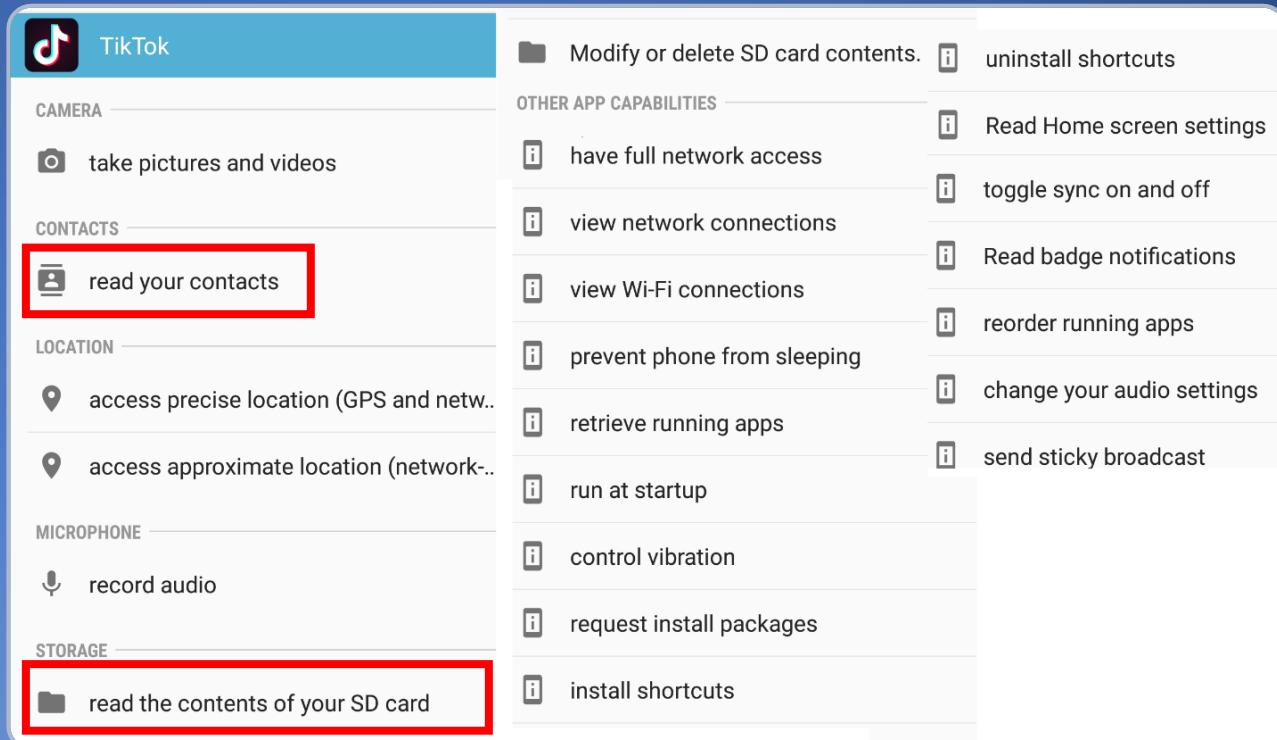
[More details](#)

¿Y tus datos, donde van? ¿y son DAC?

IOS



Android



Documental: El dilema de las redes sociales



Documental: El dilema de las redes sociales

Las reflexiones de ex ejecutivos de las principales empresas de redes sociales son:

- Alerta respecto a las formas adictivas de como se opera.
- Hoy se vende a los usuarios. Tu eres el producto
- Cuanto tiempo podemos retenerte en la pantalla.
- El producto, es el cambio gradual en nuestro comportamiento. Es un cambio sutil.
- Se vende certeza. Buenas predicciones y se necesita mucha información. Mercado de futuros que comercializa comportamientos.
- Lo saben todo.
- Crean un modelo que predicen nuestras acciones.
- Estrategia soportada en “tecnología persuasiva” que busca modificar el comportamiento y experimenta contagio a gran escala.
- Metas de crecimiento y metas de publicidad

FAKE NEWS Y REDES SOCIALES

¿HAY BRECHA EN LA REGULACIÓN VS LA TRANSFORMACIÓN?



► <https://youtu.be/Vru1iXZRHes>





CASO CAMBRIDGE ANALYTICA

**CAMBRIDGE ANALYTICA: UN RESUMEN SOBRE
CÓMO LA RECOPILACIÓN DE DATOS PUEDE
CREAR UN ARMA DE DESINFORMACIÓN MASIVA.**

Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?





CASO CAMBRIDGE ANALYTICA

TODO INICIA CON UN TEST DE PERSONALIDAD

Aleksandr Kogan, un investigador de la Universidad de Cambridge creó "This is your digital life", una aplicación de predicción de la personalidad a través de su empresa Global Science Research (GSR), que ofrecía una pequeña suma de dinero a los usuarios a cambio de completar un test de personalidad.



Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?



CASO CAMBRIDGE ANALYTICA

2014

LA 'APP' SE VIRALIZA

Según Facebook, 270.000 personas aceptaron descargar esa aplicación, pero al hacerlo también dieron acceso a información demográfica como nombres, ubicaciones, edades y géneros, así como las páginas a las que les dieron “me gusta” y algunos de los datos de sus amigos en Facebook. Se estima que se recopiló información personal de hasta 87 millones de usuarios, según las cifras del presidente de la red social, Mark Zuckerberg.

Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?





CASO CAMBRIDGE ANALYTICA

2016

COMIENZA EL TRABAJO CON ELECCIONES IMPORTANTES

Cambridge Analytica fue contratada como consultora política por la campaña de Donald Trump para las elecciones presidenciales de 2016.

Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?



CASO CAMBRIDGE ANALYTICA

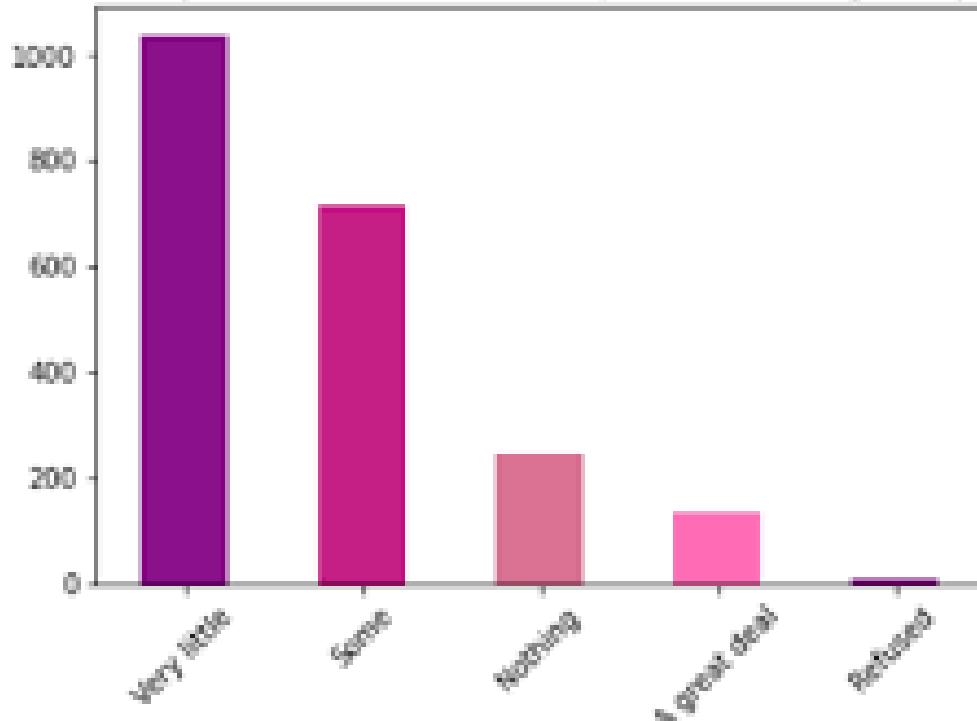
Cambridge Analytica accedió a los datos de 87 millones de usuarios de Facebook gracias a una aplicación que analiza la personalidad

- Apertura al cambio. Si estás dispuesto a vivir nuevas experiencias.
- Escrupulosidad. Que tan perfeccionista eres.
- Extraversión. ...
- Amabilidad. ...
- Eres solidario.

22 abr. 2018

Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?

How much do you understand what companies are doing with your data?



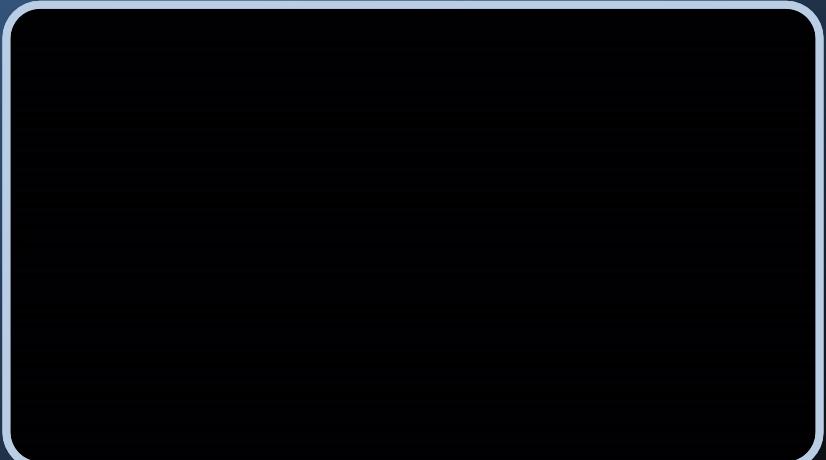
Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?



6

LAS FAKE NEWS Y LOS CASO WANNACRY Y ESTONIA

III. Ejemplos de ciber-riesgos





CASO WANNACRY

Este ataque masivo aconteció entre el 12 y el 16 de mayo del 2017 y representó una amenaza sin precedentes en el ámbito de la ciberseguridad.

Se trata de un ransomware (de “ransom”, rescate en inglés, y “ware” por “software” o programa informático), un tipo de código malicioso que explota una serie de vulnerabilidades en sistemas operativos Windows y en varios protocolos de red, bloqueando y encriptando documentos almacenados en los ordenadores de sus víctimas con el objetivo de solicitar al usuario el pago de una suma de dinero en la moneda electrónica bitcoin (más difícil de rastrear) para permitirles volver acceder nuevamente a los archivos.

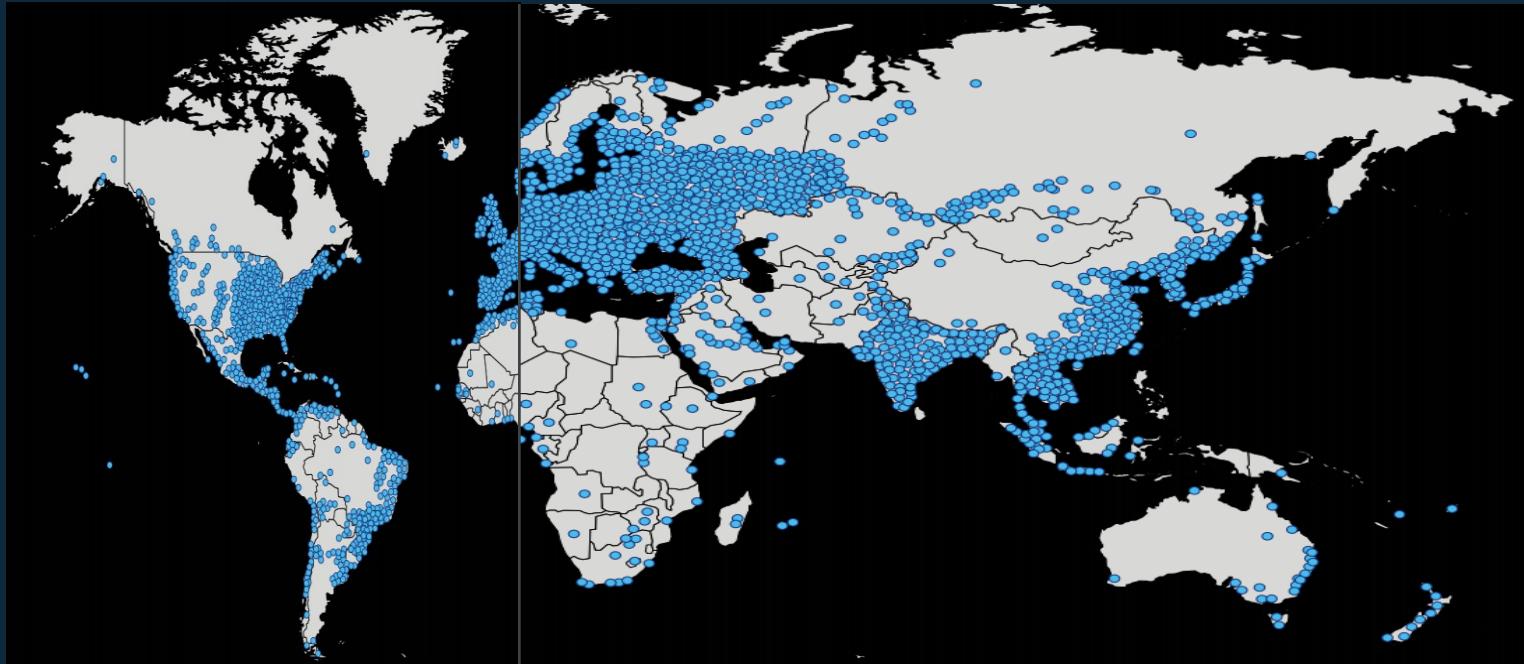
Se estima que 360.000 ordenadores en más de 180 países han sido afectados por una variante de ransomware conocida como “WannaCry” o “WannaCrypt”.



Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?

CASO WANNACRY

Mapa de infecciones de dispositivos por WannaCry



Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?

CASO ESTONIA

Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país

Damien McGuinness
BBC

6 mayo 2017



GETTY IMAGES

Estonia es uno de los países con más experiencia en temas de seguridad cibernética.

En 2007 Estonia sufrió un ciberataque sin precedentes. El país, de 1,3 millones de habitantes, emergía digitalmente tras romper con la era soviética, creando servicios para que sus ciudadanos pudieran pagar impuestos, pedir una receta médica y hasta votar (el primer escrutinio online se realizó en 2005) a través del ordenador de casa.

Este avance se tambaleó cuando un grupo de piratas informáticos de Rusia dejaron en negro las webs del Gobierno. En ese momento, el país más digital de Europa debió regresar a tiempos pretéritos utilizando el fax y el teléfono en sus comunicaciones.

Fuente: BBC, Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país.
El País, Un caso de éxito: cómo Estonia se protegió contra los ciberataques.

CASO ESTONIA



Estonia elaboró un plan estratégico para actualizar sus infraestructuras locales de TI y estableció como prioridad en las escuelas el desarrollo de habilidades informáticas y digitales, con materias como la ciberseguridad, la robótica y la programación.

Hoy en día y desde hace años, sus estudiantes copan los primeros puestos del informe PISA, que reconoce su excelencia y rendimiento académico. El 92% de la población estonia usa internet regularmente".

Los ataques quedaron grabados en el inconsciente colectivo y sirvieron para probar la importancia de la ciberseguridad.



7

FAKE NEWS Y LA CIBERSEGURIDAD



¿LAS FAKE NEWS POR QUÉ SON UNA AMENAZA PARA LA CIBERSEGURIDAD?

Las FAKE NEWS también pueden convertirse en ciberataques. En un principio, puede parecer que sólo se trata de información falsa que se va transmitiendo por la red, no obstante, se ha demostrado que éstas pueden ser un problema de ciberseguridad nacional.

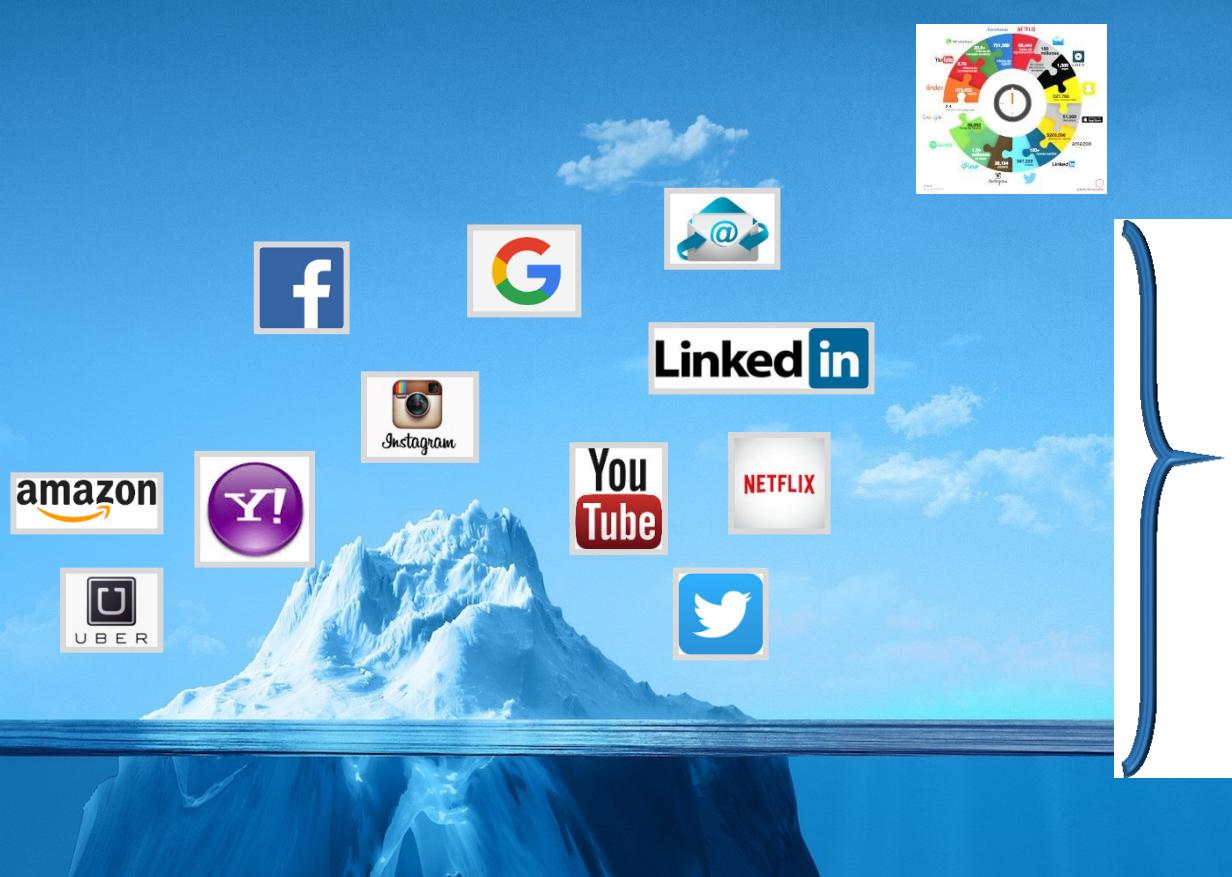
Escondiendo información maliciosa en mails cuyo contenido sea una noticia falsa para que llame más la atención del usuario e interactúe con éste.

En el 2014, los ciberdelincuentes utilizaron la desaparición del vuelo de Malaysian Airlines para mandar emails infectados con información falsa. Éstos sabían que al ser una información de interés mundial, muchos usuarios abrirían dichos emails. ¿Qué pasaba si lo hacías? **Un troyano infectaba tu sistema.**

Y no hace falta que sean compartidas a través de mail, sino que una Fake News compartida masivamente en Facebook y Twitter podría convertirse en una estrategia para atacar a los usuarios mediante malware o phishing.



CIBERESPACIO

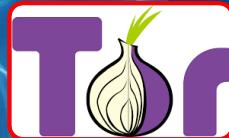


Surface Web
10% del contenido web
980MM de sitios webs

Contenido accesible a personas comunes. Todos los sitios web son indexados por los motores de búsqueda para su fácil acceso

TARINGA!

MEGA



The Hidden
Wiki

bitcoin



A screenshot of the Silk Road dark web marketplace. At the top, it shows 'Silk Road' with a small horse icon, 'messages 0', 'orders 0', and 'account \$0.00'. Below the header, there's a sidebar with links like 'Drug', 'Gel', 'De', 'Ec', 'Go', 'Dm', 'Ph', 'Pig', 'Bla', 'Anony', 'Art', 'Blot', 'Bead', 'Cone', 'Gifte', 'Digita', 'Drug', 'Sex', and 'Swag'. The main area displays several items for sale, including a 'Silk Road' t-shirt and a 'Silk Road' hoodie. In the foreground, a large table lists various items for sale, with some rows highlighted in yellow. The table columns include: Number, Type, Name, Country, City, Phone, Mail, DOB, and Price. Some entries show card numbers like 372845, 828713, 645456, 371527, 64698C, 851920, 645957, 071108, 93424E, and 071720, along with their respective details.

Number	Type	Name	Country	City	Phone	Mail	DOB	Price
372845	AMEX	Christopher 0.0	US	Los Angeles	Y	N	Y	405
828713	AMEX	Christopher 0.0	US	Los Angeles	Y	N	Y	405
645456	AMEX	Christopher 0.0	US	Los Angeles	Y	N	Y	405
371527	AMEX	El Presidente	US	New York	Y	N	Y	405
64698C	DISCOVER	El Presidente	US	New York	Y	N	Y	405
851920	DISCOVER	El Presidente	US	New York	Y	N	Y	405
645957	DISCOVER	El Presidente	US	New York	Y	N	Y	405
071108	AMEX	F. Rodriguez	US	New York	Y	N	Y	405
93424E	DISCOVER	Master 0.0	US	Los Angeles	Y	Y	Y	405
071720	AMEX	Greg 0.0	US	Los Angeles	Y	N	Y	405

Venta de drogas

Venta de armas

Alquiler de Botnets
(pc zoombies)

Trata de personas

Venta de ToolKits
para Hacking

Contrato de sicarios

Comunicación
entre terroristas

Pornografía ilegal
Pedofilia

Documentación clasificada

Venta de dispositivos
para fraude

Deep
Web

90% del
contenido
web

I. Información general

Ciberamenazas en el Ciberespacio

Realización de actos terroristas mediante la utilización de recursos informáticos y el ciberespacio.

**CIBER
TERRORISMO**

Se produce cuando el sistema informático se somete a acciones o amenazas con la negación reiterada de servicio u otros ataques. Los hackers maliciosos exigen dinero para detener los ataques u ofrecer protección.

**CIBER
EXTORSIÓN**

Es la realización de un fraude mediante manipulación de sistemas informáticos

CIBER FRAUDE

Realización de ataques sofisticados principalmente dirigidos a gobiernos. Estos cuentan con financiamiento y recursos sofisticados.

CIBER GUERRA

I. Información general

Ciberamenazas tipologías

Phishing

Man in the middle

Troyano

Ingeniería Social

Suplantación de identidad

Sabotaje informático

SCAM

Inyección de código

Botnets

Pharming

Rogueware

Crimeware

Exploits

SPAM

Ransomware

DDoS

Man in the Browser

CARDING

GROOMING

Adware

Spyware

Keylogger

Spoofing

Dialers

Defacement

Cyberbullying

Hijacking

Grayware

Ataque 0 day

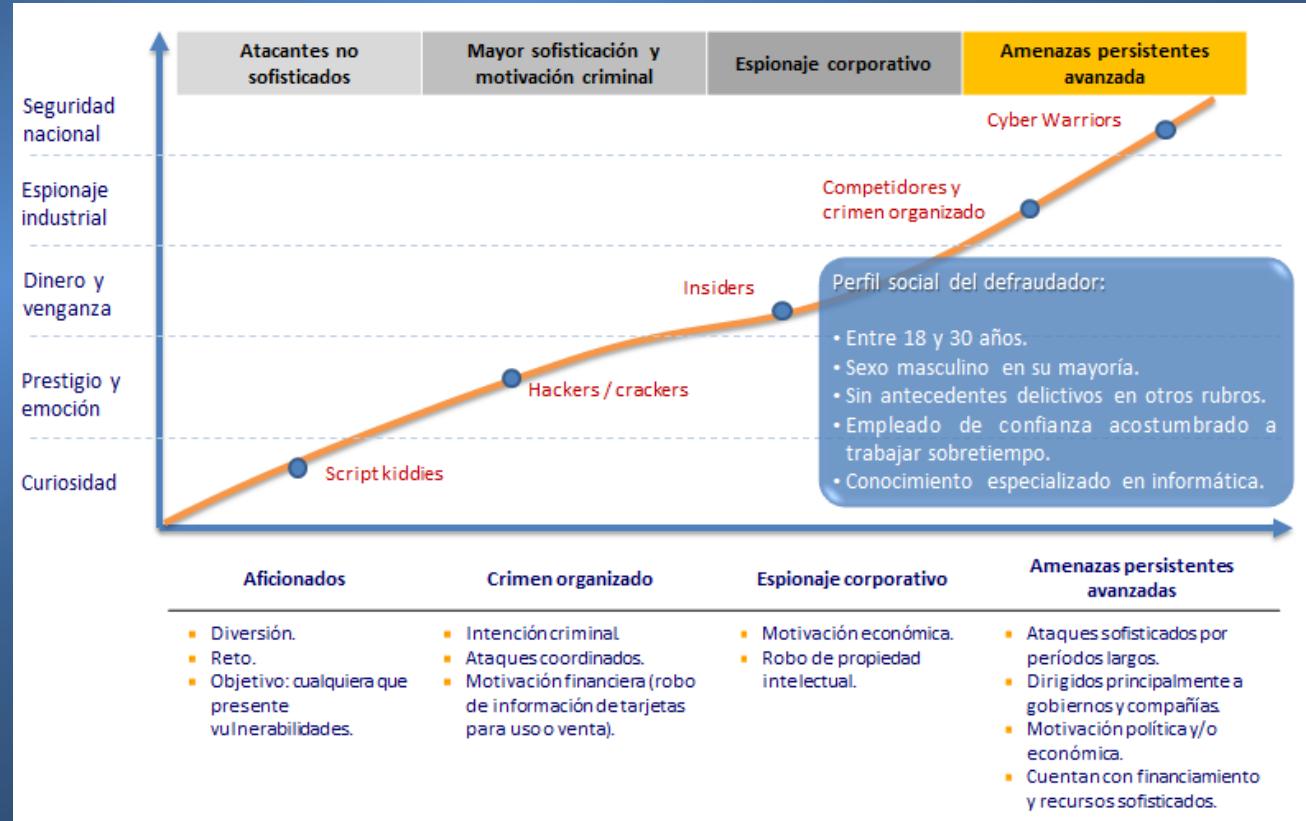
Virus

Backdoor

Malware

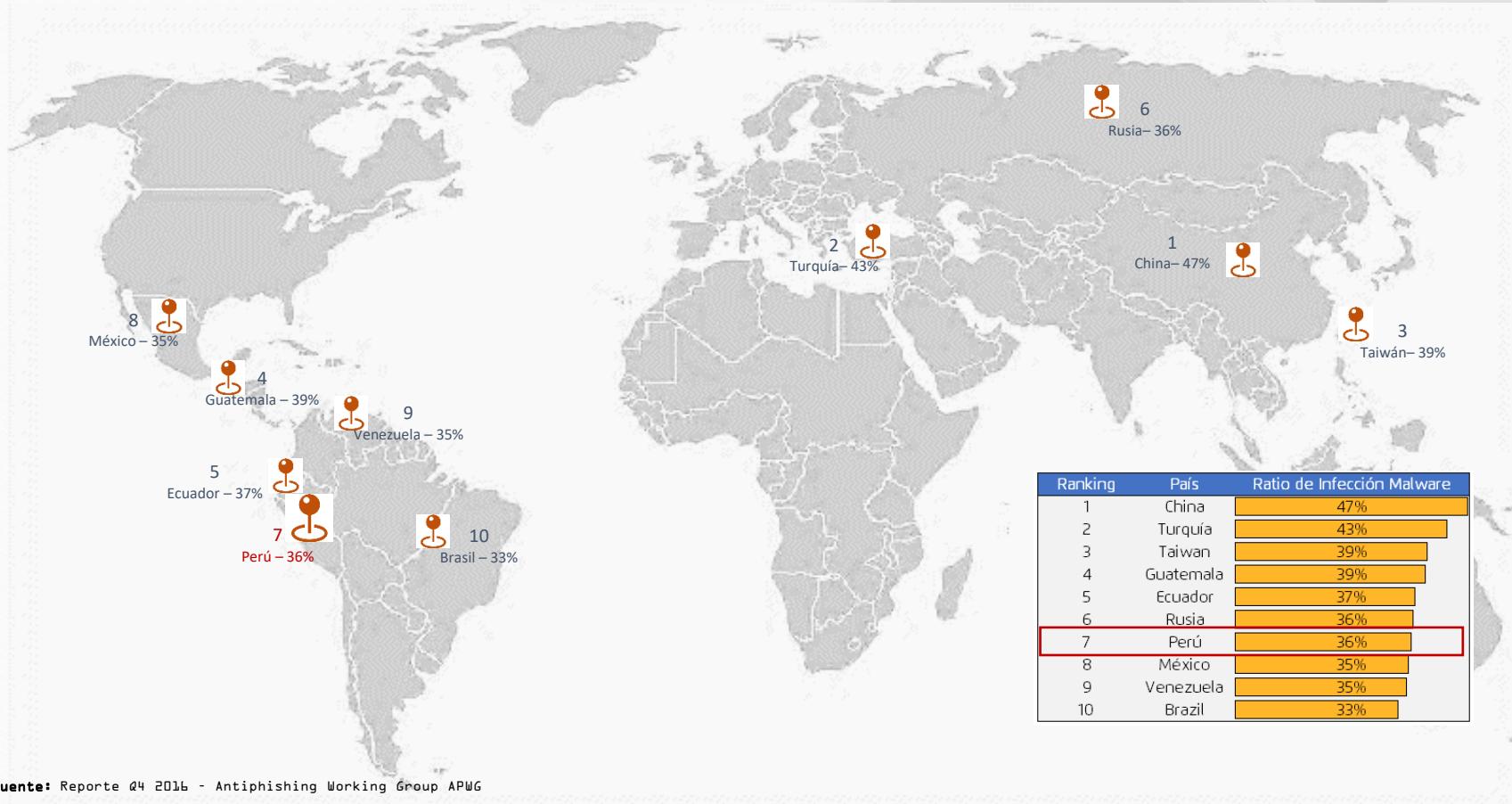


Perfil del cibercriminal



II. ¿Cómo estamos en el ecosistema digital global y sus riesgos?

Estadísticas



III. Principales Ciber-riesgos Ciberataques representativos

CIBERFRAUDE

Virus: Zeus (2010)



Más de 60 personas realizaron ataques informáticos contra la banca que permitió robar al menos 3MM de dólares en Estados Unidos y 9,5MM en el Reino Unido. Utilizaron el virus Zeus, probablemente creado en Rusia.

CIBERFRAUDE

Caso: SONY(2011)



SONY

Ataque de Hackers contra la plataforma de juegos de SONY (PLAYSTATION) afectó a 72MM de usuarios. comprometiendo datos de tarjetas de crédito

CIBERFRAUDE

Caso: Target (2014)



Fue atacada mediante un malware en sus TPV a través de un proveedor. Cuando un cliente utilizaba las tarjetas, el malware comenzaba a funcionar, lo que produjo el robo de 50M tarjetas de crédito

CIBERFRAUDE

Caso: ATM Japón (2016)



Robo en ATM's de Japón por más de US\$19MM del Banco South Africa's Standard Bank en 3 horas. Se realizaron con tarjetas de banda magnética y ATM desfasados.

CIBERFRAUDE

Caso: RSA (2011)



Hacker's violaron la red informática de RSA, sucursal de la empresa EMC, obteniendo información sobre la tecnología SecurID que se utiliza para proteger redes de ordenadores en el mundo entero

CIBERTERRORISMO

Associated Press (2013)



Se comprometió la cuenta de Twitter de la agencia AP (Associated Press) donde se publicó una información falsa sobre dos explosiones en la Casa Blanca en que el presidente Obama resultó herido..

CIBERTERRORISMO

Caso: NSA (2013)



Agencia Nacional de Seguridad de los EE.AA (NSA) sufre robo de información y se empezó a filtrar información clasificada por parte de Edward Snowden y las permanentes actividades hacktivistas realizadas por el grupo Anonymous.

CIBERFRAUDE

Caso: SWIFT (2016)



Ataque mediante el compromiso de cuentas de funcionarios que realizan transacciones con la mensajería de SWIFT. Bangladesh Bank (2016) US\$81MM.



COMENTARIOS FINALES

Como hemos visto, en el actual proceso de transformación digital global, las Fakes News son parte de un sistema de desinformación masiva o en cadena principalmente por plataformas virtuales y con fines subrepticios que obedece a intereses o móviles vinculados a motivaciones políticas, de índole reputacional, fines económicos, contra la seguridad pública o nacional e incluso pueden tener impacto de ámbito regional, entre otros.



Este sistema de desinformación toma fuerza en la baja educación que aún predomina a nivel global respecto a condiciones básicas de seguridad o ciberseguridad para operar en el mundo virtual o ciberespacio y por el otro aspecto a la alta demanda de usuarios de mecanismos de comunicación / información. Hay un tema de GAP generacional.

Fuente: Deloitte: ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?



CAEN
ESCUELA DE POSGRADO

LA DESINFORMACIÓN, FAKE NEWS Y SUS IMPLICANCIAS EN EL ENTORNO INTERNACIONAL

Expositor:

José Marangunich R.

Doctor en Desarrollo y Seguridad Estratégica

Lic. Derecho y Ciencias Políticas

Master of Business Administration

Especialista en Crimen Cibernético

Lima, Abril 2021

