# GRADO DE CONOCIMIENTO DE CIBERSEGURIDAD DE LA GENERACIÓN DIGITAL

Oleguer Rocafull

GRAU EN SEGURETAT - INSTITUT DE SEGURETAT PÚBLICA DE CATALUNYA 2018

*“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad*, *pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores*.*”*

Kevin Mitnick

# Índice

# 1. Introducción

## 1.1. Hipótesis y objeto de estudio

Viendo el desconocimiento generalizado de la sociedad en materia de ciberseguridad, uno se pregunta si estamos preparados para los cambios tecnológicos que están teniendo todos los sectores productivos, así como nuestras vidas en general. Según los medios de comunicación, hay una generación preparada para ello, la llamada generación digital o nativos digitales. Han nacido con la informática y han vivido el big bang del mar de la información, así que sus relaciones personales y su forma de interaccionar están altamente influenciadas por el entorno digital. En este trabajo de investigación se quiere conocer si realmente esta generación está preparada para no sucumbir ante los ataques de los ciberdelincuentes que nos encontramos en la red.

Para empezar, a desarrollar nuestro trabajo, hemos de definir los términos con los que trabajaremos. Debemos saber a quién se denomina nativos digitales o generación digital. El término nativo digital fue acuñado por Marc Prensky, para él, son todas aquellas personas nacidas a partir del año 1979, ya que tuvieron a su alcance los primeros ordenadores personales. Es decir, empieza con la primera generación Y en sociedades altamente desarrolladas e incluso podríamos decir que en sus inicios sólo pudieron formar parte de dicha generación los que estuvieran altamente implicados en el uso de nuevas tecnologías y/o fueran de una clase media para arriba.

A partir del año 2000, el coste de la tecnología empezó a bajar de forma exponencial a la vez que la gran mayoría de hogares en España adquirió conexión a internet. Según datos de la ITU (International Telecommunication Union), en España había un 13,6% de los hogares conectados a internet en el año 2000, en el 2017 según el INE ya son un 83,4%. Es decir, estamos refiriéndonos a la generación que se fue desarrollando a la par que nacía la era de la información.

El problema de investigación quiere conocer la verdad acerca de esa generación digital. A pesar de saberse mover por la red y de utilizar nuevas tecnologías ¿son conscientes de los riesgos? ¿Qué grado de conocimiento disponen en materia de ciberseguridad? ¿Los medios han exagerado las virtudes de dicha generación? Ya que, si nos fijamos en la imagen que se ha inculcado en los medios de comunicación, dominan las redes cómo nadie y usan con gran facilidad todos los dispositivos que están entre sus manos. Entonces, ¿son verdaderamente conscientes de las consecuencias que tienen sus actos digitales? Y entraríamos a valorar ya no actos delictivos, sino la carencia de cuidado referente a la privacidad, publicar dónde están y qué hacen de forma pública: subir imágenes de su día a día, añadir desconocidos a sus redes sociales con mucha facilidad, etc.

Ante este planteamiento, la pregunta de investigación que debemos hacernos es la siguiente: ¿Qué grado de conocimiento en ciberseguridad tienen la llamada generación digital?

Primeramente, para responderla debemos entender de qué hablamos cuándo nos referimos a ciberseguridad. Si fuésemos simplistas e hiciéramos una definición, podríamos decir que el término ciberseguridad significa la ausencia de riesgos o peligros en el entorno cibernético, es decir, en las redes. No es una definición propiamente incorrecta, pero podemos echar en falta términos cómo disponibilidad, integridad, confidencialidad.

Si buscamos una definición estándar, una de las más completas quizás sería la que aprobó la ITU en 2010 en la Recomendación UIT–T X.1205 resolución 181.

*“La ciberseguridad es el conjunto de herramientas*, *políticas*, *conceptos de seguridad*, *salvaguardas de seguridad*, *directrices*, *métodos de gestión de riesgos*, *acciones*, *formación*, *prácticas idóneas*, *seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno*. *Los activos de la organización y los usuarios son los dispositivos informáticos conectados*, *los usuarios*, *los servicios/aplicaciones*, *los sistemas*

*de comunicaciones*, *las comunicaciones multimedios*, *y la totalidad de la información transmitida y/o almacenada en el ciberentorno*. *La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno*. *Las propiedades de seguridad incluyen una o más de las siguientes:*

- *Disponibilidad*
- *Integridad*, *que puede incluir la autenticidad y el no repudio*
- *Confidencialidad*."

En este estudio se acotará esta definición al usuario y no contemplaremos el término organización. Aunque la deficiente formación en ciberseguridad pueda resultar en un riesgo evidente para las organizaciones dónde los usuarios estén integrados, nos centraremos en el entorno personal de los mismos, y el motivo no es otro que focalizar nuestra atención hacia la raíz que pueda generar un foco de inseguridad.

La definición que usaremos será la siguiente, definida a efectos de conseguir la respuesta adecuada a este trabajo de investigación:

Entendemos por ciberseguridad ese conjunto de prácticas, herramientas, conocimientos, actos y tecnología que conducen a una ausencia de riesgos o peligros en el campo cibernético, así como la resiliencia ante posibles ataques. Cuando hablamos de riesgos o peligros se hace referencia a la integridad, disponibilidad y confidencialidad de los datos e información que son inherentes o generamos nosotros, así como dispositivos telemáticos.

Esta definición es la clave para tener claro cómo debemos responder nuestra pregunta de investigación, puesto que su definición indicará los términos en la que la respuesta ha de hacerse efectiva. Y en este punto, podemos empezar a deducir hipótesis razonables que den respuesta a nuestra pregunta de investigación. Tendremos dos muy claras y definidas.

- Los nativos digitales, que a pesar de conocer la red y estar familiarizados con los entornos tecnológicos, tienen graves carencias en ciberseguridad.
- Los nativos digitales son susceptibles a ataques de ingeniería social con poca capacidad técnica, parte de este colectivo no es capaz de detectar este tipo de ataques.

Con estas hipótesis empezamos a vislumbrar con qué tipo de variables trabajaremos. Si nos fijamos en las dependientes, acotaremos las siguientes:

- Edad
- Grado de uso de tecnologías de la información
- Nivel de autoprotección cibernética
- Percepción y opinión de la privacidad de sus datos

## 1.2 Marco teórico

Cuando empezamos a buscar marcos teóricos con en los que trabajar observamos que muchos de los estudios referentes a la generación digital tienen una clara orientación hacia el marketing. Vienen a definir el comportamiento de dicha generación, así como marcar pautas para que interactúen con la misma las empresas y organizaciones. En este sentido nos será útil para comprender pautas de comportamiento y consumo de dicha generación, pero no ahondan suficiente hacia la vertiente que queremos conocer.

Por otro lado, tenemos trabajos de investigación que podríamos definir como test de penetración a la sociedad. Es decir, realizan un test de seguridad informática a una población en concreto. Un buen ejemplo es “Users Really Do Plug in USB Drives They Find” (Matthew Tischer et al, 2016). En él, dejaron 300 memorias USB en 30 campus universitarios cómo si estuvieran perdidos para probar cuántos conectarían dicho dispositivo sin realizar un escaneo de seguridad. Cómo dichas memorias incluían software malicioso, pudieron verificar a través de una baliza digital la cantidad de usuarios que actuaron de forma inconsciente.

La realidad es que la tasa de ataque efectivo se encuentra entre un 45% y un 98% dependiendo del campus.

Estos estudios son un buen comienzo para empezar a entrar dentro de los conceptos que debemos trabajar: cómo es la generación digital y qué vulnerabilidades pueden tener en el entorno digital.

## 1.3 Metodología

A partir de aquí hemos de ver cómo recopilamos dichas variables para la realización de nuestro estudio y cuáles serán nuestras técnicas de investigación. El método más efectivo para la recopilación de datos a gran escala es el cuestionario. Es posible que no sea el que ahonde más en cuánto a profundidad al estudio, pero un buen análisis comparado puede darnos grandes respuestas.

Para simplificar nuestro estudio y ser coherentes con el tiempo y recursos de los que disponemos, acotaremos la población al ámbito de la provincia de Barcelona.

Para empezar, disponemos de los resultados de la encuesta AIMC 2017 que marca los patrones de conducta de los usuarios de internet en España. Es la mayor encuesta de dichas características realizadas en el país y la usaremos para determinar patrones de consumo y conducta en la generación que trabajaremos.

Continuaremos con una entrevista semiestructurada al Sargent de Mossos d'Esquadra Roger Martínez, jefe de la unidad de Ciberseguridad, para que nos cuente qué piensa él sobre la situación actual, así como de la generación digital.

Finamente realizaremos un experimento dónde se harán preguntas referentes a ciberseguridad y pequeñas pruebas para identificar entornos seguros o inseguros a través de imágenes. En este cuestionario se realizará un ataque phishing, es decir, un robo de credenciales usando ingeniería social mediante un formulario web que aparentará ser una web legítima. Por razones éticas, se

redactarán unas condiciones de participación previa al phishing en las que estableceremos que se realizará un experimento de ciberseguridad. Así mismo se informará a la responsable de proyectos de TFG sobre esta cuestión.

Además, obviamente este cuestionario será telemático, aunque esto suponga un sesgo, pues nos interesa que exista y así podremos confirmar que el uso del entorno no justifica los conocimientos en seguridad del mismo.

Para concluir la introducción, tenemos claras las limitaciones en cuanto a tiempo y recursos, pretendiendo realizar un estudio coherente con las mismas. Es decir, nuestro objetivo es dar respuesta, aunque sea a pequeña escala. Quizás sea un pequeño filón que pueda empezar a ser un objeto de estudio viendo la magnitud de repercusiones que puede el desconocimiento generalizado de la ciberseguridad. ¿La revolución de la era de la información esta solo a manos de unos cuántos o nuestra sociedad está preparada para afrontar su impacto?

# 2. Análisis de la Generación Digital en la provincia de Barcelona, encuesta AIMC

## 2.1 Introducción

Para este Trabajo de Final de Grado, en un primer momento se planteó realizar una encuesta para poder analizar el perfil de la generación digital, comprender sus pautas de comportamiento y consumo en el entorno digital. En lugar de realizarla directamente, haciendo una valoración de esfuerzo/resultado, se ha optado por trabajar con los datos de resultados de la encuesta que realiza la Asociación para la Investigación de Medios de Comunicación (AIMC) a usuarios de internet.

La AIMC es una entidad formada por un amplio grupo de empresas cuya actividad está relacionada con la comunicación. A continuación, se desgranan el número de empresas asociadas a la entidad y sus medios:

- 34 de diarios con 98 publicaciones distintas
- 10 de suplementos con 12 publicaciones distintas.
- 20 de revistas con 96 publicaciones distintas.
- 31 con 62 emisoras de radio.
- 29 del sector de la televisión.
- 2 del sector del cine.
- 23 de comunicación en sitios web con 31 portales distintos.
- 2 agencias de publicidad y 3 de publicidad exterior.

La encuesta fue realizada entre octubre y diciembre de 2017 y se trata de su 20ª edición, los resultados fueron publicados el 6 de marzo de 2018. En total la encuesta de esta edición ha recopilado un total de 15.252 respuesta válidas de usuarios que han participado de forma activa a través de enlaces distribuidos en más de 200 sitios webs.

Para hacer un trabajo más coherente en su conjunto se filtraron las respuestas en base a la población nacida de 1979 en adelante, la anteriormente nombrada

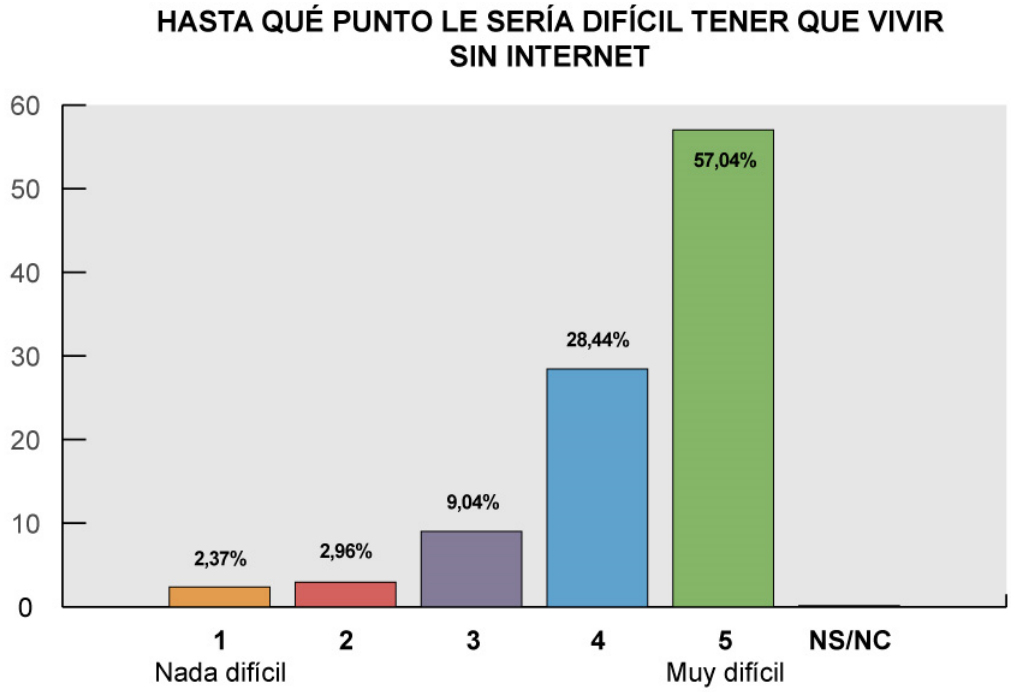
como generación digital, con residencia en la provincia de Barcelona, ya que el experimento que se realizará a posteriori se desarrollará en esa zona.

Una vez realizado el filtrado del cuestionario, y descartando toda respuesta que no cumpla con los anteriores requisitos, han resultado válidas 675 respuestas. Los datos han sido tratados con el programa de análisis estadístico SPSS, aprendido durante el Grado, ya que los datos proporcionados por AIMC estaban en este formato.

Se han realizado tablas de frecuencias con las cuestiones más indicadas a perfilar los hábitos de consumo y su percepción de (in)seguridad en la red.

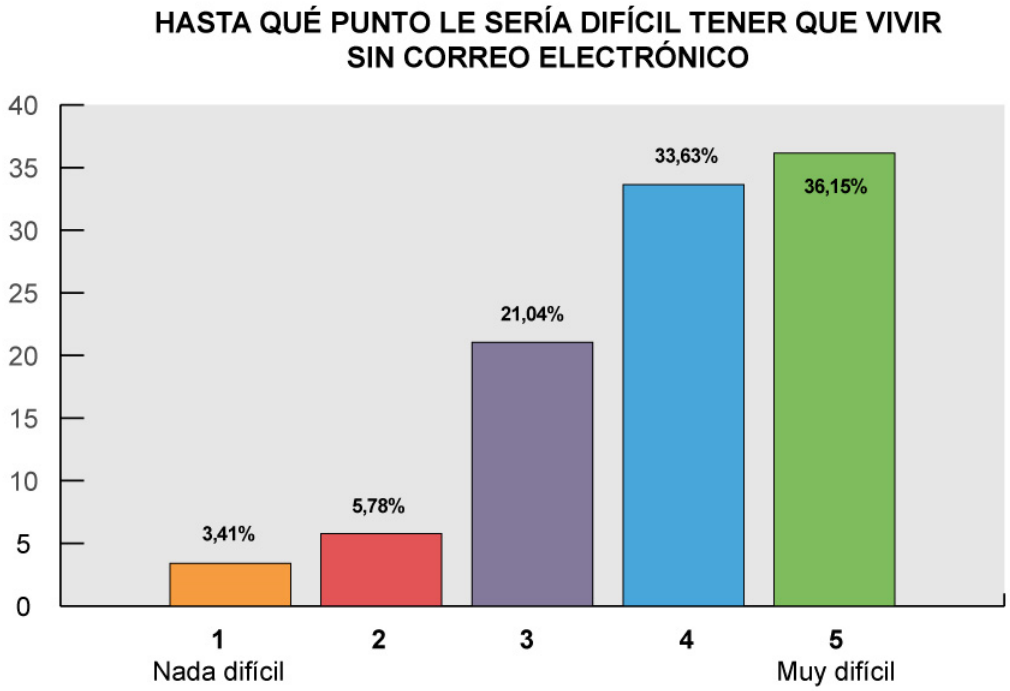
## 2.2. Hábitos y dependencias de consumo

Para empezar, se tratará una serie de cuestiones clave para ver la dependencia tecnológica de esta generación. En esta primera gráfica se pregunta: "¿Hasta qué punto le sería difícil tener que vivir sin internet?".



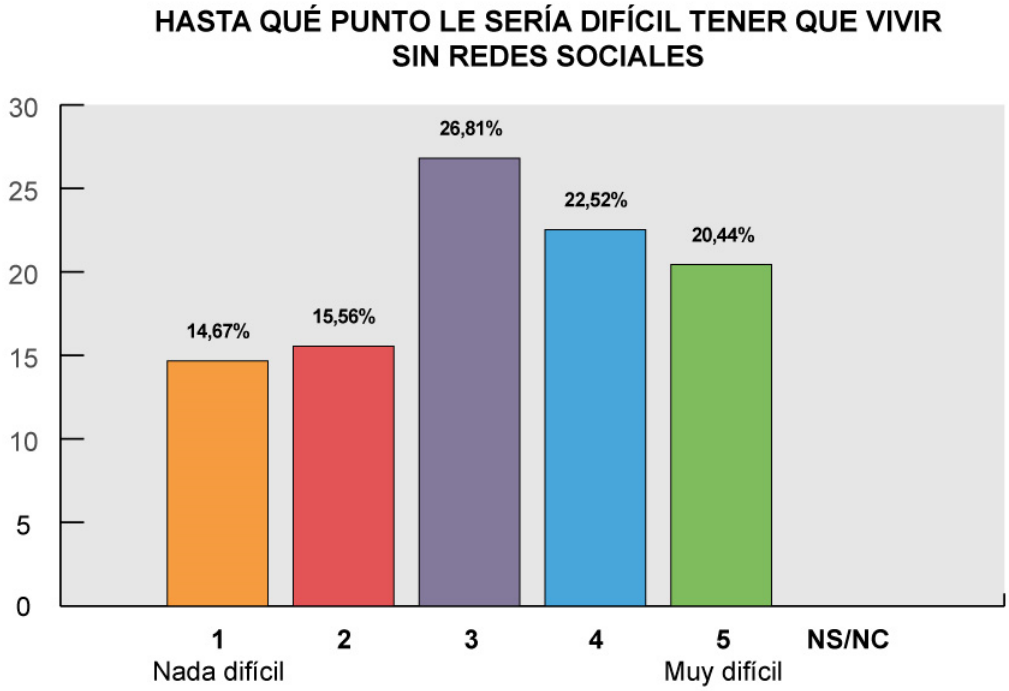
Nos encontramos que más de la mitad, un 57,04% les sería muy difícil, y un 85,48% han respondido difícil o muy difícil. Es decir, más de 8 de cada 10 de los encuestados tienen una importante dependencia de internet en su día a día. Con esta respuesta nos podemos hacer una idea de las pautas de consumo que seguiremos analizando de aquí en adelante.

En la siguiente, hace referencia a la dependencia del uso del correo electrónico, ya vemos que las cifras disminuyen, pero no son nada despreciables, un 36,15% consideraría muy difícil vivir sin correo electrónico, y si valoramos los que lo consideran muy difícil o difícil pasamos a un 69,78%.



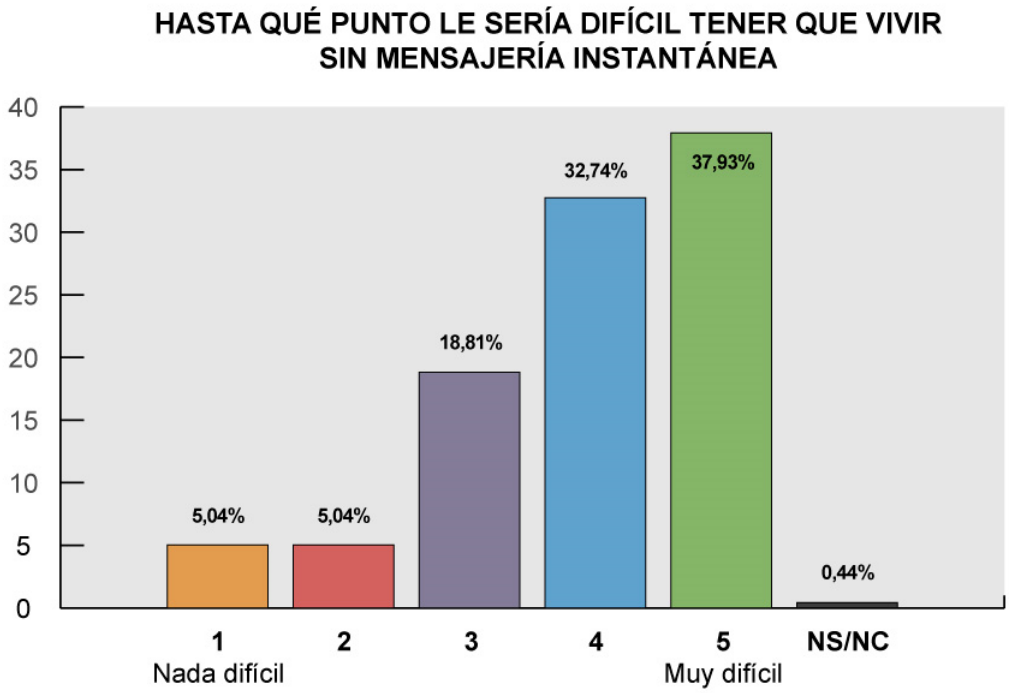

Es decir, prácticamente 7 de cada 10 tendrían dificultades por su dependencia en este tipo de comunicaciones. Nos encontramos que tan sólo un 9,19% no tendría nada de dificultad, o apenas tendrían dificultad para vivir sin correo electrónico.

La siguiente pregunta hace referencia a las redes sociales, y siguiendo la estela de las cuestiones anteriores, si sería difícil vivir sin ellas.



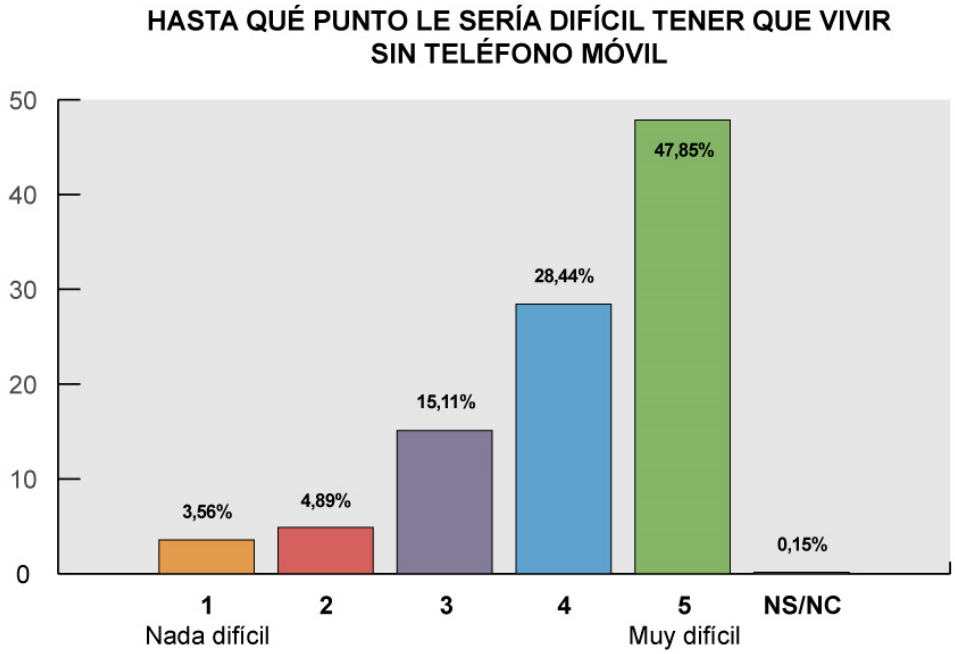

Esta cuestión realmente ha dado resultados muy segmentados. La valoración de 3, siendo “1 nada difícil” y “5 muy difícil”, ha sido la que ha aglutinado más respuestas con un 26,81%. Si nos fijamos en una valoración global podemos decir que, en general, ha ganado la opción de que sería difícil vivir sin redes sociales. Con la suma de las valoraciones 4 y 5 nos encontramos con un resultado de 42,96%, mientras que las valoraciones de 1 y 2 agrupan un 30,23%. En definitiva, a pesar de ser una pregunta bastante polarizada, la muestra indica que mayormente tendrían dificultad en vivir sin redes sociales.

Seguimos con la dificultad ahora a vivir sin mensajería instantánea. En este caso se han obtenido unos resultados con una tendencia similar a la de vivir sin correo electrónico. En esta pregunta se hace referencia a aplicaciones tales como Whatsapp, Telegram, Facebook Messenger, Signal y demás aplicaciones con las que podemos enviar mensajes y comunicarnos de forma instantánea.



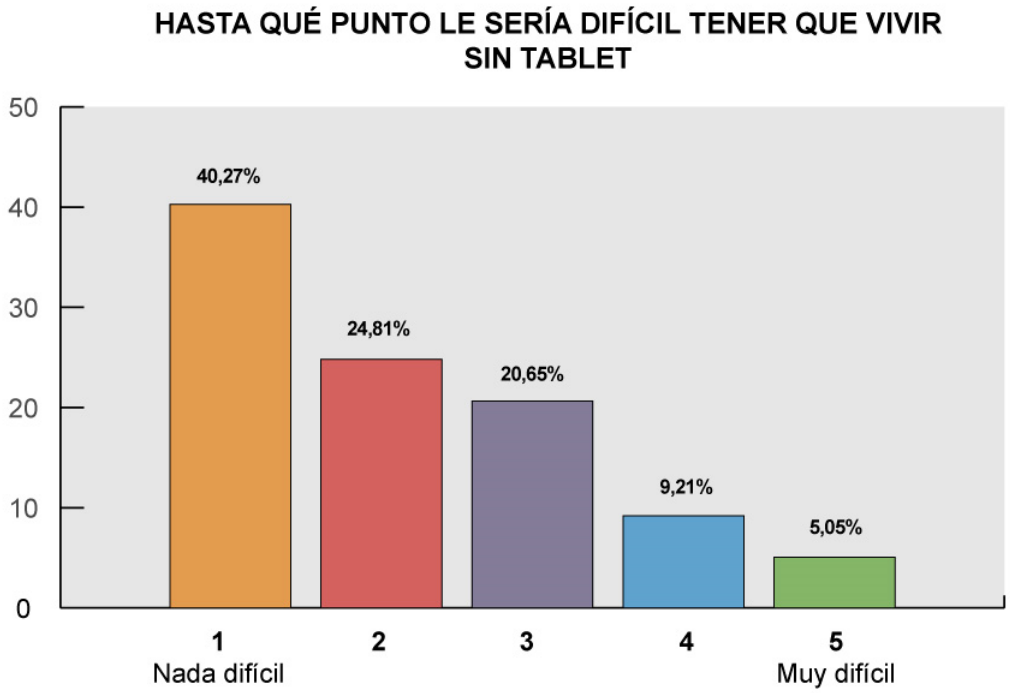

En este caso nos encontramos que un 37,93% les resultaría muy difícil, y si lo agrupamos con los que les resultaría difícil (4), obtenemos un 70,67%. Tan solo un 10,08% encontrarían poco o nada difícil vivir sin mensajería instantánea y, de hecho, como en el caso del correo electrónico, 7 de cada 10 considerarían difícil o muy difícil vivir sin poder usar este medio de comunicación.

A continuación, analizaremos los resultados referentes, ya no a aplicaciones o medios, sino a la dificultad de vivir sin un teléfono móvil o una Tablet.



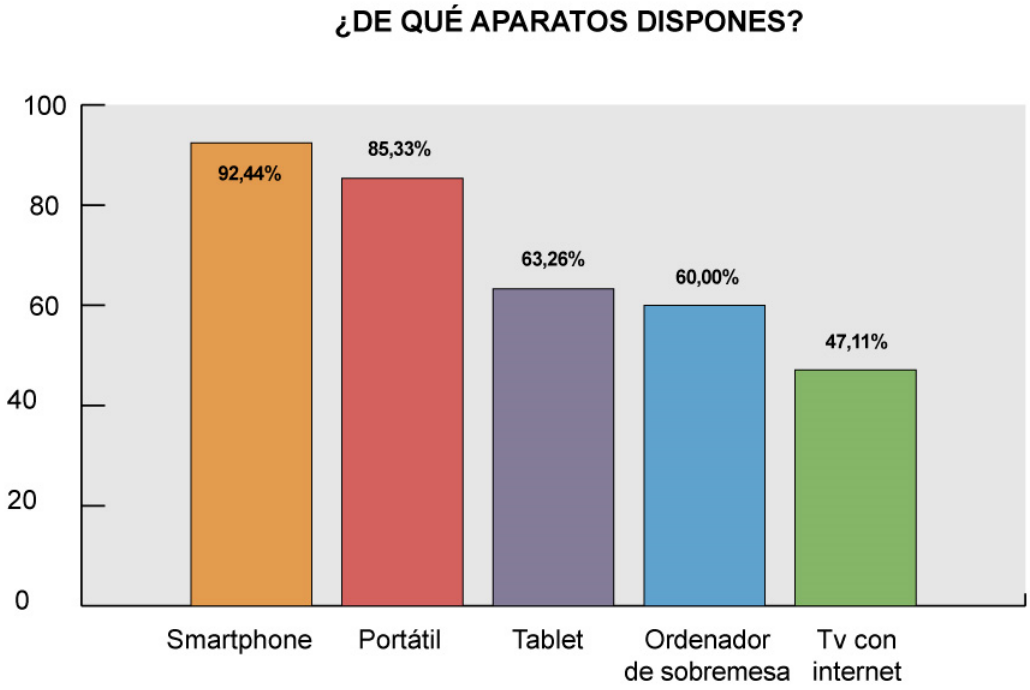

En el caso del teléfono móvil, se puede apreciar que un 47,85% vería muy difícil vivir sin él, es decir, prácticamente la mitad de la muestra. Si se agrupa este porcentaje con los que lo verían difícil (4), llevamos hasta un 76,29%, una cifra muy elevada. Por ello podríamos decir que 3 de cada 4 tienen una fuerte dependencia del teléfono móvil en su día a día, y eso teniendo en cuenta que no el total de esta generación ha nacido con el teléfono móvil en circulación, una gran parte de ella lo ha visto nacer y desarrollarse. El porcentaje de los que les resultaría poco o nada difícil se queda en un 8,45%.

La siguiente tabla hace referencia a la Tablet, un producto que fue un boom unos años atrás y del que se decía que sustituiría al ordenador.



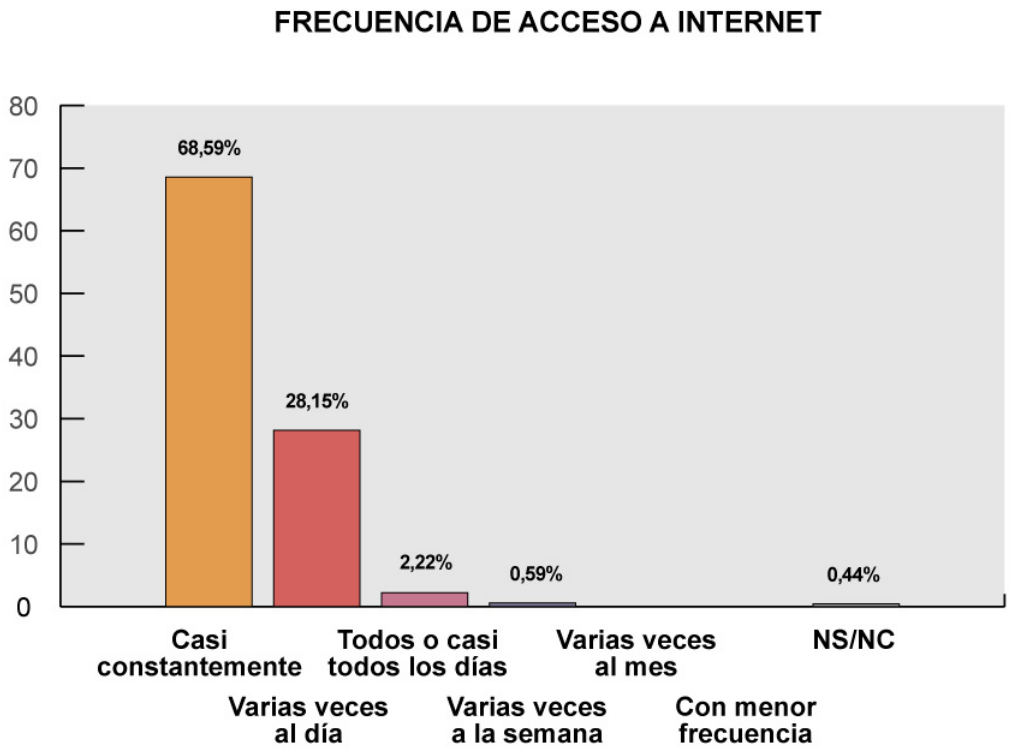

Para un 40,27% no les sería nada difícil vivir sin Tablet. Si aglutinamos el resultado con los que respondieron poco difícil nos quedamos con un 65,08%. Si nos fijamos en el otro extremo, para un 5,05% de la muestra les sería muy difícil vivir sin Tablet. Es decir, aunque un 63,26% de los encuestados dispongan de Tablet (se podrá visualizar en el siguiente gráfico), no sienten una dependencia de ella en comparación con el smartphone.

A continuación, veremos de qué tipo de aparatos digitales dispone la muestra, aunque por supuesto tener un dispositivo no hace incompatible que se posea algún otro.



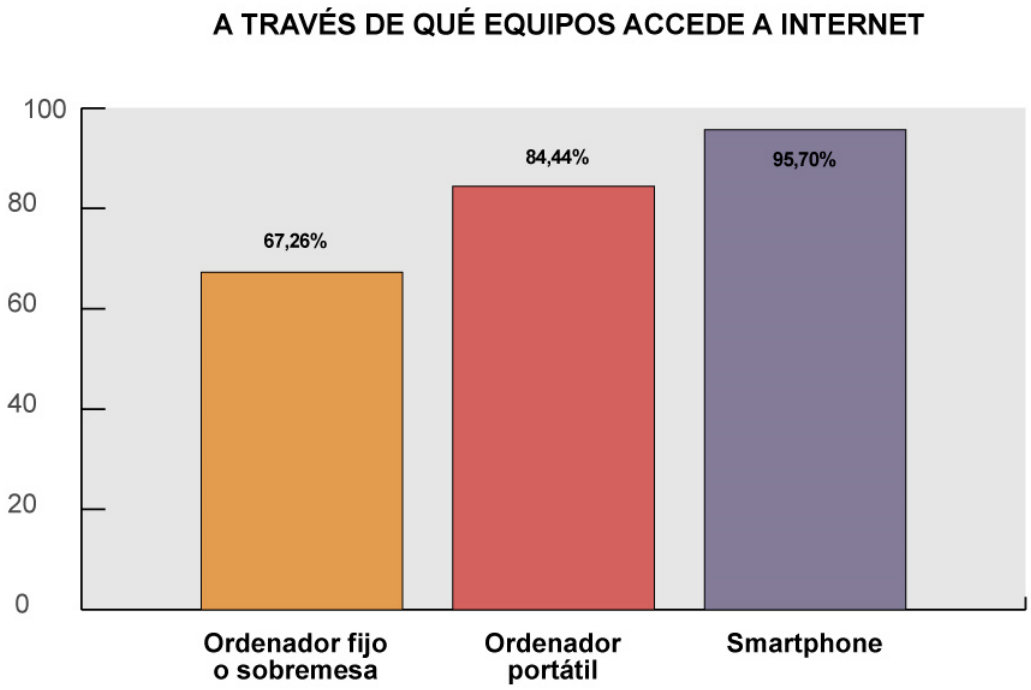

Un 92,44% dice tener un smartphone, a priori una cifra muy alta que más adelante rebatiremos si es correcta cuando la comparemos con el uso de servicios de mensajería instantánea. El siguiente producto que más dispone la muestra es de ordenador portátil con un 85,33%, en tercer puesto la Tablet con un 63,26%, ordenador de sobremesa con un 60% y televisor con conexión a internet un 47,11%. Con estos datos, podemos observar que se trata de una generación que en su gran mayoría dispone de múltiples dispositivos desde los que conectarse a internet.

Veremos ahora la frecuencia de acceso a internet. En este caso nos encontramos una cifra extremadamente alta y significativa.



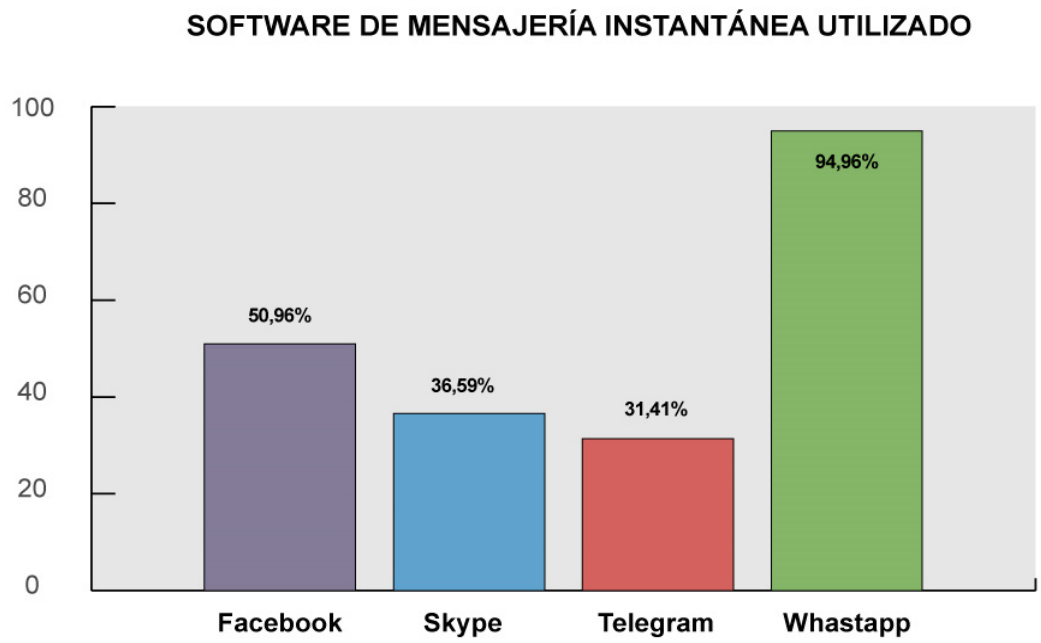

Un 68,59% afirma que está conectado de forma casi constante y un 28,15% lo hace varias veces al día. En total un 96,74% se conecta varias veces al día, la gran mayoría de forma casi constante. Un dato que nos justifica su dependencia y la respuesta anteriormente comentada sobre la dificultad de vivir sin internet. A tener en cuenta que un 2,22% se conecta todos o casi todos los días, mientras que un 0,59% varias veces a la semana.

Cómo podremos ver en la siguiente gráfica, se trata de una generación que trabaja multidispositivo.




A destacar que un 95,70% se conecta a través del móvil. Esta respuesta no concuerda con las personas que decían poseer un smartphone (92,44%), aunque existen modelos no smartphone que permitían conexión a internet con grandes limitaciones (sistema WAP), pero se considera que es más plausible que ese porcentaje de diferencia de los encuestados, 3,26%, no comprendiera el término smartphone. A destacar también el uso del ordenador portátil con un 84,44% seguido del ordenador de sobremesa con un 67,26%.

Entrando en los resultados de la pregunta, “¿Qué software de mensajería usas?”, nos encontramos un claro y evidente vencedor a día de hoy: Whatsapp, con un 94,96% de resultados.



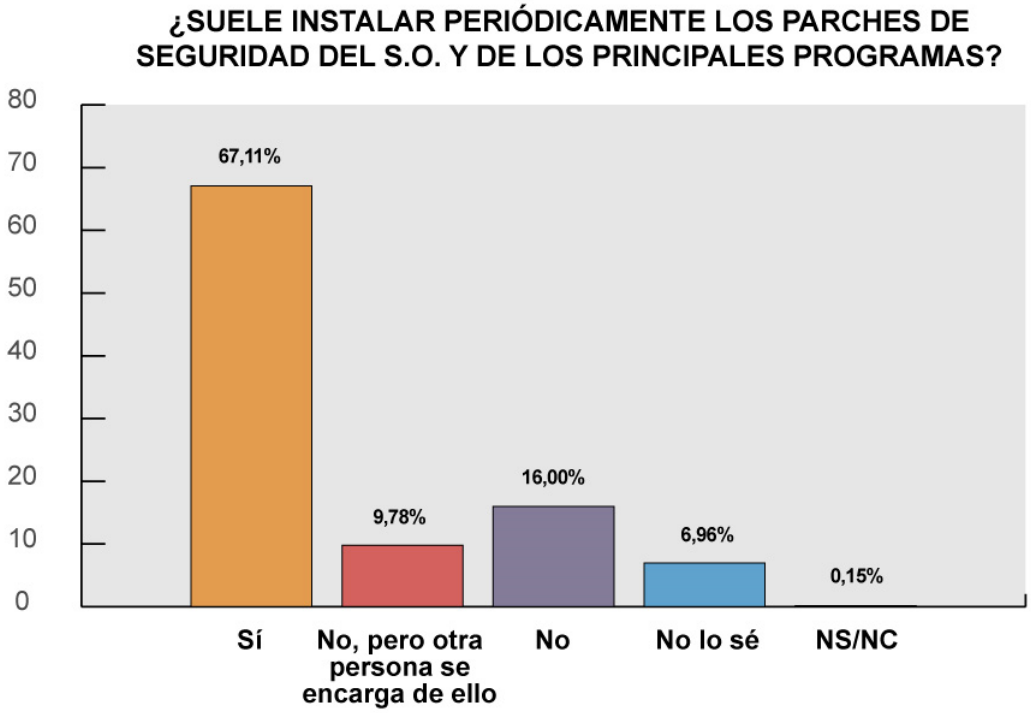

Como en la anterior cuestión, podemos argumentar el error de cierto porcentaje, un 2,52% que dice no tener smartphone, pero si utilizar Whatsapp. Algo ciertamente improbable, aunque factible a nivel técnico usando Whatsapp a través de Tablet y no de móvil, usando el móvil para registrar la aplicación que posteriormente se instalaría en la Tablet.

Al ser el sistema de mensajería más usado, ya empezamos a ver ataques de ingeniería social que se propagan a través de él, se adjunta ejemplo recibido:

La siguiente aplicación con más uso y a bastante distancia es Facebook Messenger, el sistema de mensajería de la conocida red social, usada por un 50,96% de la muestra. Cabe mencionar que la encuesta de la AIMC se realizó antes del escándalo de Cambridge Analytica, así que puede haber alteraciones en cuanto a su uso actualmente. Le siguen Skype con un 36,59% y Telegram con un 31,41%.

## 2.3 Percepción de seguridad en la red

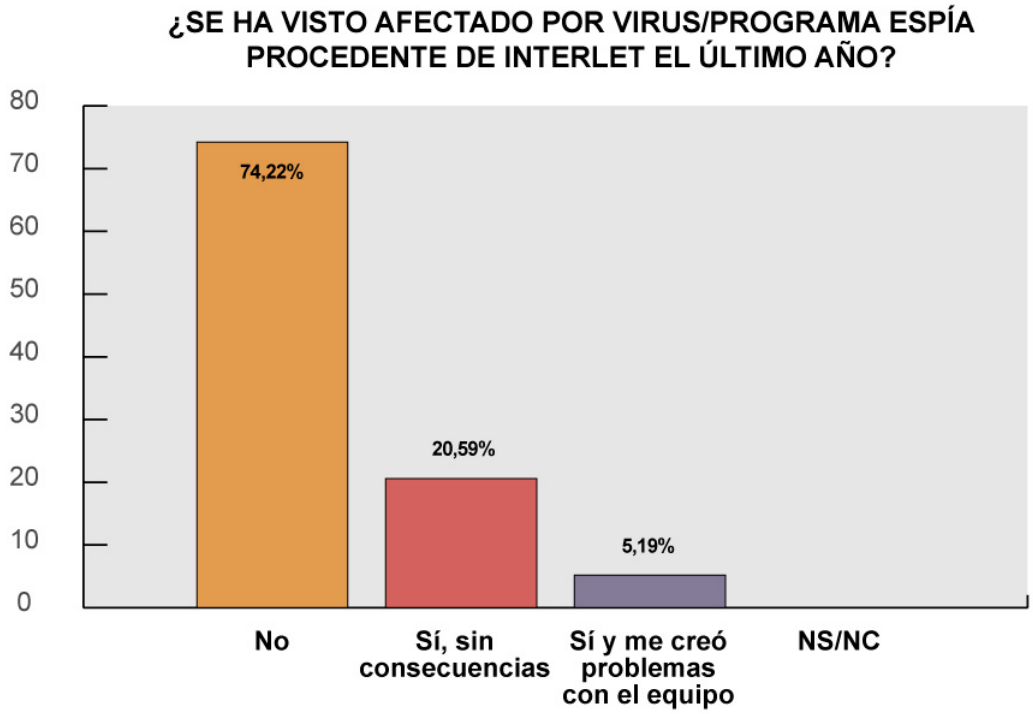
La siguiente cuestión es relativa a ciberseguridad, en concreto si los usuarios están pendientes de las actualizaciones de seguridad de los sistemas operativos y programas que utilizan.




En este caso nos encontramos que un 67,11% responden que sí lo hacen, mientras que un 16% no. Nos queda un 9,78% que indican que lo hace otra persona y un 6,96% que no lo saben.

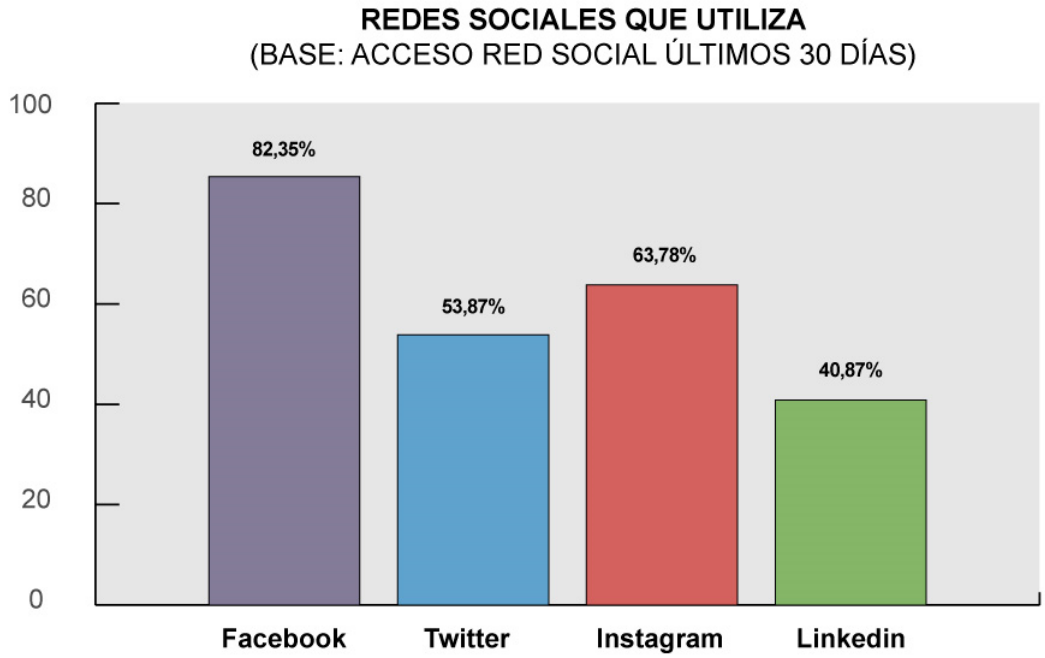
Hoy en día, la actualización de parches de seguridad es prácticamente automatizada, sólo tenemos que darle la confirmación cuándo nos salta el aviso, tanto en un entorno de escritorio cómo móvil. Resulta sorprendente que una generación con un extensivo uso de las tecnologías y de dispositivos conectados a internet, exista un perfil de usuarios que no realicen dichas actualizaciones o que incluso lo desconozcan.

En la siguiente cuestión los encuestados responden si se han visto afectados por un virus o un programa espía, donde un 74,22% respondió que no, mientras un 20,59% respondió que sí se vio afectado y sin consecuencias, sólo quedando un 5,19% que sí sufrieron un ataque y les creó problemas en su equipo.



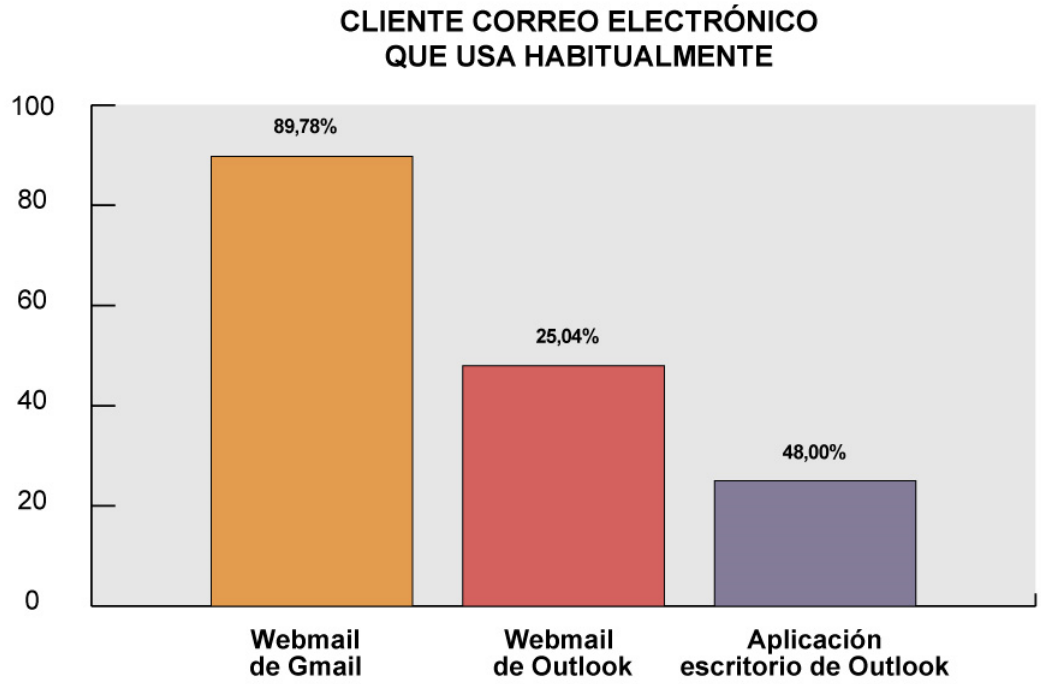

Si valoramos todos los que han sufrido un ataque de la muestra de este año son un 25,78%, es decir, 1 de cada 4 se ha visto afectado por un virus o programa espía. De este subgrupo, en 1 de cada 5 además les ha creado problemas en el equipo. Posteriormente realizaremos un experimento y valoraremos los resultados con estos datos.

En el siguiente gráfico podremos visualizar las redes sociales visitadas por nuestra muestra en los últimos 30 días.



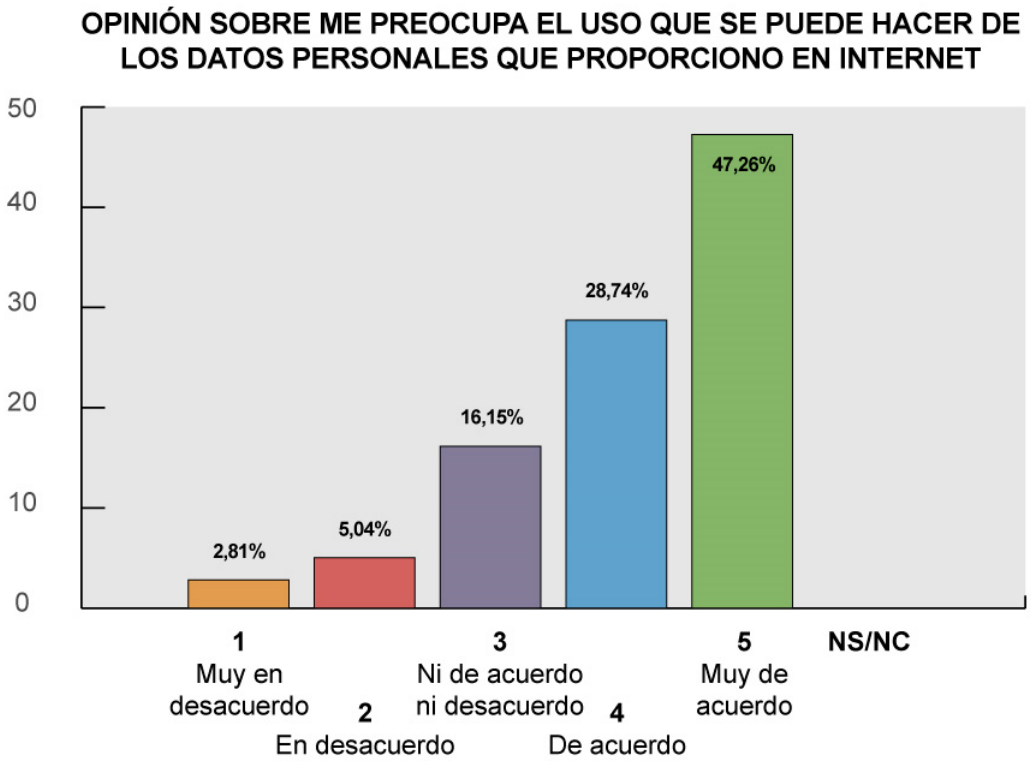

Encontramos un claro predominio de Facebook con un 82,35%. Como hemos comentado anteriormente, sería interesante visualizar los efectos que ha producido la crisis de privacidad sufrida a raíz de la filtración masiva de datos de Cambridge Analytica. No disponemos de capacidad para comprobarlo en estos momentos, puesto que no hay ningún estudio en la zona que pueda utilizarse, pero será clave la encuesta de AIMC del siguiente año para comprobar si ha tenido efectos. Tras Facebook nos encontramos con Instagram con un uso del 63,78%, Twitter con un 53,87% y finalmente la red social laboral Linkedin con un 40,87%.

Seguiremos con el cliente web que utilizan habitualmente los sujetos de nuestra muestra en el entorno de escritorio, si bien es cierto que el uso de uno de ellos no lo hace incompatible con los demás.



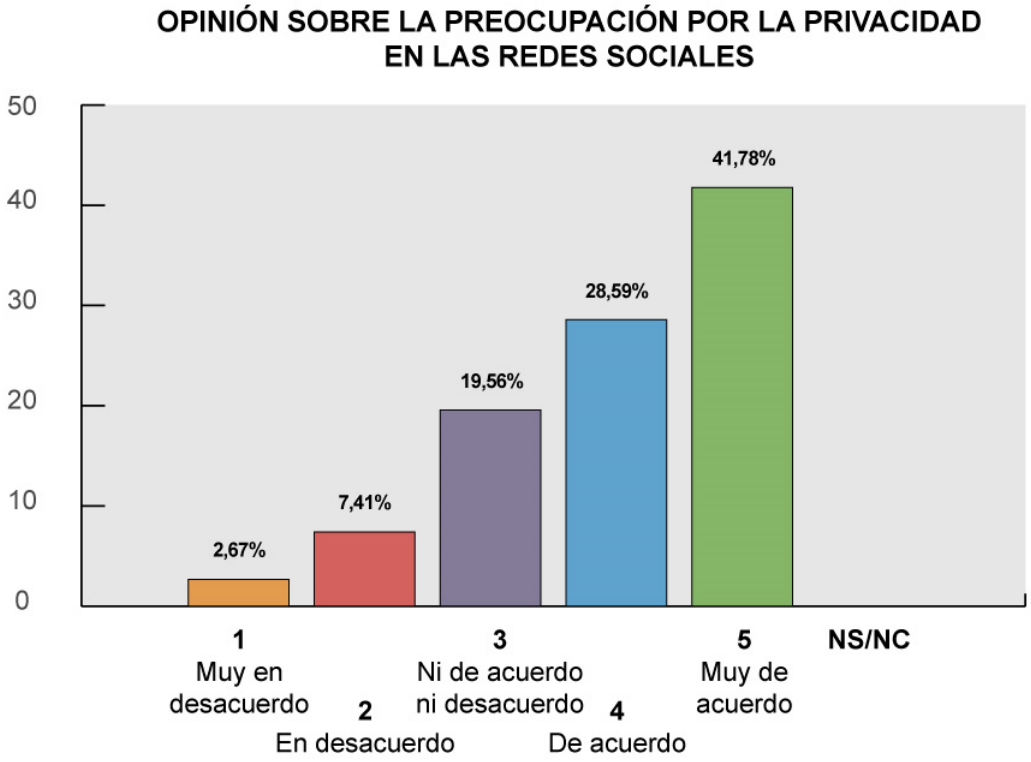

En este caso nos encontramos una clara predilección por el webmail de Gmail, el sistema de correo electrónico de Google, con un 89,78% claramente influido por el predominio de Android en el mercado móvil. Le sigue el cliente webmail de Outlook (antiguo Hotmail) con un 48% y finalmente la aplicación de escritorio Outlook con un 25,04%.

En las siguientes cuestiones nos centraremos en la opinión que tienen los usuarios sobre asuntos de privacidad de sus datos en la red, se responderá en una escala del 1 al 5, dependiendo si están muy en desacuerdo (1) o muy de acuerdo (5) con una afirmación. La primera en este aspecto es “Me preocupa el uso que se puede hacer de los datos personales que proporciono en internet”.



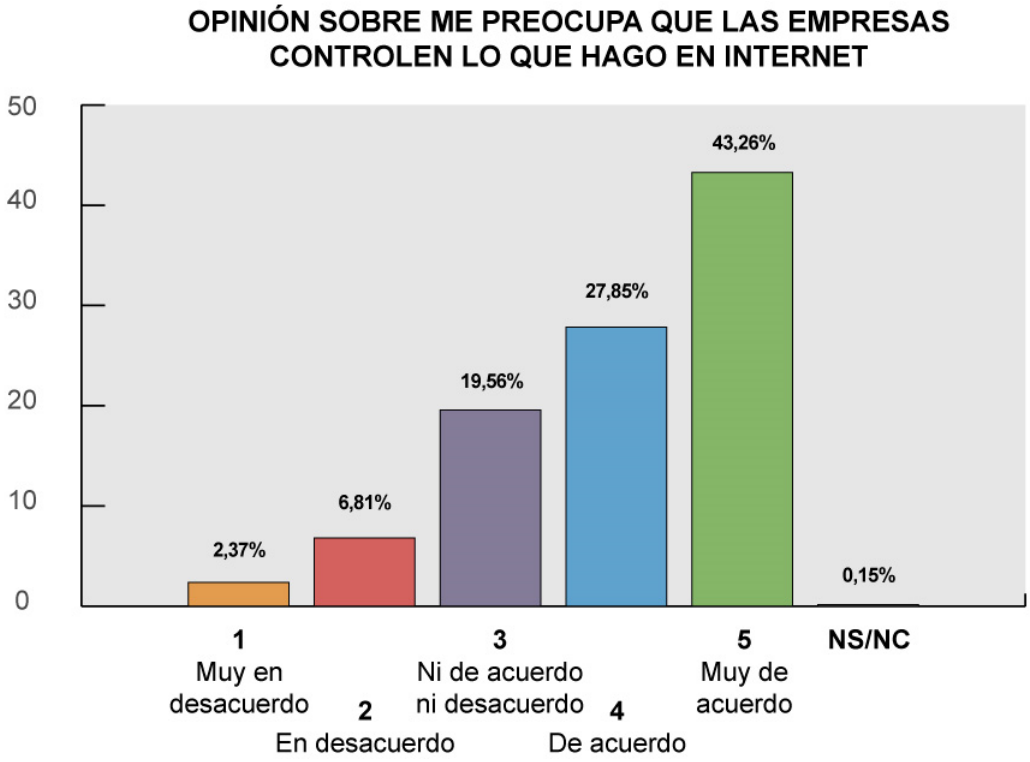

Un 47,26% estaba muy de acuerdo y un 28,74% estaba de acuerdo. En este sentido, los que se muestran preocupados, valores 4 y 5, son un 76% mientras que los que están muy en desacuerdo son un 2,81% y en desacuerdo un 5,04%. A modo de resumen, 3 de 4 está preocupado por los datos que proporcionan en internet.

En el siguiente gráfico veremos los relativos a “Me preocupa la privacidad en las redes sociales”.



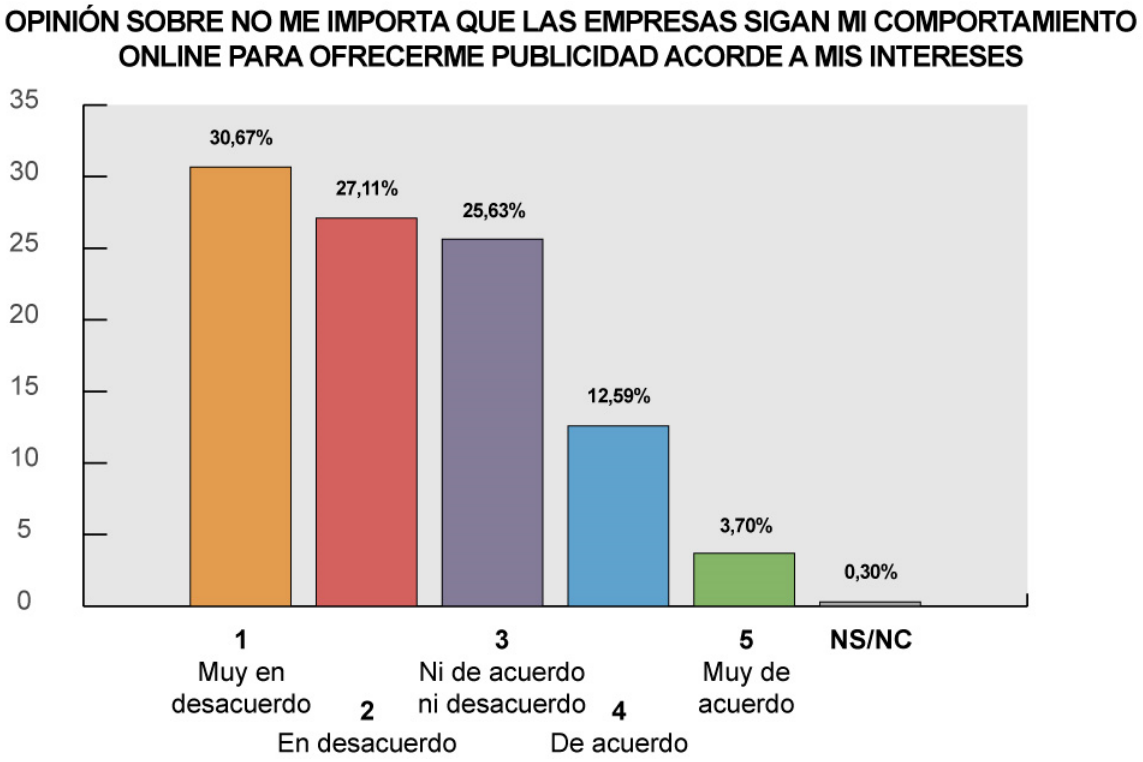

Muy parecido a la afirmación anterior, nos encontramos con un 41,78% muy de acuerdo y un 28,59% de acuerdo. En total un 70,37% le preocupa la privacidad en las redes sociales, frente a un 2,67% que se han mostrado muy en desacuerdo y un 7,41% en desacuerdo, en total un 10,08% que no están de acuerdo con dicha afirmación.

Continuaremos con la afirmación: “Me preocupa que las empresas controlen lo que hago en internet”.



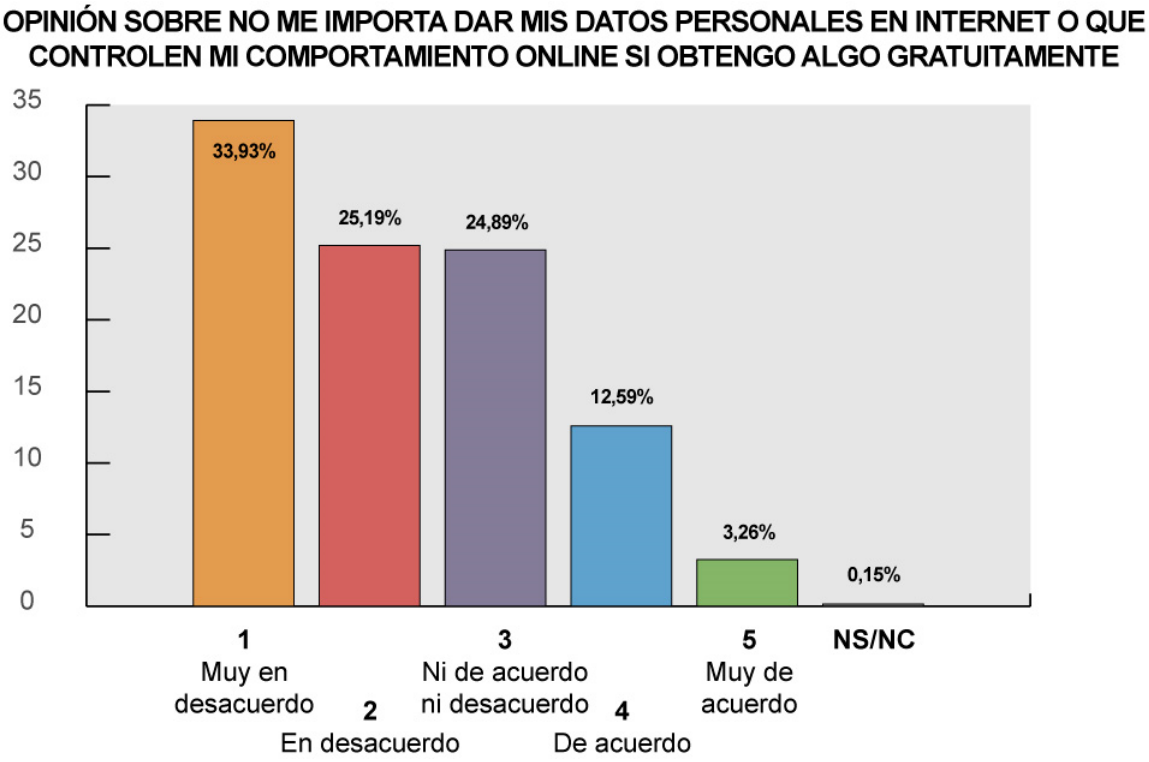

En este caso vemos como un 43,26% declara estar muy de acuerdo con la afirmación. Conjuntamente se está de acuerdo un 27,85%, muy en desacuerdo tenemos un 2,37% y en desacuerdo un 6,81%. Si agrupamos lo resultados podemos ver que los que están en acuerdo con dicha afirmación (en mayor o menor medida) son un 71,11% mientras lo que se muestran mayoritariamente en desacuerdo representan un 9,18%.

Seguiremos con una afirmación que hace referencia a las cookies y trackers que almacenan nuestras pautas, búsquedas e incluso correos electrónicos para ofrecer publicidad personalizada a nuestros intereses. La afirmación es en clave negativa: “No me importa que las empresas sigan mi comportamiento online para ofrecerme publicidad acorde a mis intereses”.



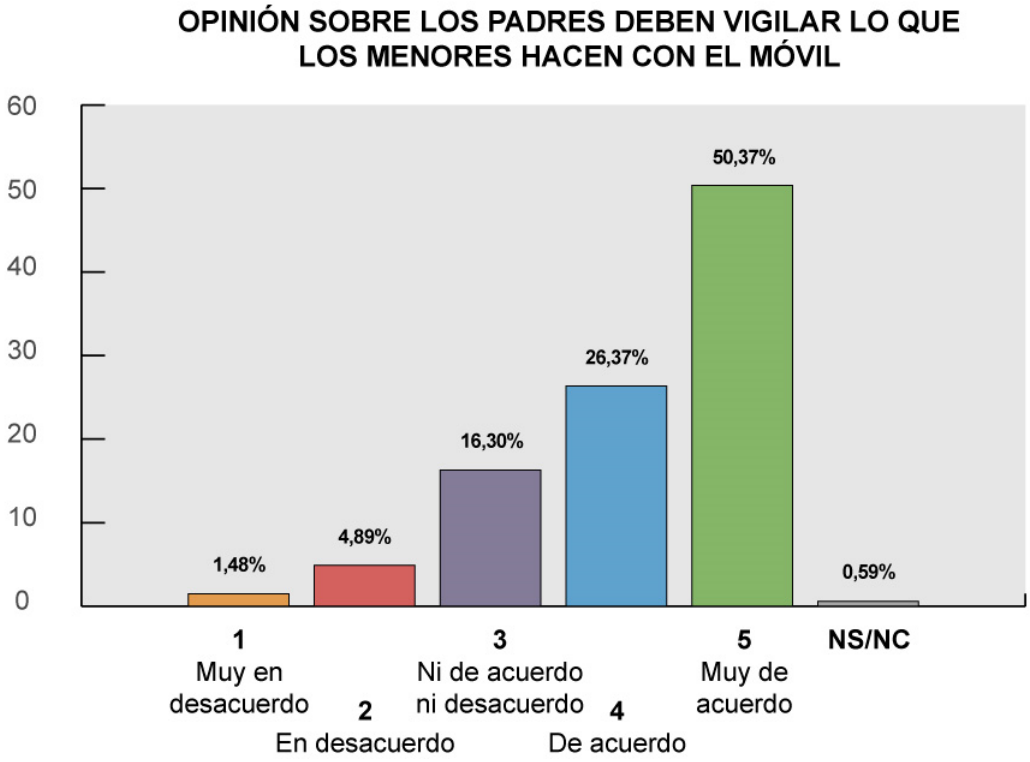

Un 30,67% se mostró muy en desacuerdo y un 27,11% se mostró en desacuerdo. De acuerdo vemos un 12,59% y muy de acuerdo un 3,70%. Los que sintieron indiferencia a esta afirmación alcanzan un 25,63%.

La siguiente afirmación también es negativa: “No me importa dar mis datos personales en internet o que controlen mi comportamiento online si obtengo algo gratuitamente”.




Un 33,93% se muestra muy en desacuerdo y en desacuerdo un 25,19%, en la misma línea que la anterior. En el extremo opuesto, un 3,26% está muy de acuerdo y un 12,59% de acuerdo. Los indiferentes representan un 24,89%.

La siguiente afirmación hace referencia a la vigilancia de lo que hacen los menores usando el móvil: “Los padres deben vigilar lo que los menores hacen con el móvil”.




En ella, un 50,37% se muestra de muy de acuerdo y un 26,37% de acuerdo. Es decir, un 76,74% estaría de acuerdo con los sistemas de control parental en los dispositivos de los menores, mientras que un 1,48% se mostraría muy en desacuerdo y un 4,89% en desacuerdo. En conclusión, un 6,37% desaprobarían la vigilancia.

## 2.4. Conclusiones

Podemos concluir que es posible definir un perfil estándar de la generación digital en la provincia de Barcelona. Éste tiene una alta dependencia de internet, servicios de correo y mensajería instantánea. Además, está conectado de forma permanente a internet, dispone de smartphone y ordenador portátil y utiliza como correo el servicio de Gmail a través de webmail. La red social que más utiliza es Facebook junto con Instagram y no siente que sea dependiente de ellas. Le preocupa la privacidad de sus datos, así como el uso que se hace de ellos y cree en la monitorización del uso del móvil por parte de los padres de un menor.

## 3. Entrevista al Sargent Roger Martínez

Para hacernos una idea de la situación actual hemos querido contar con un experto que trabaje en su día a día con delitos informáticos. Hemos podido contar con Roger Martínez, Sargent de Mossos d'Esquadra y jefe de la unidad de Ciberseguridad, cargo que ocupa desde Julio de 2014. Es graduado en Gestión y Derecho de la seguridad por la Universidad Autónoma de Barcelona y además es Certified Information Security Manager por CISM – ISACA, Deloitte Certified Ethical Hacking Associate, así como Director de Seguridad.

A petición del entrevistado no se adjuntará la transcripción de la entrevista. Se desarrollarán las respuestas y valoraciones que ha dado a las preguntas realizadas. A tener en cuenta que la entrevista ha sido realizada en catalán y, por lo tanto, sus expresiones han sido traducidas, procurando que sea de la forma más fidedigna posible.

1. ¿Como está la situación delictiva en el ámbito de la Ciberseguridad en Cataluña? Refiriéndome desde el punto de vista de las personas y no de las organizaciones.
2. ¿Cuáles son las prácticas delictivas más habituales?
3. Explica qué grado de vulnerabilidad crees que tiene nuestra sociedad en este ámbito.
4. ¿En este sentido, crees que la cifra negra en estos delitos es muy elevada?
5. ¿Cuál crees que es el nivel de conocimientos en materia de Ciberseguridad de la sociedad? ¿Y en concreto, de la generación digital?
6. ¿Crees que los agentes de Mossos d'Esquadra están preparados y tienen conocimientos suficientes en esta materia?
7. ¿Qué crees que falla en la sociedad para que haya esta disrupción entre avance de las tecnologías de la información y los conocimientos de la gente?

8. ¿Crees que la administración da suficiente información de los riesgos de internet?

   Roger Martínez empieza indicándonos que la situación de Catalunya no es distinta de la que nos encontramos en Europa, tenemos las mismas tendencias delictivas en el ámbito de la ciberseguridad. Al final, por mucha sofisticación técnica que tenga el malware, habitualmente acaba entrando a través de un phishing y si *"esta persona no tiene la sensibilización adecuada*, *o no es capaz de identificar una cabecera extraña*, *abre el PDF y inicia la parte técnica del ataque […] el phishing continúa y continuará siendo el ataque por excelencia*, *ya sea por spam muy generalizado o un ataque dirigido"*.

   El Sargent prosigue narrándonos lo que a su parecer es el estado de la sociedad actualmente en materia de ciberseguridad "*aún está en la infancia*, *desde pequeños nuestro entorno nos ha inculcado que cosas nos pueden generar riesgo físico: no pases por ese callejón de noche […] actualmente en el entorno digital tenemos una falsa sensación de seguridad*, *nuestra realidad física es que estamos en el sofá de casa*, *cómodo y la percepción de seguridad es alta*. *Tú no eres consciente que es página web está ejecutando un control Active X o tiene un Javascript incrustado que puede hacer peligrar tus datos*, *tu economía*, *tu reputación digital*, *etc*. *Todo eso no se percibe de una forma tan clara cómo se percibe en la realidad*."

   Según el Sargent Martínez, tan sólo comparando las estadísticas de grandes fabricantes del sector de la ciberseguridad con estadísticas policiales o judiciales en cuánto a denuncias o condenas, vemos que hay una discrepancia muy grande. Continúa añadiendo *"Es muy difícil que una persona en el entorno físico sufra una agresión y no lo denuncie*, *una persona cuándo sufre un robo denuncia*, *en el ámbito digital*, *aún hay muchísimos casos que la agresión o acoso no son denunciados*. *Aún no se percibe como una cosa real*. *La gente aún hace diferencia entre lo que*

*es real y lo digital*. *Las dos cosas son extremadamente reales*, *lo que pasa es que una cosa ocurre en el plano físico de nuestro entorno y lo otro en un plano virtual que está en la red*. *Pero las dos son igual de reales y el impacto que tiene sobre las personas u organizaciones es muy real*." Referente a la cifra negra, el Sargent nos dice que el problema reside en que los denunciantes no saben cómo ni cuándo se ha producido el delito *"He sido yo*, *que sin saberlo tenía una pantalla superpuesta y tengo un virus*, *no lo tengo ¿es el teléfono lo que está infectado? Al final esa persona denuncia un movimiento no autorizado*, *básicamente para que el banco le devuelva el dinero"*.

Referente a cómo combatir el cibercrimen y reducir cifras nos cuenta que no *"los recursos disponibles a nivel social y de la administración no permiten que cada uno de estos casos sea investigado con un análisis forense de su dispositivo para determinar si saber si la persona ha caído en un phishing*, *que no era ni técnicamente sofisticado o si estaba infectado con un malware específico para su tipo de banco*, *entonces claro*, *la cifra oculta es altísima"*.

Cuando hablamos del nivel que pueda tener la generación digital, comenta que en este sentido es pesimista, que es una generación que ha tenido desde bien pequeños dispositivos a su alcance y que los controlan de forma ágil y *"eso es percibido por sus padres como una habilidad o capacidad del niño […] no confundamos la capacidad de interactuar con el dispositivo*, *que al final son dispositivos pensados para ser usables*, *con el saber y conocer lo que están haciendo"*. Prosigue contando que esta generación está integrada en multitud de redes sociales, están conectados continuamente a internet con diversos dispositivos, pero que, si les preguntas acerca de mecanismos básicos de seguridad, el desconocimiento es alto, eso sí, quizás no tanto cómo sus padres.

Referente a la formación de Mossos en este ámbito, nos explica que se están haciendo esfuerzos para capacitarlos y formarlos, para que al poder coger una denuncia esta tenga una redacción correcta a nivel legal. Se publican manuales, se realizan cursos de formación y actualización y en las nuevas promociones el curso básico integrará estos conocimientos. Y añade *"Al final hay una realidad*, *y es que la edad de los Mossos es la que es*, *no es precisamente de 20 años*. *[…] Y al final la policía es un reflejo de la sociedad*, *evidentemente tienes unos conocimientos legales*, *sobre el crimen y cómo combatirlo*, *pero hay carencias"*. Y añade, *"para eso estamos las unidades especializadas"*. A pesar de eso, Martínez cree que se está trabajando mucho para revertirlo, y en la buena dirección.

Acerca de la disrupción entre avances tecnológicos y conocimientos de la sociedad, Martínez opina que es debido a intereses tecnológicos y empresariales y que los usuarios no piden medidas de seguridad, sino ítems que tienen que ver con la experiencia de usuario. Ya sea porque dan por hecho la seguridad o no percibe la inseguridad. Añade que los fabricantes incorporan medidas de seguridad por dos razones: por una normativa que les obliga o por una fuerte demanda social. En este sentido cree que el legislador es el que tiene fuerza para presionar a los fabricantes y comenta *"Tú puedes tener un juguete para un niño*, *que necesariamente tiene que pasar una serie de controles antes de poder estar a la venta […] Este mismo dispositivo puede tener una webcam que interactúa con el niño y que se conecta por wifi*. *Respecto a esta conexión*, *no hay ninguna normativa*, *ningún estándar ni ningún control"*.

Respecto a la información que dan las administraciones sobre ciberseguridad, Martínez cree que hay buenas campañas y organismos cómo INCIBE que lo hacen de forma excelente, pero el ámbito de difusión es dónde acaban fallando, el mensaje no llega a todos los usuarios. Para finalizar añade que Mossos d'Esquadra empiezan a interactuar y ofrecer

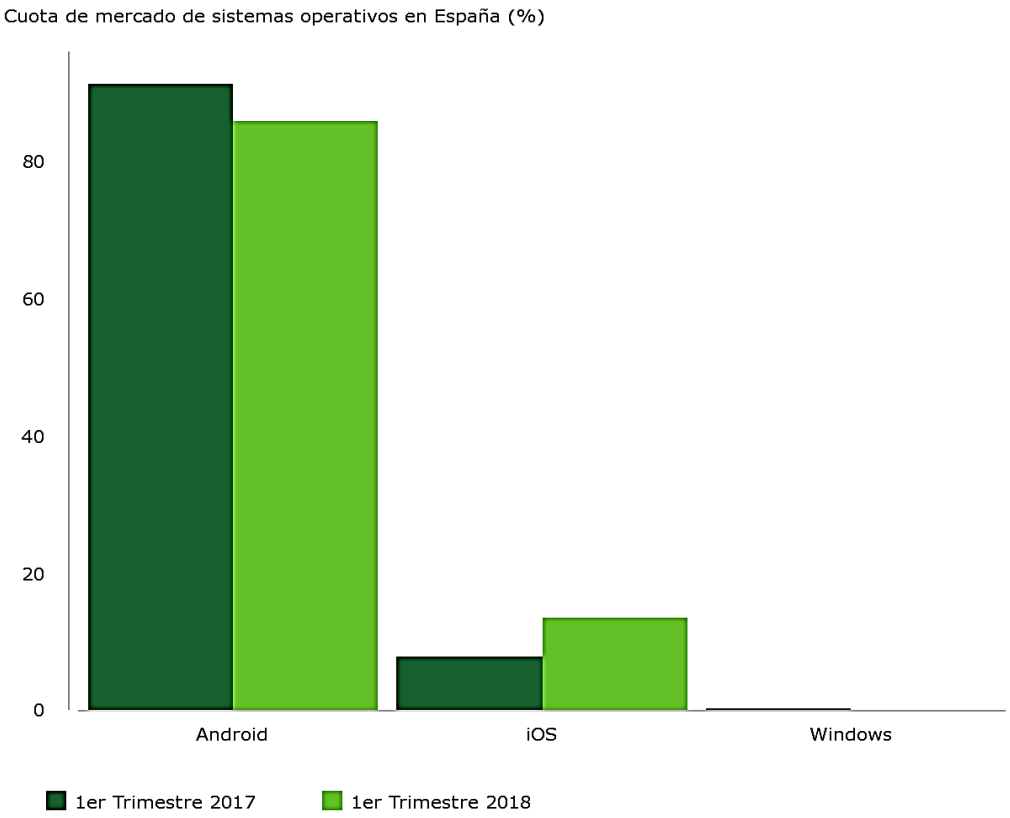
programas para concienciar a los menores de los riesgos cibernéticos. Aun así cree que es un mensaje muy diseñado a quién hay detrás en la red y que habría que tecnificarlo, es decir, no solo centrarnos en el ciberacoso, sextorsión y demás, sino que debemos empezar a hablar de malware.

# 4. Experimento de phishing

## 4.1 Elaboración y desarrollo del experimento

Para poner a prueba los conocimientos de ciberseguridad de forma práctica se decidió elaborar un phishing, es decir, una suplantación de identidad de una página web para poder robar las credenciales de acceso de los usuarios.

Basándonos en datos anteriormente mencionados en el análisis de la generación digital en el ámbito de Barcelona, éste nos indicaba que el 89,76% de los usuarios usaban habitualmente una cuenta de correo de Gmail. Creemos que se debe principalmente por el predominio del sistema operativo móvil de Google, Android, en España. Según Kantar Media, en el primer trimestre de 2018, el Sistema Operativo Android tiene una cuota de mercado del 86,1% en España. Tener un terminal con dicho S.O. implica el uso de una cuenta de Google, y dicha cuenta está asociada a multitud de servicios de la compañía, a destacar Gmail, el servicio de correo de la compañía.




Con un predominio de mercado tan claro, se decidió realizar el phishing basándonos en una suplantación de la página de acceso de Google. Es usual que algunos servicios o aplicaciones web hagan que no sea necesario registrarnos, sino que podemos acceder a través de cuentas de Google o Facebook. Así pues, nos basamos en esta situación para realizar la suplantación de la página.

Lo primero que se necesitó fue un dominio dónde hospedar la página de phishing, para realizar el experimento de una forma más verosímil a la realidad se registró con una identidad inexistente y sin realizar ningún pago. Se aprovechó la llegada de unos servicios de hosting a España que ofrecía sus servicios de forma gratuita durante un año. En el registro se utilizó una dirección de correo electrónico creada para la ocasión y no vinculada con el investigador. Se generó un número de DNI, así como un nombre para registrarnos en ese dominio. Curiosamente no fue necesario ningún documento de identidad, como

sí hacen otros servicios de hosting. El dominio que se registró fue: www.investigacionub.es.

Lo siguiente fue crear un gancho para que la gente accediera a poner sus credenciales. Los phishing más habituales suelen utilizar medidas que requieren o incitan a la urgencia.

A continuación, se muestran ejemplos de phishing reales recibidos en la cuenta personal del investigador:

Phishing de correos: provenía cómo remitente de “servicio@correos.es”, y el hipervínculo del correo de “acceso@correos.es” en realidad dirigía a “correos.es@sfr.fr”.

Buenos dias,

Tienes un paquete en la oficina de correos.
Tiene un período de **72 horas** para recuperar su paquete de lo contrario, se lo devolverá al remitente.
Confirme el envío a su hogar siguiendo los pasos a continuación:

1. Para recibir su código por **SMS**, envíe **CODE** a **997100**
2. Recibe el código de acceso
3. Envíe el código de acceso a la siguiente dirección de correo electrónico: acceso@correos.es

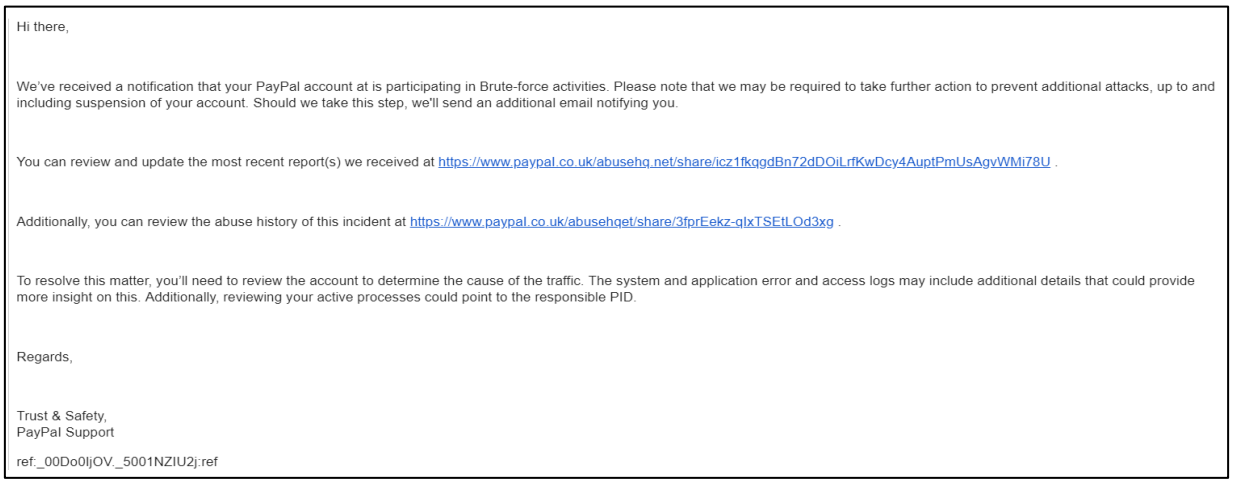
Hasta muy pronto,
©Sociedad Estatal Correos y Telegrafos, S.A.

En este primero, podemos observar que muy posiblemente el español no es el idioma nativo del atacante, podemos deducirlo por estos indicios:

- Utiliza el tratamiento de tu y de usted en distintas frases.
- Utiliza “tiene” cuándo lo correcto sería “dispone”.
- No está correctamente puntuado, en la segunda frase la coma aparece situada al final de “lo contrario”, cuándo debería situarse al final de “su paquete”.
- La expresión “se lo devolverá al remitente” es incorrecta, lo debería ser “se le devolverá al remitente”.

Se trata de un phishing que consigue obtener beneficios a través de mensajes premium. La ventaja de este es que al ser pequeños importes poca gente presentará una reclamación o denúncia.

Phishing de paypal: este otro correo provenía de paul@nuskope.com.au y aparecía cómo “PayPal(UK) Trust & Safety Team”.



Hi there,

We've received a notification that your PayPal account at is participating in Brute-force activities. Please note that we may be required to take further action to prevent additional attacks, up to and including suspension of your account. Should we take this step, we'll send an additional email notifying you.

You can review and update the most recent report(s) we received at https://www.paypal.co.uk/abusehq.net/share/icz1fkqgdBn72dDOiLrfKwDcy4AuptPmUsAgvWMi78U .

Additionally, you can review the abuse history of this incident at https://www.paypal.co.uk/abusehqet/share/3fprEekz-qIxTSEtLOd3xg .

To resolve this matter, you'll need to review the account to determine the cause of the traffic. The system and application error and access logs may include additional details that could provide more insight on this. Additionally, reviewing your active processes could point to the responsible PID.

Regards,

Trust & Safety,
PayPal Support

ref:_00Do0IjOV._5001NZIU2j:ref

Los dos enlaces conducían a http://orders.southeasternfood.com/emptyordersuk/index.html. En dicho enlace se nos conducía a un phishing para robar las credenciales de Paypal.

Phishing de Endesa: éste simulaba tratarse de la compañía Endesa, provenía de este remitente “6573811@movil.endesaclientes.com”.

¡Bienvenido a Mi Endesa!

Estimado cliente, skunkred@hotmail.com

**Notamos que pagaste la factura al mismo tiempo dos veces.**

**Importe : 37 Euro**

**Referencia : ENDESA-1912005W**

Para confirmar su reembolso

Haga clic en el siguiente enlace : Haga clic aquí

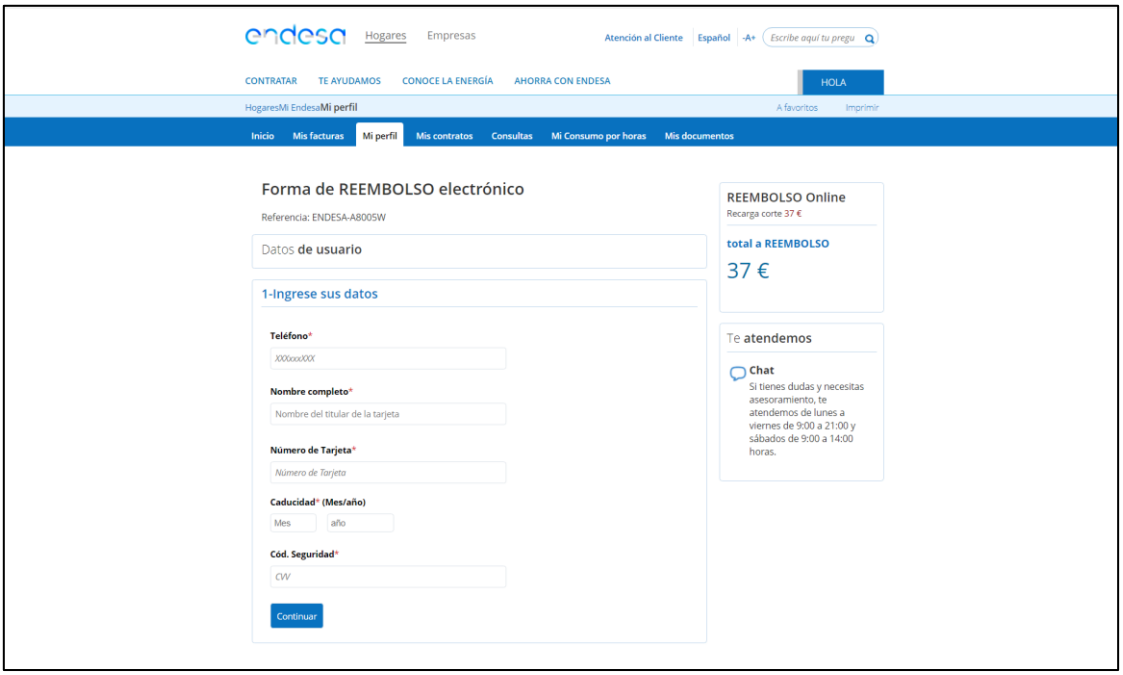
Recuerda que desde **Mi Endesa**, puedes realizar todas tus gestiones online cómodamente.

Este correo electrónico enviado a

Gracias por confiar en nosotros.
Equipo de Atención al Cliente.

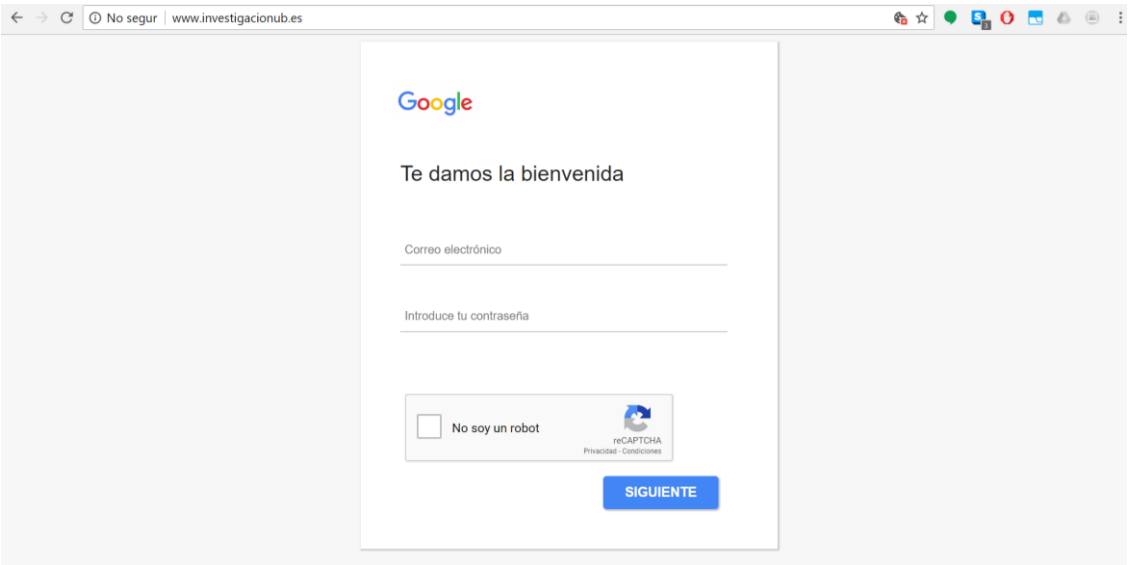
www.endesaclientes.com

Si hacíamos clic en el enlace nos llevaba al siguiente enlace: http://b.scheeg.com/nombreremitente@dominio.com dónde veíamos el siguiente formulario para capturar datos bancarios.




En este trabajo de investigación no se ha optado por esta vía, puesto que es más agresiva y suelen implicar datos bancarios. En su lugar, se ha elegido la

realización de una encuesta de investigación y la realización de un sorteo entre los participantes de la misma. Al finalizar la encuesta el usuario era redirigido al dominio www.investigacionub.es dónde aparecía lo siguiente:




Como podemos observar, pretende engañar al usuario para que introduzca sus credenciales, aunque para mucha gente puede parecer un phishing evidente por varios factores:

- La dirección URL, no es la propia de Google.
- El propio navegador ya lo marca como no segura.
- Actualmente Google pide el usuario y la contraseña en dos pasos.
- No usa la opción de recaptcha en los de accesos de credenciales.

En el anexo 1 se puede consultar el código del índice y el del formulario del sitio web.

A tener en cuenta que debemos introducir el correo electrónico de forma correcta, no funcionaría con sólo el nombre de usuario como sí ocurre en Google. Es necesario que se introduzca de esta forma:

- Nombre_de_usuario@dominio.es

La razón de hacerlo de esta manera ha sido para evitar ataques automatizados de inyección SQL a través de la casilla del correo electrónico.

En cuanto a la casilla de la contraseña, en un primer momento se barajó la posibilidad de capturarlas, tal y como se haría en la realidad, aunque no se quiso asumir el riesgo para no comprometer las credenciales en caso de que cayeran a manos de un atacante, ni como para cometer una ilegalidad. Por ello que se decidió evaluar la contraseña sin capturarla, usando un sistema que tan sólo anota en la base de datos si la contraseña se compone de letras, letras y números o si lleva algún símbolo.

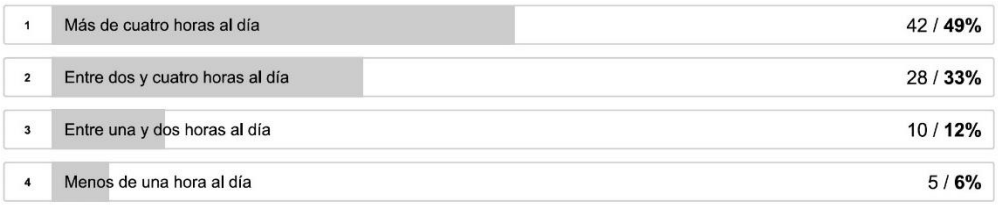
La encuesta tiene cuestiones demográficas, referentes al uso de internet, así como de autoevaluación y percepción de seguridad en la red. Se trata de una encuesta muy breve, de diez preguntas y con un tiempo de realización medio de un minuto y cincuenta segundos.

De todas las visitas que ha recibido la encuesta se han finalizado un 54.8% de las entradas.

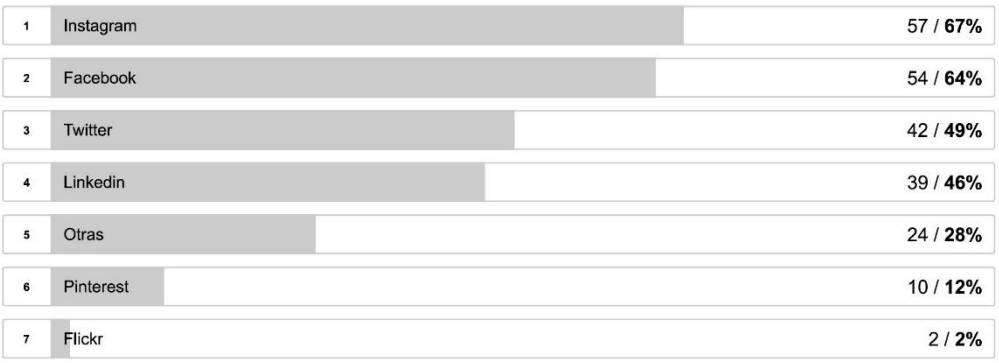
La encuesta ha sido realizada en la plataforma Typeform, puesto que permitía redireccionar a los usuarios al finalizar la misma y por cuestiones prácticas, ya que tiene una interface amigable y que se adapta automáticamente al navegador del equipo o dispositivo. Se adjuntan las preguntas de las encuestas, así como los resultados obtenidos.

Preguntas y respuestas del cuestionario:

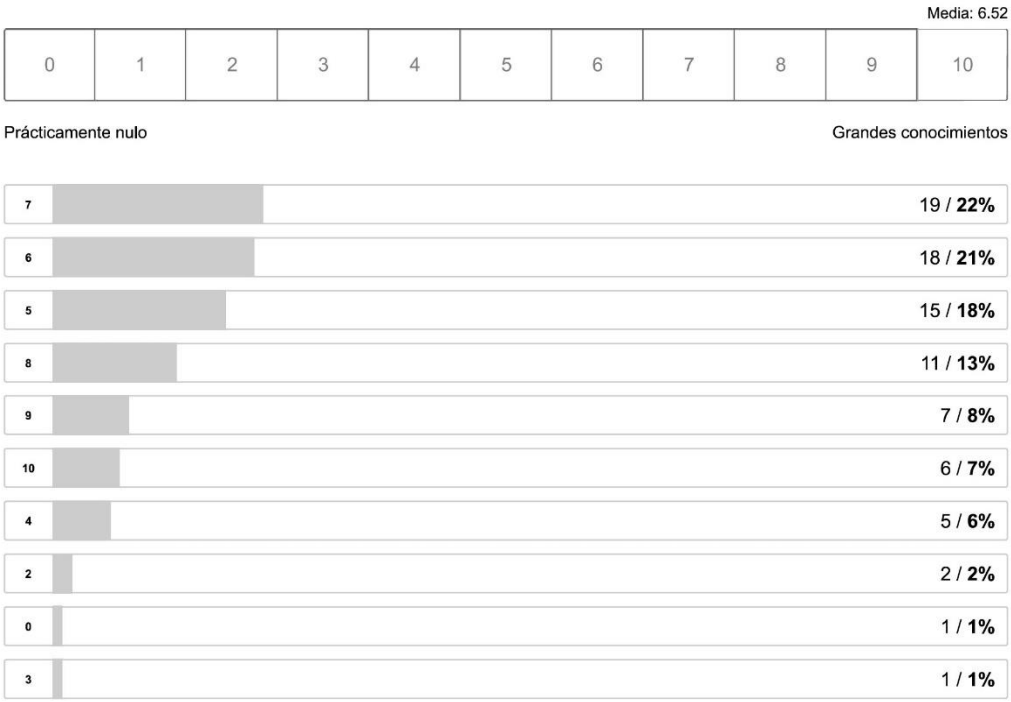
1. ¿Cuánto rato dedicas al día a conectarte a internet?



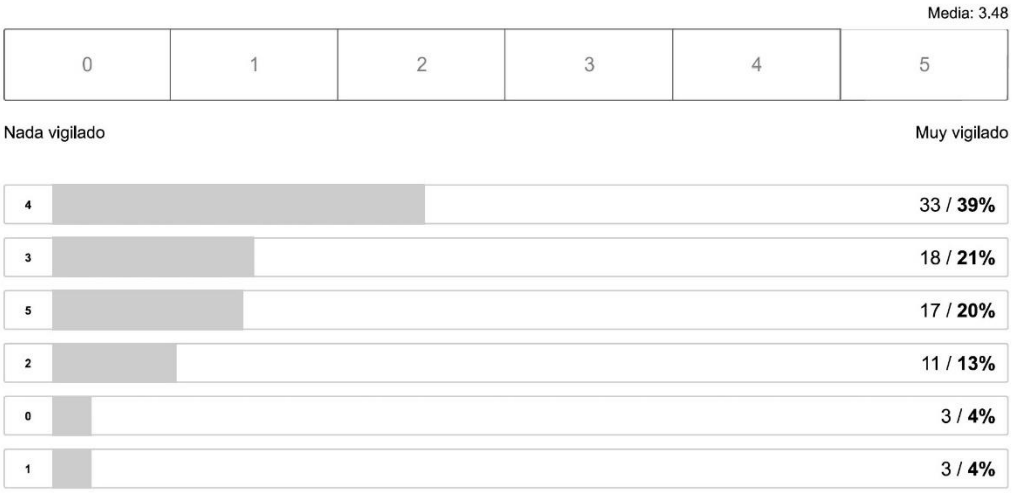

2. ¿Qué redes sociales utilizas? (Posibilidad de contestar múltiples respuestas)



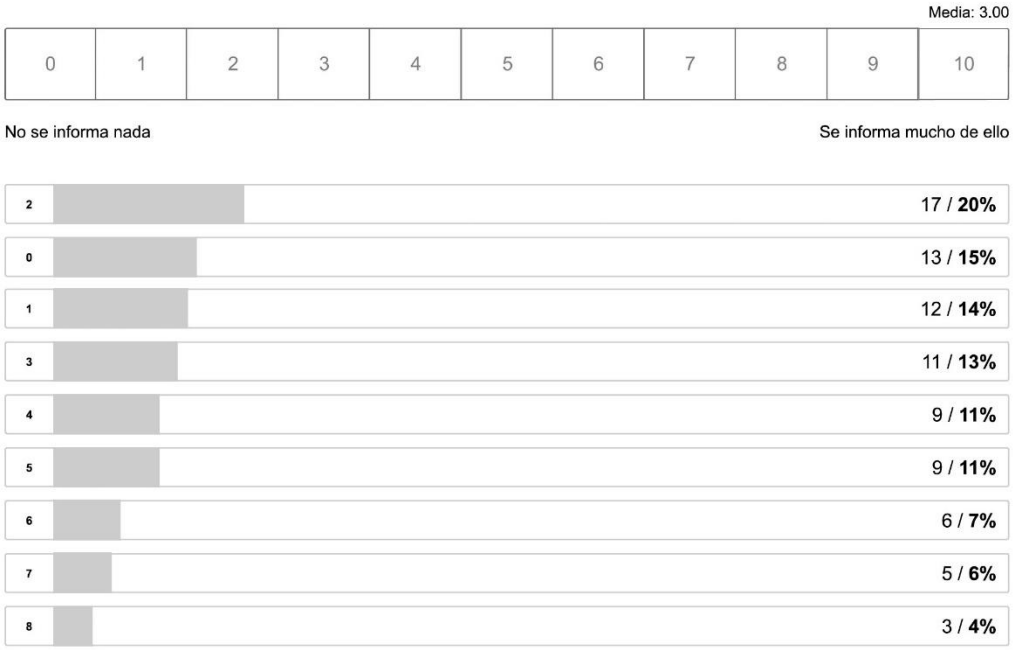

3. Indica tu grado de conocimientos informáticos.



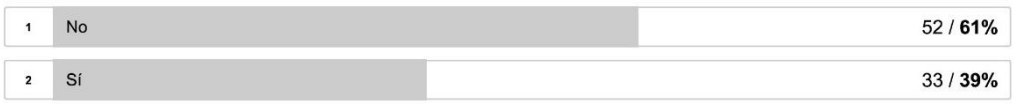

4. ¿Te sientes vigilado en internet?



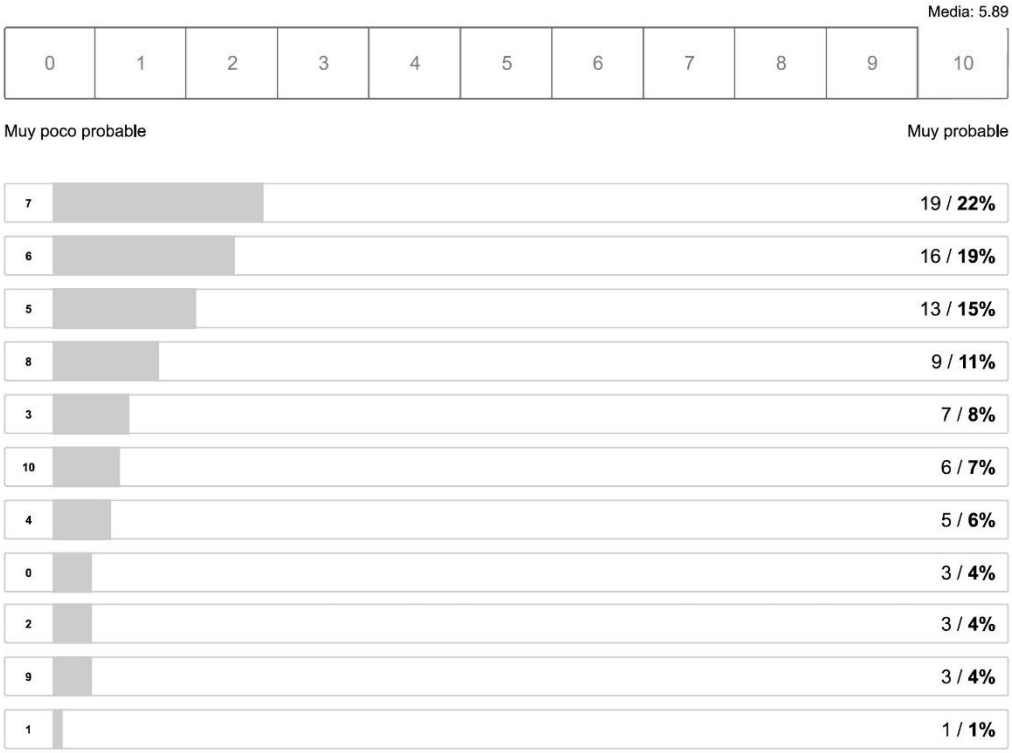

5. ¿Crees que se informa suficiente de los riesgos de internet y del uso de tecnologías de la información?



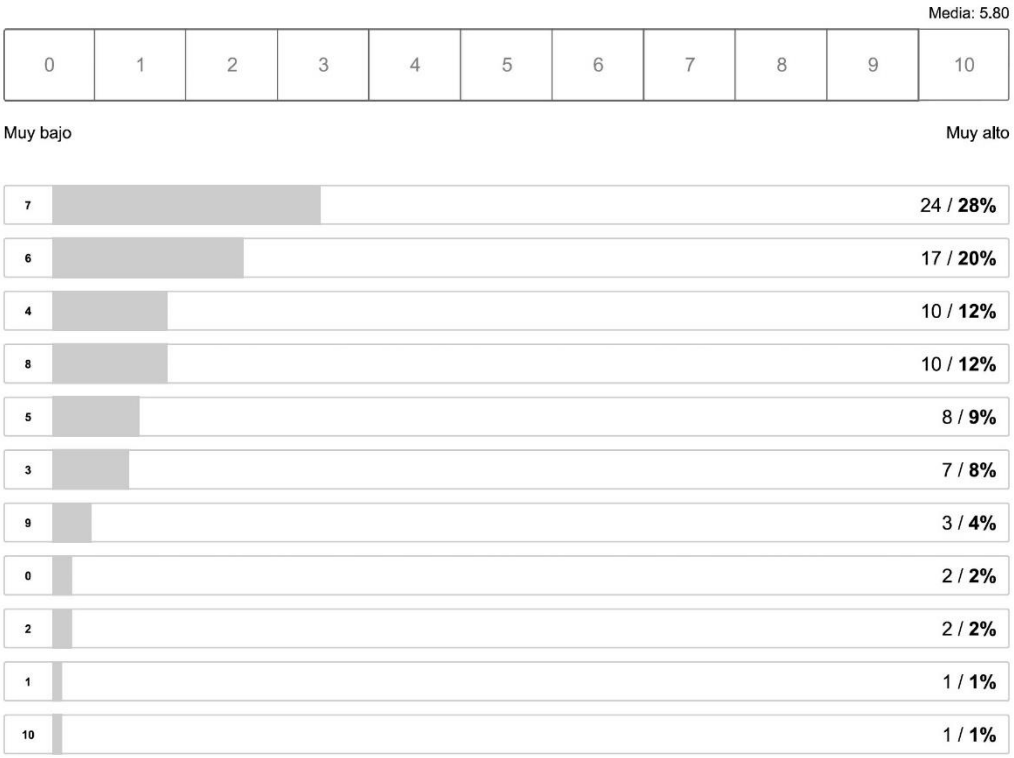

6. ¿Has sido víctima de algún ataque informático?




7. Indícanos en qué grado consideras que eres susceptible a sufrir un ciberataque.




8. ¿Qué grado de confianza te da el comercio electrónico?



9. Indica tu provincia de residencia.


10. Indica tu año de nacimiento.

La media de edad de los participantes se sitúa en 32,72 años.

Y el año más respondido, la moda, ha sido el 1996 (22 años) con 12 veces.

Para hacer difusión del experimento se ha realizado un cartel con un código QR para facilitar el acceso desde dispositivo móvil. El cartel puede consultarse en el anexo 2. Se decidió colocado un total de 50 carteles entre distintas localizaciones:

- Institut de Seguretat Pública de Catalunya.
- Facultat de Dret de Universitat de Barcelona.
- Facultat de Farmàcia i Ciències de l'Alimentació de Universitat de Barcelona.
- Facultat de Biologia de Universitat de Barcelona.
- Bibliotecas públicas de Barcelona:
    - Ignasi Iglesias-Can Fabra.
    - El Clot – Josep Benet.
    - Jaume Fuster.



Cartel colocado en el parquin de bicicletas de la Facultad de Farmacia (izquierda) y cartel colocado enfrente la entrada de la Facultad de Derecho de Avinguda Diagonal (derecha).

Aunque cómo se puede ver en la fotografía derecha el cartel queda deformado por la farola, siempre se han realizado comprobaciones acerca de si los códigos QR resultaban leíbles.

## 4.2 Resultados

Realmente, y tras trabajar con los datos de la AIMC, éstos difícilmente nos revelan algún otro dato destacable más, ya que disponemos de una muestra mucho menor. Es por eso que las cuestiones sobre el perfil demográfico y la percepción de seguridad en la red de los participantes en el experimente serán analizados, pero no tan valoradas como las del AIMC.

Para hacer un seguimiento de los accesos, tanto de la encuesta de Typeform como de la página de phishing, se ha optado por usar enlaces acortados, de esta manera hemos tenido información de cuántos accesos ha recibido cada una de

las páginas, aunque también se ha hecho para facilitar a los sujetos el acceso tanto a la encuesta cómo al phishing. Los enlaces acortados son los siguientes:

- http://bit.ly/encuestaUB
    - Este enlace redirigía a la encuesta de Typeform: https://investigacionub.typeform.com/to/pax7IJ
- http://bit.ly/googleUB
    - Este enlace redirigía a la página dónde se encontraba el phishing: http://www.investigacionub.es/

En total ha habido 164 clics (155 visitas únicas) a los enlaces acortados de la encuesta, 78 a los de la página del phishing. La encuesta ha sido completada por un 54,8% de los participantes y el tiempo medio de respuesta ha sido de 1 minuto 52 segundos. La encuesta fue completada desde entorno de escritorio por 14 personas (16,47%) y 71 desde dispositivo móvil (83,53%).

Durante el trascurso del experimento, la web de phishing sufrió un ataque de inyección SQL. En total este ataque supuso 2631 entradas en la base de datos que han requerido ser limpiadas a la hora de presentar los datos. Dicho ataque intentaba hacerse con el acceso a la base de datos por si podía obtener los datos almacenados del phishing, pero nuestro código no contenía defectos que lo hicieran vulnerable ante esos ataques. Aun así, para evitar que se continuara con el ataque, se añadió un sistema de captcha para evitar ataques automatizados (como era el caso), optando por la solución de Google Recaptcha v.2.

A destacar que el experimento ha sido notificado a Fuerzas y Cuerpos de Seguridad para poder evitar malentendidos, así como implicaciones legales. Concretamente, se ha comunicado a Mossos d'Esquadra en su departamento de Ciberseguridad y en la UCDI (Unitat Central de Delictes Informàtics) y a Guardia Civil en su departamento de GDT (Grupo de Delitos Telemáticos). De

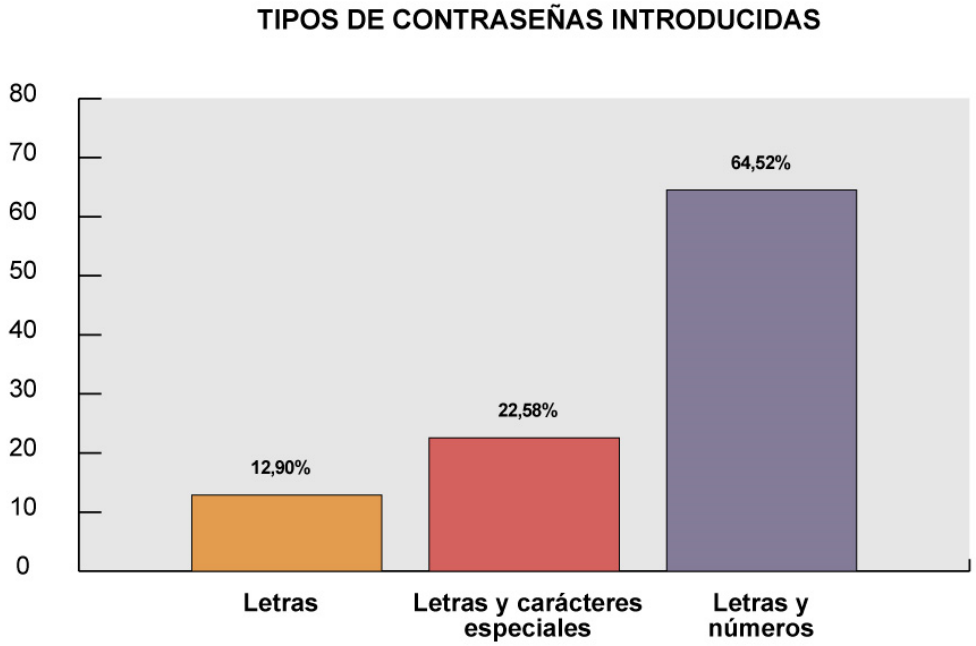
Guardia Civil no se ha recibido respuesta, mientras que Mossos ha verificado incluso el código empleado.

A pesar de tratarse de un phishing realizado sin herramientas específicas y con un diseño no adaptado a distintos dispositivos, de 85 participantes que han finalizado en la encuesta, 78 han acabado llegando hasta el phishing (la web que suplantaba el acceso de Google) y de estos 31 han introducido su correo electrónico y contraseña. Es decir, un 39,74% de los que llegaron hasta el phishing han introducido sus credenciales, una cifra mucho más elevada de lo esperado.

No tenemos forma de determinar si la contraseña introducida es verdadera o no, pero se adjuntan los tipos de contraseñas utilizadas.

Las contraseñas se contabilizaban según si sólo tenían letras, contenían letras y números o letras y letras algún carácter especial. A continuación, se especifican los tipos y número de contraseñas analizadas.

- Sólo letras – 4 (12,90%)
- Letras y números – 20 (64,52%)
- Letras y algún carácter especial – 7 (22,58%)




Por motivos de privacidad obvios, no se incluirá la base de datos capturada. Una vez sea presentado este trabajo de final de grado, se realizará el sorteo durante la presentación y, además, se notificará a todos los participantes que han sido víctimas de un phishing indicando las precauciones que deben tomar. Se les enviará el siguiente texto:

*La investigación sobre ciberseguridad que se ha realizado cómo TFG para la UB ha concluido*,

*Muchas gracias por haber participado en este experimento. Debes saber que tras la encuesta que realizaste, fuiste dirigido a una página web que suplantaba ser un acceso de Google. Se trataba de un phishing para ver si los usuarios sabían detectar esta clase de ataques. Este proyecto ha sido notificado al departamento de ciberseguridad de Mossos de Esquadra, así como al Grupo de Delitos Informáticos de la Guardia Civil*.

*Queremos destacar que en ningún momento se ha guardado tu contraseña, tan sólo tu correo electrónico para poder contactar contigo en caso de ser ganador y para notificarte los riesgos de introducir tus credenciales de acceso*.

*No podemos saber si la contraseña que introdujiste era la real o no*, *en todo caso*, *cuando te pidan las credenciales de acceso:*

- *Verifica que la dirección de la web concuerde con quién te lo pida*.
- *Plantearnos ¿Para qué quieren nuestros datos*, *es necesario darle acceso a nuestra cuenta?*
- *Piensa que nunca tu proveedor de servicios te pedirá la contraseña con la que accedes*.
- *Y*, *además*, *si no lo tienes activado*, *usa un doble factor de verificación para acceder a tu cuenta*.

*De nuevo muchas gracias por tu participación*.

# 5. Conclusiones

En el momento de elegir la temática de este Trabajo de Final de Grado nos encontramos con la duda de si trabajar con un tema que tuviera una amplia bibliografía, o empezar a indagar en un tema no investigado. Finalmente se decidió por la segunda opción, a pesar de que la limitación de tiempo y recursos podía influir en los resultados. La realidad ha sido que, a pesar de no poder hacer un estudio muy amplio, en el sentido de poder distribuir el experimento de una forma más masiva, estamos satisfechos con los resultados.

Si nos fijamos en el estudio más parecido, trabajada en el ámbito físico, nos topamos con el estudio de Matthew Tischer, muy parecido al kit de concienciación que ofrece Incibe. En este trabajo se ha querido llegar más allá y desarrollarlo en un ámbito digital en el que trabajarían los ciberdelincuentes, aunque para su difusión ha sido necesario trabajar a nivel de calle.

Tal y como hemos podido analizar en la encuesta de AIMC, nos encontramos que los nativos digitales tienen una alta dependencia de internet y de sus servicios, cómo pueden ser el correo electrónico o los servicios de mensajería instantánea. Este perfil se encuentra preocupado por su situación de privacidad y seguridad en la red, pero, aun así, no realiza acciones para corregirlo ya que no sabe qué debe hacer. Como hemos podido ver en el experimento realizado, a pesar de ser técnicamente sencillo de realizar, podríamos haber capturado las credenciales del 39,74% de los participantes. Al final, cómo explicó el Sargent Roger Martínez en su entrevista, *"todo se trata de escalabilidad"*, una vez se ha creado este phishing, sólo es cuestión de hacer difusión del mismo para obtener más resultados. La clave la tenemos en los phishing que recibimos y que hemos puesto de ejemplos, siguen difundiéndose porque funcionan y dan los resultados esperados a los delincuentes.

Es evidente que nuestra administración, al ser un reflejo de la sociedad, no está preparada para asumir estos ataques, tanto por sus integrantes, cómo por la

capacidad de la misma. Como hemos visto, es posible el problema resida en que en nuestros dispositivos y nuestro entorno no percibimos o palpamos la inseguridad.

A efectos de este trabajo de investigación, nos alegra poder verificar las hipótesis establecidas al inicio. Realmente las tres metodologías utilizadas nos han conducido en una misma dirección. Lo más relevante ha sido el experimento de phishing, que nos ha permitido probar de una forma tangible las carencias de conocimientos de ciberseguridad en los nativos digitales. En contraposición, que los conocimientos de dicha generación tengan este déficit es un motivo evidente de preocupación y un toque de alerta, y no sólo para los propios usuarios, sino también para la administración y cualquier organización. Las organizaciones deben empezar a ser autoconscientes de los riesgos que empleados con déficits formativos pueden suponer para ellas. Como dijo Álvarez-Pallete (2015) "los datos se han convertido en el petróleo del siglo XXI". Esta frase cobrará mayor sentido cuándo empecemos a saber procesar toda la información que se está recolectando con el Big data y si además no tenemos control sobre los mismos, tenemos el riesgo de perecer. Según la compañía Kaspersky Lab, el 60% de las pequeñas y medianas empresas que sufren un ciberataque, desaparecen en los 6 meses siguientes. Estas compañías son el 43% de los blancos de ataques y las más vulnerables, pues no suelen invertir en protección digital ni en formación.

Después de comentar todas estas conclusiones, es probable que todo el entorno de malware y phishing que nos encontramos en los entornos de escritorio empiece a migrar al entorno móvil. A pesar de ello el móvil sigue siendo el dispositivo preferido para conectarse, aunque el ordenador se niega a morir. Si bien es cierto que el ritmo de ventas desciende, entre los nativos digitales de nuestra muestra siguen usándolo un 85,33% de ellos.

La solución al déficit de conocimiento parece evidente: formación. El Sargent Roger Martínez nos ha indicado cómo debe ser, tecnificándola. La formación no debe ser únicamente conocer qué males pueden ocurrirnos, si no cómo, en la

realidad, debemos poder distinguir qué entornos son potencialmente peligrosos y cuáles seguros. El usuario medio debería ser capaz de identificarlos y, tal y como hemos demostrado en el experimento, esto no es así. Nos parece muy peligroso que casi 4 de cada 10 usuarios pueda sucumbir ante un ataque técnicamente simple, ya no sólo de cara al usuario doméstico, también por las grandes organizaciones en las que se encuentran integradas dichas personas. Hay que tener en cuenta que, como dice Roger Martínez, la gran mayoría de ataques empiezan con ingeniería social. Y como hemos mencionado en la cita inicial de este trabajo de Kevin Mitnick: el eslabón más débil de la cadena de seguridad cibernética somos las personas.

# 6. Bibliografía


ABC. (2017). Obtenido de http://www.abc.es/tecnologia/redes/abci-empresa-sufre-ciberataque-desaparece-seis-meses-despues-201710030142_noticia.html

IDC. (2018). *https://www.idc.com*. Obtenido de https://www.idc.com/getdoc.jsp?containerId=prUS43596418

IESE. (2015). Obtenido de https://www.iese.edu/es/conoce-iese/prensa-noticias/noticias/2015/julio/alvarez-pallete-datos-son-petroleo-siglo-xxi

Incibe. (2018). *https://www.incibe.es*. Obtenido de https://www.incibe.es/protege-tu-empresa/kit-concienciacion

INE. (5 de Octubre de 2010). *http://www.ine.es*. Obtenido de http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608

ITU. (2010). *International Telecommunication Union*. Obtenido de WEBSITE de ITU: https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Kantar. (10 de Mayo de 2018). *https://es.kantar.com*. Obtenido de Cuota de mercado de smartphones en España primer trimestre 2018: https://es.kantar.com/tech/m%C3%B3vil/2018/mayo-2018-cuota-de-mercado-de-smartphones-en-espa%C3%B1a-primer-trimestre-2018/

Rubio Gil, Á. (2010). Generación digital: patrones de consumo de Internet, cultura juvenil y cambio social. *Revista de Estudios de Juventud*, 201-221.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Michael, B. (2016). Users Really Do Plug in USB Drives They Find. *Security and Privacy*, *IEEE* , 14.

# 7. Anexos

1. Código fuente índex 1

```
<!DOCTYPE html>

<html>

<head>
<?php
  foreach ($_POST as $key => $value) {

    echo '<p><strong>' . $key.':</strong> '.$value.'</p>';
  }
?>
<style>

body {
background-color: #f7f7f7;
}


input[type=email], select {
    width: 100%;
    padding: 5px 5px;
    margin: 20px 5px;
    display: inline-block;
    border-bottom: 1px solid #ccc;
    border-top: 0px solid #ccc;
    border-left: 0px solid #ccc;
    border-right: 0px solid #ccc;
    border-radius: 0px;
    box-sizing: border-box;
    height: 35px;
}


input[type=password], select {
    width: 100%;
    padding: 5px 5px;
    margin: 20px 5px;
    display: inline-block;
    border-bottom: 1px solid #ccc;
    border-top: 0px solid #ccc;
    border-left: 0px solid #ccc;
    border-right: 0px solid #ccc;
    border-radius: 0px;
    box-sizing: border-box;
    height: 35px;
}

input[type=submit] {
    width: 130px;
    background-color: #4285f4;
    color: white;
    padding: 10px 20px;
    margin: 10px 10px;
    border: none;
    border-radius: 4px;
    cursor: pointer;
right: 0px;
font-weight: bold;
```

```
font-size: 15px;
        box-shadow: 1px 1px 1px 1px #ccc;
    float: right;
}

input[type=submit]:hover    {
    background-color: #2a56c6;
}

div {
    border-radius: 5px;
    padding: 5px;
}
table {

    font-family: arial, sans-serif;
    border-collapse: collapse;
    width: 430px;
  box-shadow: 1px 1px 1px 1px #ccc;
  margin: auto;
  margin-left: auto;
    margin-right: auto;
  display: block;
  background-color: #ffffff;
    padding: 20px;
}


td, th {
    border: 0px solid #dddddd;
    text-align: left;
    padding: 15px;
}

tr:nth-child(even) {
    background-color: #ffffff;
}



</style>


<script src='https://www.google.com/recaptcha/api.js'></script>
</head>
<body>
<table>

<tr><td><img src="https://cdn.vox-cdn.com/thumbor/Pkmq1nm3skO0-

j693JTMd7RL0Zk=/0x0:2012x1341/1200x800/filters:focal(0x0:2012x1341)/cdn.
vox-

cdn.com/uploads/chorus_image/image/47070706/google2.0.0.jpg" width="100px
">
</td></tr>
  <tr>
  <td>
  <font style="font-size:24px;font-family: Arial; color:#212121; margin-
left:10px;">Te damos la bienvenida</font></td>
  </tr>
  <tr><td><div>

  <form action="index2.php">
    <input type="email" id="fname" name="email" placeholder="Correo
electr&#243;nico" required>
```

```
    <input type="password" id="password" name="password" placeholder="In
troduce tu contrase&#241;a" required>
</td></tr><tr><td>
<div style="float:left;" class="g-recaptcha" data-
sitekey="6LdgpFkUAAAAAHmefxTJmBWLuljdWhMHPGKeYQ1r"></div><br>
<input type="submit" value="SIGUIENTE">
</form>
</div></td>
  </tr>
</table>
</body>
</html>
```

2. Código fuente índice 2

```php
<?php

  $email = $_REQUEST['email'];
  $pwd = $_REQUEST['password'];

  $pwd_content = passtest ($pwd);

  $servername = "localhost";
  $username = "ELIMINADO";
  $password = "ELIMINADO";
  $dbname = "ELIMINADO";

  $conn = new mysqli($servername, $username, $password, $dbname);
  if ($conn->connect_error) {
      die("Error: " . $conn->connect_error);
  }

  $sql = "INSERT INTO dades (id, usuari, password)
  VALUES (NULL, '$email', '$pwd_content')";

  if ($conn->query($sql) === TRUE) {
      echo "Insertad";
  } else {
      echo "Error: " . $sql . "<br>" . $conn->error;
  }

  $conn->close();

  header('Location: http://www.gmail.com');

  function passtest($pwd) {
    if (empty($pwd)) {
      $retorn = "Empty";
    }
    if (ctype_alpha($pwd)) {
      $retorn = "Charts"; //asdfghjkl
    }else if(ctype_digit($pwd)){
      $retorn = "Digits"; // 12345678
    }else if(ctype_alnum($pwd)){
      $retorn = "Alphanumeric";// asdf1234
    }else{
      $retorn = "Special";// $%&/()asd12124
    }

    return  $retorn;

  }


?>
```

3. Cartel publicidad encuesta