DESCUBRE CÓMO PROTEGER A TUS HIJOS EN INTERNET

MÉTODO CANGURO DIGITAL

IVÁN GONZÁLEZ MORENO

DESCUBRE CÓMO PROTEGER A TUS HIJOS EN INTERNET

Método Canguro Digital

Iván González Moreno

DESCUBRE CÓMO PROTEGER A TUS HIJOS EN INTERNET

1º Edición: 2022

Este libro no puede ser considerado como consejo legal o asesoramiento profesional. El contenido de cada capítulo es la sola expresión y opinión de su autor. No hay ninguna garantía expresa o implícita incluida en los contenidos de este libro, por lo que el autor no será responsable de los daños o perjuicios físicos, psicológicos, emocionales, financieros, físicos o comerciales.

Los consejos o estrategias contenidos en el libro pueden no ser adecuados para todas las situaciones, consulte siempre su caso particular con un profesional de la materia.

Las Webs y enlacen que se citan a lo largo del libro, pueden haber desaparecido o cambiado desde el momento que se escribió este libro. El autor no se hace responsable del contenido o información que puedan contener, ni de las recomendaciones que estos sitios Webs puedan realizar.

Dios existe porque yo conozco un ángel.

Te quiero Raquel.

UNA INVITACIÓN ESPECIAL

Si estas interesado en proteger a tus hijos en internet y compartir experiencias con otros padres, ¡entonces puede que esto resuene contigo!

Este libro viene acompañado por una comunidad exclusiva, donde podrás intercambiar opiniones y realizar preguntas a referentes en la protección de menores en internet, preocupados también por hacer de internet un sitio más seguro. El autor del libro se encuentra dentro de la comunidad.

Dale clic o escanea el código QR para unirte. ¡Nos vemos ahí!

https://www.facebook.com/groups/395580149103001/?ref=share

Recuerda: *"A veces sentimos que somos una gota en el mar, pero el mar sería menos sin esa gota".* Santa Teresa de Calcuta.

ÍNDICE

UNA INVITACIÓN ESPECIAL

UNA ESTRELLA DE MAR: ¿POR QUÉ ESCRIBO ESTE LIBRO?

1.- ¿QUÉ SABE INTERNET DE TI Y DE TU HIJO?

1.1.- BUSQUEMOS EN EL PASADO DE INTERNET: LA PUERTA DEL TIEMPO

1.2.- BUSQUEMOS EN EL PRESENTE: BÚSQUEDAS PROFUNDAS

1.3.- AUTOMATIZAMOS EL FUTURO: SABER SI ALGUIEN EN TIEMPO REAL MENCIONA A TUS HIJOS

2.- LOS SECRETOS DE LAS FOTOGRAFÍAS EN INTERNET

2.1.- ¿CÓMO SABER DÓNDE ESTÁN LAS FOTOGRAFÍAS TUYAS Y DE TUS HIJOS?

2.2.- LAS FOTOGRAFÍAS REVELAN DÓNDE VIVES: LA FICHA DEL LIBRO

2.3.- RIESGOS DE COMPARTIR FOTOGRAFÍAS SIN PERMISO

3.- DERECHO AL OLVIDO: CÓMO ELIMINAR DATOS DE INTERNET

3.1.- DE LA PROPIA WEB DONDE LO ENCONTRAMOS

3.2.- UTILIZANDO GOOGLE

3.3.- DESDE EL ORGANISMO DE PROTECCIÓN DE DATOS

3.4.- CANAL PRIORITARIO DE RETIRADA DE CONTENIDOS DE LAS REDES SOCIALES

4.- ¿SABES SI ALGUNA VEZ TE HAN HACKEADO?

4.1.- WEB CENTRAL DE HACKEOS

4.2.- ¿CUANTO TIEMPO SE TARDA EN HACKEAR TU CONTRASEÑA?

4.3.- CONTRASEÑAS SEGURAS Y FÁCILES DE MEMORIZAR

4.4.- MERCADO NEGRO DE LOS DATOS: ¿CUÁNTO VALE UN GMAIL EN EL MERCADO NEGRO?

5.- ¿QUÉ SABE GOOGLE DE TI Y DE TU HIJO?

5.1.- ELIMINANDO AL MONSTRUO DE LAS GALLETAS

5.2.- PARTE PRIVADA DE GOOGLE

5.3.- CÓMO NOMBRAR A UN HEREDERO DE MI VIDA EN INTERNET

5.4.- DESCARGANDO UNA COPIA DE MI VIDA EN INTERNET

6.- POSTUREO Y RIESGOS EN LAS REDES SOCIALES

6.1.- QUE SABE EL MUNDO FACEBOOK DE TI (FACEBOOK, INSTAGRAM Y WHATSAPP)

6.2.- CÓMO NOMBRAR UN HEREDERO DEL MUNDO FACEBOOK

6.3.- DESCARGAR UNA COPIA DE TODO LO QUE EL MUNDO FACEBOOK SABE DE MÍ

6.4.- COMPRA DE SEGUIDORES, COMENTARIOS Y RESEÑAS. MANIPULACIÓN O INFLUENCIA

7.- ¿QUÉ SABE TU MÓVIL DE TI Y DE TU HIJO?

7.1.- EL N.I.F. DE TU MÓVIL
7.2.- TU MÓVIL SABE DÓNDE VIVES Y CUÁNDO VAS AL SUPERMERCADO
7.3.- DETECTIVE DE APLICACIONES FALSAS (QUE HACEN COSAS QUE NO DICEN)
7.4.- CÓMO NOMBRAR UN HEREDERO EN APPLE (CERRANDO EL CÍRCULO)

8.- PROTEGER A TU HIJO EN WHATSAPP Y TELEGRAM
8.1.- CONFIGURAR WHATSAPP PARA QUE SEA SEGURO
8.2.- CONFIGURAR TELEGRAM PARA QUE SEA SEGURO

AHORA TE TOCA A TI

¿TE PUEDO PEDIR UN FAVOR?

CÓDIGOS QR DE LAS WEBS Y APLICACIONES MENCIONADAS EN EL LIBRO

REGALO PARA LOS LECTORES

AGRADECIMIENTOS

UNA ESTRELLA DE MAR: ¿POR QUÉ ESCRIBO ESTE LIBRO?

Hace un tiempo, caminaba por el paseo marítimo de Málaga (España). A lo lejos vi a una persona que se agachaba con esfuerzo y recogía algo de la orilla, tirándolo al mar. No te lo he dicho, pero soy abogado, eso significa que soy curioso (algunos dirían cotilla) por naturaleza. Así que decidí acercarme.

Cuando me aproximaba, pude ver que se trataba de una persona mayor y que efectivamente le costaba un esfuerzo agacharse y arrojar algo al mar. La curiosidad ya me podía. Cuando estaba muy cerca, me di cuenta que lo que arrojaba al mar eran estrellas de mar. Toda la orilla estaba llena de estrellas. Al llegar a su altura, pude confirmar que era una persona muy mayor, como ya había intuido desde lejos por su forma de moverse.

No lo dudé y le pregunté:

—Disculpe caballero, si me permite una pregunta. ¿Qué sentido tiene devolver estas estrellas al mar? Seguramente como esta orilla existirán muchas otras donde también habrá estrellas. Y solo en esta, aunque estuviera todo el día, jamás podrá devolverlas todas al mar. ¿Se da cuenta que lo que hace no tiene ningún sentido?

Al decirle esto, se agachó de nuevo, cogió otra estrella de mar, me miró fijamente unos instantes, pude sentir la mirada de la sabiduría que solo se obtiene con la edad. Después devolvió la estrella al mar, me volvió a mirar y me dijo algo que no olvidaré:

—Para esta estrella tiene todo el sentido.

Este antiguo cuento es una adaptación de un cuento sufí. Recuerdo una frase que nunca olvidaré, se atribuye a Jorge Bucay, que dice algo así: *"Los cuentos sirven para dormir a los niños y despertar a los adultos"*.

Desde hace muchos años, cada vez que comienzo una conferencia lo hago con un cuento. Y no podía ser menos en este, mi primer libro. Cuando vuelvo pasado un tiempo al mismo lugar, casi nadie recuerda el contenido de la conferencia (y mira que son buenas jeje), pero pocos olvidan el cuento que dio paso a la misma.

Este cuento expresa cuál es mi intención con este libro. Mi ilusión es que llegue a muchas personas. Este es un libro donde encontrarás multitud de ejemplos reales de mi vida profesional como abogado en ejercicio (lógicamente he cambiado los nombres y he utilizado nombres de familiares y amigos, espero que les haga ilusión, a mí sí me hizo), mis experiencias, mis aprendizajes y la creación de un método: el **"Método Canguro Digital",** que te va a descubrir el paso a paso para proteger y educar a tus hijos en internet.

Como dijo la madre Santa Teresa de Calcuta: *"A veces sentimos que lo que hacemos es tan solo una gota en el mar, pero el mar sería menos si le faltara esa gota".*

Ese es mi objetivo, para ello voy a realizar mi mejor esfuerzo, pondré toda mi pasión y conocimientos en este libro. Lo prometo.

Puedes pensar que quién soy yo para escribir este libro. Mi historia no es importante, el contenido del libro sí. Pero déjame que me presente y así nos vamos conociendo, aunque cuando termines el libro me conocerás muy bien. Mi nombre es Iván, soy un abogado especializado en la privacidad y la tecnología, vivo en un pueblecito de 5.500 habitantes, llamado Villanueva del Trabuco. Mi pueblo está situado en Málaga (España). Te confieso que soy un pelín friki y empollón. Desde que terminé mi carrera, sabía que quería dedicarme a este mundo de la privacidad y la tecnología (aunque un amigo también tuvo influencia en esa decisión, desde aquí aprovecho para darle las gracias). Hace 13 años creé mi despacho: Privacidad Global. Estoy orgulloso de las personas que me acompañan en esta aventura, hoy más de 15 personas, con una pasión común: ayudar a las personas a un uso seguro de la tecnología.

Mi trabajo y mi pasión, me han llevado a ser colaborador semanal en radio y televisión desde hace años, tener columnas en prensa, impartir cientos de conferencias (alguna de ellas para miles de personas), conocer a gente muy divertida (esto es lo mejor), en fin, cosas que no hubiera imaginado nunca cuando estudiaba. Y que son difícilmente explicables para un abogado de pueblo como yo.

Esto te lo cuento porque no te voy a dar ninguna recomendación que no haya vivido en primera persona. Alguien me dijo una vez: antes de darme consejos enséñame tus cicatrices. A lo largo del libro, las verás todas. Desde hace 13 años estoy en el campo de batalla. Lo que encontrarás en este libro es fruto de mi experiencia. No hay teoría sin aplicación práctica desde el primer capítulo. Podríamos decir que el libro es como un taller práctico, y no has visto a ningún mecánico con las manos limpias: ¿verdad? Pues prepárate para comenzar un viaje apasionante. En la mayoría de los capítulos, encontrarás lo que yo llamo "Jueretos", una mezcla entre juegos y retos para realizar con tus hijos, además de formularios para llevar a la práctica lo que aprendas.

Este libro, también tiene recursos adicionales para desarrollar al cien por cien el mismo, que podréis utilizar tanto tú como tus hijos:

- Cuaderno de "Jueretos" y Hojas de Ruta.
- Sopa de letras sobre el contenido del libro.
- Libro de contraseñas para padres e hijos.
- Y finalmente un cuaderno de apuntes (ya te dije que era un pelín friki).

Mi idea es que este contenido se pueda utilizar en: colegios, ampas, asociaciones y clubes, reuniones de padres, etc...

Soy padre de dos pequeños: Jesús y Sofía, de diez y siete años. Eso desde luego es mucho más importante que ser abogado y os podéis imaginar que con esa edad, ya tenemos que estar pendientes de ellos en el ámbito offline y online. Enseñarles cómo caminar en este

mundo de forma segura. Esta fue una de las mayores motivaciones para crear el "Método Canguro Digital".

Siempre le digo a mis hijos que existen dos palabras que son mentira, siempre son mentira: la primera es "gratis" y la segunda "fácil".

En la vida no hay nada que merezca la pena que sea fácil, y desde luego tampoco será gratis. El mundo de internet no es diferente. Intento que mis hijos lo comprendan. Estoy seguro de que tú también lo harás cuando leas este libro, y lo más importante, podrás transmitirlo a tus hijos.

Hay una frase que define internet, si solo te llevaras la misma de este libro ya sería feliz: "Si algo es gratis en internet el producto eres tú".

Desconozco quién hizo la mejor campaña de publicidad del mundo, que es hacernos creer que internet es gratis. Pero eso es mentira. Simplemente no pagamos con dinero, sino con el petróleo (o el bitcoin) de este siglo que llamamos datos.

Los padres con hijos entre 9 y 14 años sabemos que no nos podemos desconectar. Tenemos y debemos estar cuidando a nuestros hijos también en este ámbito. Es cierto que ellos son nativos digitales y que nosotros somos inmigrantes digitales. Que ellos han nacido con el uso de la tecnología de forma natural, algo que para nosotros supone un esfuerzo. Pero es nuestra responsabilidad.

Voy a ayudarte, a pesar de no tener conocimientos avanzados de la tecnología e internet. Aunque no tengas mucho tiempo, vas a tener un paso a paso que te lleve a proteger a tus hijos de los mayores riesgos que se dan en internet. Podrás enseñarles a manejarse de forma segura por este nuevo mundo que tiene sus propias reglas, su propio lenguaje y sus propias normas. Déjenme que lo exploremos juntos.

La tecnología no es ni buena ni mala en sí misma. Somos las

personas las que debemos darles un buen uso. Me imagino que sabes lo que es la nomofobia, esa adicción a los móviles que tienen muchos de nuestros peques (y también adultos). Ese miedo a perderse algo, a estar constantemente conectado.

En mis charlas suelo comenzar diciendo, que se pongan de pie y que hagan todos el signo de la victoria con los dedos. Además de ser una imagen maravillosa, les digo que se miren entre sí y que me digan si ven algún peligro en lo que están haciendo. La mayoría contesta que no. Pero lo cierto es que este gesto, subido a redes sociales y realizado a menos de un metro y medio, permite extraer la huella dactilar de una persona con casi el 100% de éxito. Si te alejas de un metro y medio a tres, la probabilidad de extraerlas disminuye. A más de tres metros es casi imposible.

Este gesto es muy habitual en determinadas partes del mundo y supone un riesgo innecesario. Después de esto, les hago una pregunta simple: ¿podríais recordar de memoria 5 números móviles?.

Antes de seguir leyendo: ¿tú podrías?

A continuación les digo que los que no puedan recordarlo se sienten. La mayoría se sienta. Siempre les explico que si visitaran la plaza de mi pueblo, y preguntaran a cualquier persona mayor la matrícula de su último coche, seguramente no tendría ningún problema para decírsela, pero no la del último, sino la de la mayoría de coches que ha tenido a lo largo de su vida.

Con estos dos ejercicios ya los tengo predispuestos a escucharme. Espero que a ti te hayan servido para despertar tu curiosidad, y seguir leyendo las siguientes páginas. Comenzamos un viaje apasionante, estoy emocionado por ser tu guía. Recuerda que cualquier duda en el viaje, aquí estoy contigo:hola@metodocangurodigital.com. Relájate y disfruta.

¿Qué sabe internet de ti y de de tu hijo?

1.- ¿QUÉ SABE INTERNET DE TI Y DE TU HIJO?

Me encanta la cara que ponen los asistentes a mis conferencias cuando les pido que cojan un folio en blanco y que apunten en el mismo todo lo que internet sabe de ellos. Algunos me miran con cara de póquer, otros no saben qué poner y la mayoría me dice que mucho. A lo que yo les respondo: exactamente qué es mucho.

Es increíble que nadie nos enseñe a buscar nuestra huella digital en internet, sobre todo porque esta huella digital va a influir en nuestra vida a futuro: cuando busquemos trabajo, en los estudios, amigos, incluso pareja. etc…

Te pongo un ejemplo real que me ocurrió en mi despacho hace tiempo. Salvador había sido albañil toda su vida, durante la última crisis decidió aprovechar y sacarse el carnet para poder conducir camiones. Tras estudiar con esfuerzo, hacía mucho que no estudiaba logró sacarse el carnet. Con toda la ilusión salió a buscar trabajo, pero se dio cuenta de que nadie lo contrataba. Era raro, se estaban buscando camioneros y amigos suyos que se sacaron el carnet después que él ya lo habían encontrado. Tras un nuevo rechazo, decidió que tenía que saber qué ocurría, se armó de valentía y preguntó si le podían decir cuál era el problema. Salvador había llegado a pensar que era cosa de la edad, de su forma de vestir, de expresarse etc…, en fin ya no sabía que pensar. Lo que menos esperaba es que le dijeran que el problema estaba en internet.

Le explicaron que siempre se hacía una comprobación de los aspirantes a un puesto de trabajo en Google, y que en su caso aparecía una multa de tráfico por alcoholemia. Ese era el motivo de no contratarlo. Salvador no podía creerlo. Tras realizar la consulta al llegar a casa, allí estaba la multa. Publicada en un Diario Oficial de la Provincia de Málaga, hacía años. Salvador tardó en recordar el motivo, se trataba de una multa de tráfico a la salida de una boda

en la que bebió un poco más de lo habitual. Ya la pagó en su día. No entendía cómo esa situación que ocurrió hace años, influía en la búsqueda de trabajo que estaba realizando ahora. Esto es la huella digital.

En el siguiente capítulo te contaré cómo le ayudamos a eliminar esto. Pero lo importante ahora, es que te enseñe a buscar tu huella digital y la de tus hijos: en el pasado de internet, en el presente y automatizarlo para el futuro.

Por mi experiencia, casi el 50% de las personas que buscan como yo te voy a enseñar, encuentran cosas que no deberían estar en internet. Manos a la obra, comencemos a buscar tu huella digital y la de tus hijos.

1.1.- BUSQUEMOS EN EL PASADO DE INTERNET: LA PUERTA DEL TIEMPO

¿Se puede viajar al pasado?

Cada vez que hago esta pregunta a los niños, su mirada tiene un tono divertido. La mayoría no dice nada. Algunos dicen que sí, que con la memoria se puede viajar al pasado (lo que es bonito, la verdad). Pero la gran mayoría dice que eso es imposible. Es cuando se me escapa una sonrisa y les digo que están pensado en modo offline, y que hay que pensar en modo online.

Por supuesto que en internet se puede viajar en el tiempo, esto es el pan mío de cada día. De hecho, podemos retroceder a cualquier año (a partir de 1990), mes y casi cualquier día. Para ello tendremos que utilizar una puerta del tiempo. Existen varias en internet pero déjame que te enseñe la más sencilla, y cómo podemos sacarle el máximo provecho.

Me gustaría presentarte el proyecto **WaybackMachine**. Con su web:www.web.archive.org. **(al final del libro encontrarás** códigos QR de todos las webs y enlaces mencionados). Una auténtica puerta al pasado de internet. Este es un proyecto creado para ser un repositorio y una hemeroteca de internet. Su utilización es muy sencilla, tras entrar en la web podemos buscar cualquier página web, aunque ya no exista en la actualidad.

Hagamos un ejemplo con una web con bastante tráfico. Utilizaremos una de las webs más leídas del mundo: el periódico deportivo Marca (www.marca.com).

Una vez introduces la web, te da la opción de retroceder en el tiempo hasta el año 1998. Por ejemplo: vamos a imaginar que queremos ir al año 2007. Dentro de ese año buscaremos el mes de marzo. El día 15 para ser más exactos (me gusta ese día, es mi cumpleaños). Al hacer "clic" nos llevará exactamente a la web tal y

como era ese día. Nos podremos mover con total tranquilidad por la misma. ¡Una pasada!. Por cierto ese día, era noticia que Robinho amenazaba con marcharse del Real Madrid si seguía sin jugar. Y que creía que si se marchaba su entrenador Capello jugaría más. Qué cosas.

Pero sé que estás pensando. Oye Iván, ¿y esto cómo puede ayudarme a proteger a mis hijos? Es una gran pregunta, déjame que te la conteste con un ejemplo real.

Hace un tiempo, en un foro de internet, un compañero de clase de Gerardo, haciéndose pasar por él, se dedicó a publicar comentarios despectivos del resto de compañeros. Parecía que los publicaba Gerardo, os podéis imaginar cómo se sentía. Alguien le dijo al suplantador que se estaba pasando, que esto ya había pasado hacía mucho el límite de una broma de niños. Cuando vio la repercusión que estos comentarios estaban alcanzando, decidió borrarlos. Para cuando Gerardo habló con sus padres y estos decidieron ponerlo en conocimiento del centro donde estudiaban (esto no te va a pasar a ti con lo que te voy a enseñar en este capítulo), los comentarios habían desaparecido. Esto es algo que nuestros hijos tienen que comprender, una vez subido algo a internet se pierde el control de lo que uno sube. Puede ser como en este caso que se borrara del presente, pero nunca se borran del pasado. Por lo que fue tan sencillo como acceder a www.web.archive.org, irnos un par de días atrás y volver a tener los comentarios que se habían realizado.

Para aquellos que tengáis curiosidad, os diré que estos certificados de esta página web son admitidos como prueba por los juzgados españoles, que consideran que se trata de un tercero imparcial, bajo una búsqueda automatizada y no manipulable, siendo además gratuito por lo que no tienen intereses en juego para ninguna de las partes.

En este caso no fue grave, pero desafortunadamente he tenido otros casos en el despacho que sí lo han sido, y esta puerta del tiempo siempre fue muy útil.

JUERETO 1.- LA PUERTA DEL TIEMPO

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Este es el aprendizaje para nuestros hijos: **cualquier cosa que subas a internet escapa a tu control**. Si hace falta leer esto un par de veces, se lee.

Ahora bien, no es lo mismo decirlo que enseñárselo. A lo largo de este libro te propondré diferentes juegos y retos (los he llamado "Juereto", qué friki soy, jeje) para que los pongas en práctica junto a tus hijos. Me encanta la frase que utilizaré siempre como subtítulo de los "Juueretos": Me lo contaron y lo olvidé; lo vi y lo entendí; lo hice y lo aprendí. Creo firmemente en esto.

El juego consiste en que primero busquen el día que Cristiano Ronaldo o Messi debutaron con el Madrid o el Barca. Tú conoces a tus hijos y sabrás cuál de los dos ejemplos encaja mejor. Tras localizar el día, **el reto es que localicen la portada del: Marca, Sport, As y el Mundo Deportivo de ese día**. Si localizan las cuatro **serán 4 puntos**, un punto por portada. Explícale el concepto de puerta del tiempo.

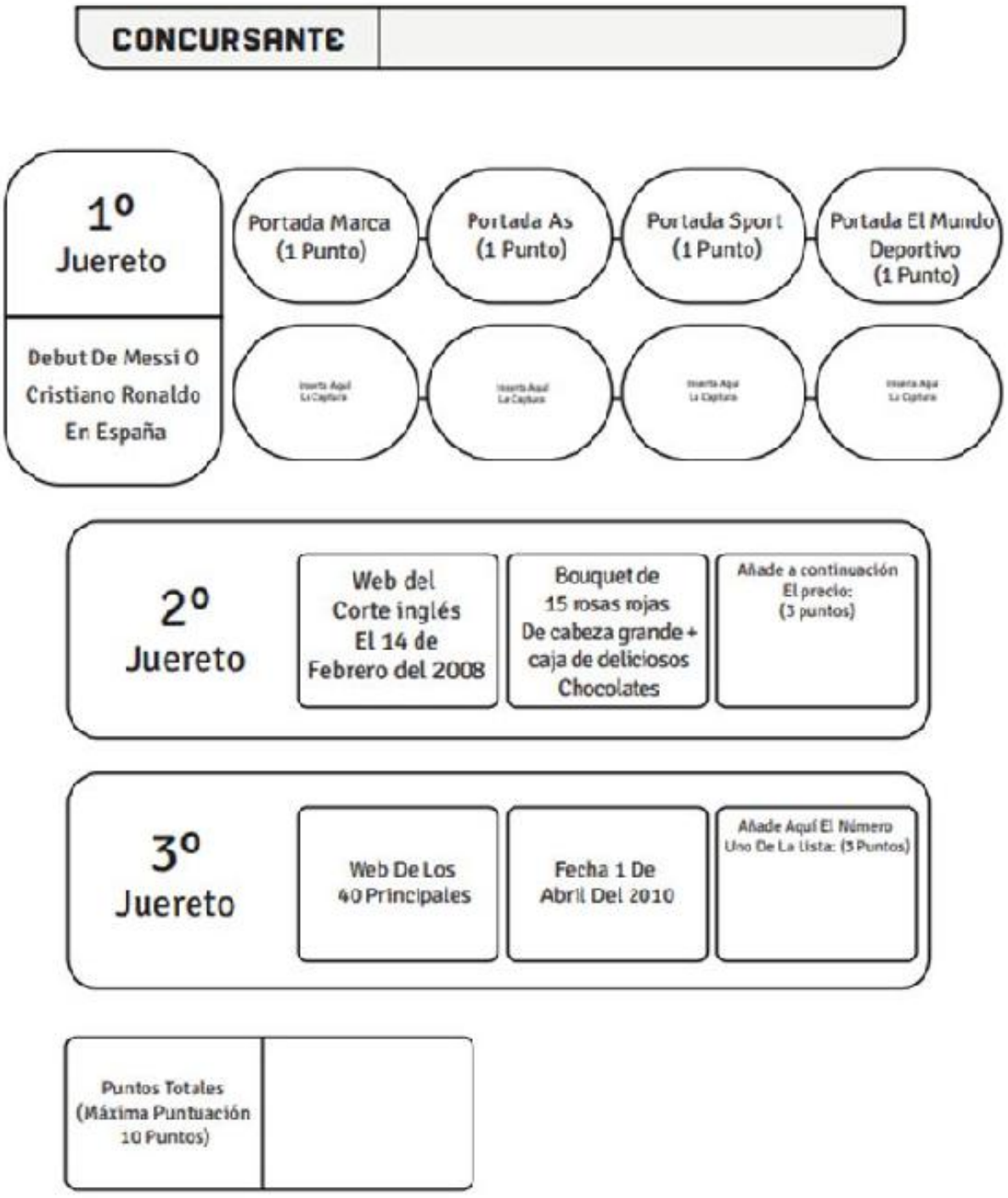
En segundo lugar, buscarán la web del Corte Inglés el 14 de febrero del 2008 y tocará descubrir el precio de un: **"Bouquet de 15 rosas rojas de cabeza grande + caja de deliciosos chocolates"**. Esto vale **por 3 puntos.**

Y por último, por un valor de **3 puntos más**, en la página web de los 40 principales, qué canción ocupaba el número uno, **el día 1 de abril del 2010.**

Quien más puntos obtenga gana, tú decides el tiempo máximo. **¿Te atreves a competir con tus hijos o hacer parejas?** De esta forma vas a poder enseñarles de forma visual y práctica como retroceder en el tiempo. Seguro que no lo olvidarán. Ahora es cuando tú les dejas caer aquello de que: en internet todo permanece

y nada se borra.

Por cierto te voy dejando modelos que te sirvan para los “Jueretos”. Pero como ya te adelantaba, he realizado un cuaderno de “Jueretos” y “Hojas de Ruta” que acompañan a este libro para que podáis utilizarlos e interactuar con el libro. En este libro ya no me cabían más, lo siento. Mi ilusión es que estos cuadernos, junto con la sopa de letras, puedan ayudarte a aprender junto a tus hijos jugando.



Pero ya que estamos aquí, no me resisto a contarte alguna utilidad más que puede tener este servicio. Más allá de las que ya te he contado, os pongo tres ejemplos reales como siempre.

El primero, ocurre más de lo que uno se imagina. Navegando por internet encuentras algo que estabas buscando: viaje a Punta Cana. El precio no parece real, así que llamas por teléfono para asegurarte y realizar la reserva. Más tarde pasarás por la agencia. Ya te imaginas en esas playas paradisíacas, descansando, relajado, tú sabes que te mereces esas vacaciones. Pero tu gozo en un pozo. Cuando estás hablando con la persona responsable de la agencia de viajes, te dicen que ese precio nunca ha sido el que tú dices, que te has confundido. Es posible, porque necesitas unas vacaciones, el año está siendo largo. No, no puede ser. No te van a hacer dudar, estás seguro de que has visto ese precio. Entras de nuevo, ya no tiene el precio que recuerdas. Pero entonces recuerdas este libro y el concepto de puerta del tiempo. Esbozas una sonrisa, entras de nuevo a la web y retrocedes al pasado. Efectivamente, ahí estaba el precio. Ahora sí te vas a Punta Cana.

El segundo es más personal y siempre que lo recuerdo me emociono. En una de mis conferencias (sí, ya sé que me han ocurrido muchas cosas en conferencias, pero es que doy muchas, jeje), recuerdo a una persona sentada en la primera fila. Le cambia el rostro cuando yo explico esta parte. Este tipo de cosas no son extrañas porque me suelo meter en "fregados" a menudo. Aunque siempre sin querer, lo prometo. Así que al terminar la charla me acerqué a aquella persona. Le pregunté si había dicho algo que le hubiera ofendido, de ser así le pedía disculpas por anticipado. Lo que me dijo no se me olvidará jamás. Es una de las cosas que guardaré en mi corazón para siempre.

Me contó que tenía una empresa de aire acondicionado con su hermano. Hacía años que su hermano había fallecido, al decirlo se le quebró la voz (no quise preguntar cómo, pero por la forma de decirlo tuvo que ser algo traumático). Ambos tenían una web y en la portada de la misma, había una fotografía de ambos hermanos abrazados, felices de comenzar esa nueva aventura. La web hacía mucho que no existía. Había intentado recuperar esa fotografía (era muy importante para él), pero fue imposible. Cuando yo le había

explicado cómo hacerlo, lo hizo sobre la marcha en mitad de la conferencia. De repente, allí estaba la foto con su hermano. En ese momento, había pensado cómo era posible que la gente no conociera lo que yo estaba explicando. También estuvimos hablando de lo útil que hubiera sido en casos como este, nombrar un heredero en internet, pero eso te lo cuento en otros capítulos. Me dio las gracias, te juro que en esos momentos todo el sacrificio y trabajo que le dedico a mi profesión merece la pena. Olé mi trabajo. Por cosas como estas escribo este libro.

En tercer lugar, (aunque así podría estar todo el libro), tengo unos amigos que son diseñadores de webs. Esta puerta del tiempo les viene genial. Cuando los contratan para hacer una web, pueden ver qué han hecho a lo largo de su historia las páginas webs de su competencia y qué errores han cometido para aprender de los mismos. Les encanta ver la cara de sus clientes cuando le explican por qué al final han puesto el formulario de contacto arriba a la derecha y no en la parte inferior, en base a los errores que han cometido las páginas web de sus competidores. Además se lo enseñan y les explican todos los cambios que ha realizado su competencia desde que existen. Esto les da una capacidad competitiva que otras empresas de su sector no tienen. Alguna vez le han preguntado si es legal tener todas las webs de su competencia, que si son una especie de hackers. ¡Qué bonito es el conocimiento!

Visto por tanto la utilidad que tiene buscar en el pasado, ahora nos toca hacerlo en el presente. Así que espero que estés preparado porque como te comentaba, por estadística serás uno de los que encuentre cosas en internet que no sabía. Recuerda que también ayudamos a nuestros hijos, teniendo unos padres con una huella digital “sana”.

1.2.- BUSQUEMOS EN EL PRESENTE: BÚSQUEDAS PROFUNDAS

Por mi experiencia, la mitad de las personas que buscan como te voy a enseñar, encuentran datos suyos o de sus hijos en lugares que desconocían. Así que no perdamos tiempo y vamos de nuevo a ponernos en marcha. Realizaremos tres tipos de búsquedas.

¿Preparado para ser un auténtico investigador digital?

Para todas estas búsquedas vamos a utilizar a quien lo sabe todo: Google.

De nuevo puedo leerte el pensamiento: "Pero Iván, yo ya me he buscado con mi nombre y apellido alguna vez en Google, eso no es tan difícil". La verdad es que esto lo ha hecho la mayoría de la gente, pero es una búsqueda por decirlo suave, muy inocente. En Google no se busca así. Déjame que te enseñe las búsquedas profundas y encontrarás un nuevo universo de información:

A. BÚSQUEDAS EXACTAS DE GOOGLE

Estas son mis favoritas. Son sumamente sencillas pero muy útiles. Tan solo tenéis que acudir al buscador de Google y poner lo que queráis buscar entre comillas. Fácil.

Por ponerte un ejemplo, si buscamos este N.I.F.:

- "74747474R".

Lo que el navegador de Google entiende es que debe chequear todo internet (al menos todo lo que enlaza Google, que es mucho), buscando este N.I.F. exactamente y no otros parecidos, sino literalmente ese.

Mi recomendación es que hagas las siguientes búsquedas (como mínimo), de todos los que formáis las familia:

- **"N.I.F"**. Por ejemplo: "74747474R"

- **“Móvil”**. Por ejemplo: “666666666”
- **“Correo electrónico”**. Por ejemplo: “hola@metodocangurodigital.com”

Claro que puedes ser más creativo, todo lo que quieras en realidad, puedes hacer otras búsquedas como por ejemplo: con nombre y apellidos, cuenta corriente, tarjeta de crédito, número seguridad social, vuestra dirección etc… Pero las tres que te he comentado son obligatorias, no lo dejes. Cuando hagáis esto vas a encontrar tus datos y los de tus hijos en lugares que desconocías:

- Boletines Oficiales
- Foros
- Universidades
- Páginas Webs
- Ayuntamientos
- Subvenciones
- Oposiciones, etc…

Déjame que te adelante algo, tu N.I.F. completo o el de tus hijos no deben estar en internet. Punto. Es así de simple, esté donde esté. Sea un organismo público o privado. No debe estar, con tu NIF completo y tu nombre y apellidos se pueden hacer muchas cosas, por personas malintencionadas. En el capítulo tercero te enseñaré a eliminar todos estos datos personales, tuyos o de tu familia, que hayas encontrado.

B. BÚSQUEDA POR REDES SOCIALES

En este tipo de búsqueda vamos a comprobar que no tengas algún perfil creado con tu nombre o el de tus hijos. En el buscador de Google haremos la siguientes búsquedas (como mínimo), con este formato:

- **@facebook nombre y apellidos**. Por ejemplo: @facebook

Iván González Moreno

- **@facebook móvil**. Por ejemplo: @facebook 666666666
- **@facebook correo electrónico**. Por ejemplo: @facebook hola@metodocangurodigital.com
- **@instagram nombre y apellidos**. Por ejemplo: @instagram Ivan Gonzalez Moreno
- **@instagram móvil**. Por ejemplo: @instagram 666666666
- **@instagram correo electrónico**. Por ejemplo: @instagramhola@metodocangurodigital.com
- **@tiktok nombre y apellido**. Por ejemplo: @tiktok Iván González
- **@tiktok móvil**. Por ejemplo: @tiktok 666666666
- **@tiktok correo electrónico**. Por ejemplo: @tiktokhola@metodocangurodigital.com

De esta forma, sabremos qué "tocayos" tenemos por el mundo. Comprobaremos que nadie haya creado un perfil con tu nombre o el de tus hijos. Y por último, que tu correo electrónico o móvil no esté por algún lugar de estas redes sociales. Fácil. Adelante.

C. BUSCAR ARCHIVOS CON DATOS PERSONALES TUYOS O DE TUS HIJOS

Esta búsqueda también es curiosa. La mayoría de las personas piensan que Google solo indexa páginas webs. Esto es un error habitual. Pero Google es capaz de indexar cualquier tipo de archivo. Sus robots (arañas) llegan a la mayoría de lo que conocemos como internet pública.

¿Internet Pública?

Exacto, por si no lo sabes existe una internet privada u oculta (Deep Web), te hablaré de ella en poco más adelante en otro capítulo.

Mi recomendación es que hagas las siguientes búsquedas (como

mínimo, qué cansino soy, pero sé que puedes ser mucho más creativo que yo, confío en ti.) de los tipos de archivos más habituales, tus datos y los de tus hijos.

Así que de nuevo a Google y pondremos lo siguiente:

- **filetype:doc N.I.F**. Por ejemplo: filetype:doc "74747474R"
- **filetype:doc nombre y apellidos**. Por ejemplo: filetype:doc "Iván González Moreno"
- **filetype:doc** móvil. Por ejemplo: filetype:doc "666666666"
- **filetype:doc correo electrónico**. Por ejemplo: filetype:doc "hola@metodocangurodigital.com"

(La misma búsqueda la repetiremos con la extensión **"docx",** que son las dos extensiones de Microsoft Word)

- **filetype:pdf N.I.F**. Por ejemplo: filetype:pdf "74747474R"
- **filetype:pdf nombre y apellidos**. Por ejemplo: filetype:pdf "Iván González Moreno"
- **filetype:pdf** móvil. Por ejemplo: filetype:pdf "666666666"
- **filetype:pdf correo electrónico**. Por ejemplo: filetype:pdf "hola@metodocangurodigital.com"

(Formato de Adobe)

- **filetype:ppt N.I.F**. Por ejemplo: filetype:ppt "74747474R"
- **filetype:ppt nombre y apellidos**. Por ejemplo: filetype:ppt "Iván González Moreno"
- **filetype:ppt** móvil. Por ejemplo: filetype:ppt "666666666"
- **filetype:ppt correo electrónico**. Por ejemplo: filetype:ppt "hola@metodocangurodigital.com"

(La misma búsqueda la repetiremos con la extensión **"pptx"**, que son las extensiones de Microsoft PowerPoint)

- **filetype:xls N.I.F**. filetype:xls "74747474R"
- **filetype:xls nombre y apellidos**. Por ejemplo: filetype:xls "Iván González Moreno"
- **filetype:xls** móvil. Por ejemplo: filetype:xls "666666666"
- **filetype:xls correo electrónico**. Por ejemplo: filetype:xls "hola@metodocangurodigital.com"

(La misma búsqueda la repetiremos con la extensión **"xlsx"**, que son las extensiones de Microsoft Excel)

- **filetype:odt N.I.F**. filetype:odt "74747474R"
- **filetype:odt nombre y apellidos**. Por ejemplo: filetype:odt "Iván González Moreno"
- **filetype:odt** móvil. Por ejemplo: filetype:odt "666666666"
- **filetype:odt correo electrónico.** Por ejemplo: filetype:odt hola@metodocangurodigital.com

(La misma búsqueda la repetiremos con la extensión **"ods"** y **"odp",** que son las extensiones de las hojas de cálculo de OpenOffice y las presentaciones de OpenOffice).

Tras esto, habrás comprobado que no se encuentren datos personales tanto tuyos como de tus hijos en estos tipos de archivos. Por cierto, sé que te habrás dado cuenta, pero es importante cómo mezclo las primeras búsquedas con estas también.

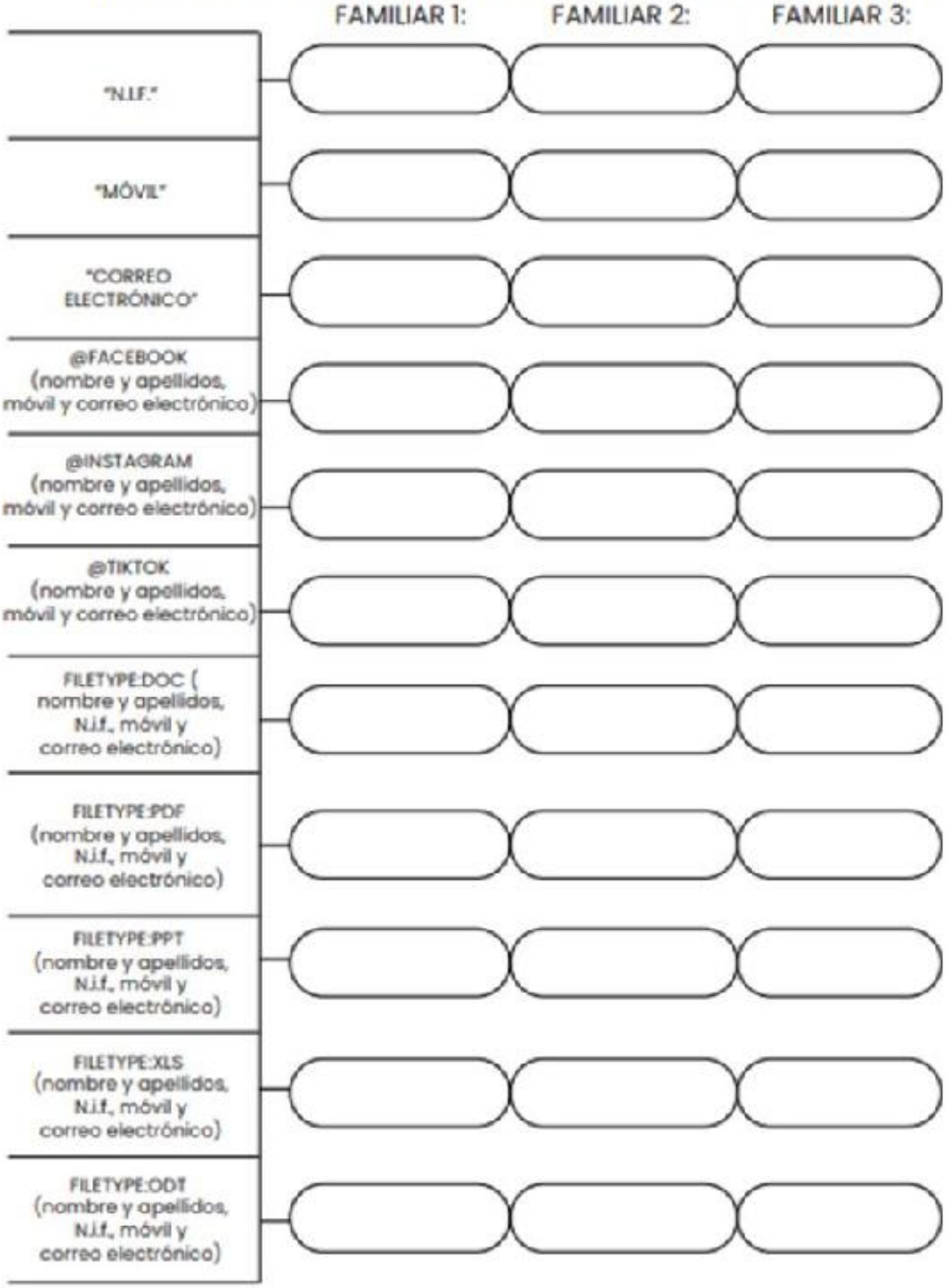
Te cuento un secreto, escribiendo el libro me acabo de dar cuenta que existe un documento con mis datos donde no debería. Siguiente paso, eliminarlo. Todo eso lo veremos como ya te adelantaba en el capítulo tercero.

HOJA DE RUTA 1.- CHECK LIST: EL PRESENTE DE TU FAMILIA EN INTERNET

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Este es nuestro primer formulario: **"Hoja de Ruta"**. Estos documentos están creados para ser un check list (es una tabla resumen de verificación de aquello que tienes que revisar, pero queda más guay check list). Creo que os puede ayudar a monitorizar el presente de internet, de cada uno de los miembros de tu familia, e incluso de otras personas conocidas a las que queráis ayudar. Como ya sabes, tienes a tu disposición recursos adicionales para tener más "Hojas de Ruta", por si la necesitas. En el libro por espacio solo puede incluir una. Ah y siempre estaré feliz de que me cuentes qué descubriste en tus búsquedas: hola@metodocangurodigital.com.

CHECK LIST: EL PRESENTE DE TU FAMILIA EN INTERNET



1.3.- AUTOMATIZAMOS EL FUTURO: SABER SI ALGUIEN EN TIEMPO REAL MENCIONA A TUS HIJOS

Te conozco. Tu trabajo, la casa y la agenda de los peques absorben tu tiempo. Sientes que no puedes llegar a todo, a veces te preguntas cómo lo hacían tus padres. Piensas que eran otros tiempos, menos estrés, menos carreras como un pollo sin cabeza. Para colmo, la única manera de tener cierta tranquilidad es que estén conectados a las pantallas, sea un móvil, tablet, ordenador o videojuego. Pero eso también te preocupa. Sientes que no les dedicas el tiempo suficiente. Pero además también te preocupa que durante tantas horas que están conectados: puedan hablar con extraños, entrar en sitios seguros o ser víctimas de acoso.

Y ahora llega este abogado friki y te da un check list de cómo buscar la información que hay de tus hijos en internet. Piensas que lo puedes hacer. Lo vas a hacer. Pero en el fondo sabes que sería inviable estar haciendo esto constantemente.

¿Me he acercado?

Tanto si es así como si no, tengo la solución. Te pido que hagas lo anterior solo una vez, porque las siguientes se harán automáticamente. ¿A qué suena bien? Pues en marcha.

Para automatizar las búsquedas vamos a utilizar de nuevo a Google. En concreto un servicio que se llama "alertas". Llegáis al mismo poniendo en Google directamente: **"Alertas Google".** También lo podéis hacer en la siguiente dirección: www.google.es/alerts. (como ya te comentó, recuerda que al final del libro te dejaré todos los enlaces y webs que menciono, con sus respectivos códigos QR).

Este servicio de Google es muy sencillo de configurar y nos va a permitir poner a Google de nuestro lado. De esta forma, cada vez que indexe un contenido que nosotros le diremos nos avisará por

correo electrónico. No os lo he dicho, pero para utilizarlo necesitaremos tener una cuenta de Gmail. Lógico, todo queda dentro de Google.

Vamos a configurarlo entonces.

Una vez que aterrizas en la Web, encontrarás una "caja" de texto en la parte superior. Solo tienes que introducir tu alerta: por ejemplo hagamos una con el N.I.F. tal y como ya sabemos.

- "74747474R"

Tras esto le damos al botón de <crear alerta>. Ya está creada. Esto significa que nadie podrá poner tu N.I.F. ni el de tus hijos sin que lo sepas. ¿A que mola?

¿A qué correo electrónico nos avisaran?

Pues al mismo con el que hemos creado la alerta. Pero no corras, todavía no hemos terminado. Tendremos que configurar algunos parámetros más. Justo al lado de la alerta que has creado aparecerá un lápiz, haz "clic" en el mismo. Te aparecerán tan solo cinco cuestiones para configurar, así que será sencillo:

- **Frecuencia.** Con tres opciones: <cuando se produzca>, <como máximo, una vez al día> y <como máximo, una vez a la semana>.
  Esta opción se refiere a la frecuencia con la que quieres que te avise. Siendo contenido sensible tuyo y de tu familia, la opción ideal es cuando se produzca. Las otras opciones tienen más sentido: si estás monitorizando tu marca, la competencia, noticias sobre un tema o las veces que se pone el fijo de tu empresa. Que son cuestiones para las que también podría servir esto.
- **Fuentes.** <Automático>, <noticias>, <blogs>, <web>, <vídeo>, <libros>, <foros>, <finanzas>.
  Aquí ya intuyes la opción que marcaremos. Quiero que me avise siempre, aparezca donde aparezca. **Marca**

<automático>.

- **Idioma.** <Todos los idiomas> o el que consideres oportuno. Nunca se sabe, así que **todos los idiomas** son la opción correcta.
- **Región.** <Todas las regiones> o las que estimes oportunas. Igualmente lo ideal es que dejes **todas las regiones.**
- **Cantidad.** <Solo los mejores resultados> o <todos los resultados>.
  Aquí queremos que nos muestre **todo los resultados.**

Listo. Alerta de Google configurada.

HOJA DE RUTA 2.- CHECK LIST: CREANDO UN ESCUDO DIGITAL A FUTURO

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Pues ahora a trabajar, tienes que hacer un listado de aquellas cuestiones que quieres que Google te avise. **Yo comenzaría por añadir todas las alertas que ya hiciste de manera manual en el apartado anterior**. Así las tendríamos configuradas para que se hagan automáticamente, ojo es importante, todos los parámetros utilizados también se pueden utilizar aquí.

Trabajo de una vez, alertas para toda la vida. Merece la pena el esfuerzo. Además, te pediría que algunas las configuraras con tus hijos, para que vean cómo se hace y cómo sus padres también los cuidan en el mundo digital. Te dejo también un formulario para que te sea más sencillo. ¡marchando la "Hoja de Ruta 2"!

FAMILIAR

FRECUENCIA

- Cuando se produzca
- Como máximo, una vez al día
- Como máximo, una vez a la semana

FUENTES

- Automático
- Noticias
- Blogs
- Web
- Video
- Libros
- Foros
- Finanzas

IDIOMA

- Todos los idiomas
- El que consideres oportuno

REGIÓN

- Todas las regiones
- Las que consideres oportunas

ALERTAS SUGERIDAS: CREANDO UN ESCUDO DIGITAL A FUTURO

	FAMILIAR 1:	FAMILIAR 2:	FAMILIAR 3:
"N.I.F."			
"MÓVIL"			
"CORREO ELECTRÓNICO"			
@FACEBOOK (Nombre Y Apellidos, Móvil Y Correo Electrónico)			
@INSTAGRAM (Nombre Y Apellidos, Móvil Y Correo Electrónico)			
@TIKTOK (Nombre Y Apellidos, Móvil Y Correo Electrónico)			
Filetype:doc (Nombre Y Apellidos, N.I.F., Móvil Y Correo Electrónico)			
Filetype:pdf (Nombre Y Apellidos, N.I.F., Móvil Y Correo Electrónico)			
Filetype:ppt (Nombre Y Apellidos, N.I.F., Móvil Y Correo Electrónico)			
Filetype:xls (Nombre Y Apellidos, N.I.F., Móvil Y Correo Electrónico)			
Filetype:odt (Nombre Y Apellidos, N.I.F., Móvil Y Correo Electrónico)			
Sé Creativo:			
Sé Creativo:			
Sé Creativo:			
Sé Creativo:			

Esta es mi propuesta, pero puedes ser creativo y añadir más. Se me ocurre que sería buena idea también añadir la dirección de tu casa, el número de la seguridad social, tarjeta de crédito y cuenta del banco etc… el límite es tu imaginación. Te he dejado algunos espacios en blanco para que puedas utilizarlos.

Si se te ocurren más alertas que puedan ser útiles no dudes en contármelo:hola@metodocangurodigital.com, y las añado para la siguiente edición.

Con esto hemos llegado al final del capítulo primero. Ya estás en disposición de buscar todo lo que hay de ti y de tu familia en internet. Tanto en el pasado, como en el presente, como automatizando el futuro. Felicidades. Pero puede ser que alguien se esté preguntando y con razón que estas búsquedas son solo de texto. ¿Y las fotografías? Son el contenido rey en internet. ¿Se quedan fuera de nuestras búsquedas? Cierto, de estas sí. Pero ahí entra el capítulo segundo, vamos a por él.

Los Secretos de las Fotografías en internet

2.- LOS SECRETOS DE LAS FOTOGRAFÍAS EN INTERNET

La Red ama nuestras fotografías y las de nuestros hijos.

Nos premian y posicionan mejor por subir fotografías, cuantas más mejor. Existen redes sociales que nacieron para lo visual: fotografías y vídeos. Me imagino que en algún momento, te habrás preguntado por qué tanto interés en nuestras fotografías. ¿Recuerdas la frase de inicio del libro? Si algo es gratis en internet el producto eres tú.

Cuando subes texto eres consciente de lo que publicas (más o menos). ¿Pero lo eres también cuando subes imágenes? Y la pregunta del millón: ¿lo son nuestros peques?

La respuesta es fácil: ¡no tienen ni idea!

Si cuando subes texto es como si hablaras, cuando subes fotografías es como si gritaras a pulmón lleno toda tu vida, a miles o millones de personas. ¿Crees que exagero?

Las fotografías arrojan tanta información, que cuesta procesar todo lo que regalamos de nuestra privacidad al subir fotografías: dicen dónde vivimos, dónde estudiamos, a qué hora vamos al supermercado, el día que vamos al gimnasio, dónde hemos estado de vacaciones, la marca y modelo de nuestro teléfono, si hemos retocado la fotografía o es la original, etc…

¿No me crees? Pues en este capítulo te enseño cómo mirar todo esto. Así que comencemos que tengo mucho que contarte (cómo disfruto este libro, jeje).

2.1.- ¿CÓMO SABER DÓNDE ESTÁN LAS FOTOGRAFÍAS TUYAS Y DE TUS HIJOS?

Tras leer lo anterior y el capítulo primero, me imagino que estarás con ganas de responder a esta pregunta.

¿Cómo saber dónde están las fotografías tuyas y de tus hijos?

Así que no vamos a dar vueltas. Ya me vas conociendo y quiero que este libro vaya a lo práctico. No estoy aquí para hacerte perder el tiempo.

De nuevo vamos a acudir a Google (en estos dos capítulos lo hemos utilizado mucho, por esto tengo con Google una relación de amor-odio), y utilizaremos las llamadas: búsquedas inversas. Ahora, si se pudiera poner música en los libros, sonaría un redoble de tambores.

¿Cómo funcionan estas búsquedas inversas?

Pues como todo lo que te estoy enseñando: de forma muy sencilla. Por cierto, nunca confundas mantener las cosas sencillas con simples. Me voy a poner yo de conejillo de indias.

En el buscador de Google vas a escribir: Iván González Moreno. Una vez le des a la tecla de <Intro>, por defecto estarás en la pestaña de <Todo>. Cámbiala a la que tienes justo a su derecha que indica: **<Imágenes>.** Varias recomendaciones previas:

- Utiliza el navegador **Google Chrome**, pongámoslo fácil para Google.
- Hazlo **desde un PC**, no desde el móvil o tablet.
- **Haz búsquedas abiertas**. Como puedes leer no he puesto mi nombre entre "". Quiero que busque lo más ampliamente posible. Prefiero que aparezcan otros Iván González, aunque

no sea yo. Aquí filtraremos manualmente.

Cuando haces esto pueden ocurrir dos cosas diferentes: la primera que no aparezcas. Es decir, que seas invisible a Google. ¡Piropazo! Esto es una de las cosas más bonitas que te pueden ocurrir en internet, felicidades.

Cuidado. No seas inocente. No confundas no aparecer en las búsquedas de Google con no estar en internet. Recuerdo no hace mucho, que una persona me dijo que no estaba en internet. Le pedí una hora de tiempo, ¡suficiente para hacerle un informe de más de 20 páginas! Todos estamos en internet, no lo olvides. Te guste o no es así.

Me encanta poner este ejemplo: internet es como un bloque de vecinos. La comunidad de propietarios de Internet, jeje. Tú que vives en el 4A decides no hablar con nadie. Puedes hacerlo. Es tu decisión. Pero no puedes controlar que el resto de vecinos de tu bloque no hable de ti. Es más, conociendo la forma de ser que tenemos, seguramente hablarán más. Dirán cosas como: se cree mejor porque no habla con nadie, tú has visto a qué horas sale, las pintas que me lleva, dónde dices que trabaja, sus hijos son iguales, etc…

Internet es el mayor bloque de vecinos del mundo. Pero sin administrador de fincas.

Dicho lo anterior, reventaba si no lo decía. Vamos con la segunda opción. Resulta que sí sales en Google imágenes. Tanto tú como tus hijos. Puedes aparecer en un sitio al que hayas dado permiso o no. Las preguntas son las mismas:

- ¿Cómo puedo asegurar que esa fotografía no esté en lugares donde yo lo desconozco?
- ¿Se puede haber utilizado para crear perfiles falsos?
- ¿Alguien con mi foto está buscando pareja?
- ¿O quizás animando a las personas a invertir en

criptomonedas?

- ¿Mi imagen se está utilizando para poner reseñas o comentarios falsos?

Todo esto es muy típico, y yo he vivido todas las opciones en mi despacho. Es aquí donde entran las búsquedas inversas de Google (gracias Google por esta opción que utilizo casi cada día):

- Nos situaremos sobre la **fotografía en cuestión** (lo siento, no se puede hacer con todas a la vez). Haremos "clic" en el botón derecho del ratón y abrimos el desplegable. Tenemos que darle a la opción **<copiar dirección de imagen>** o **<copiar dirección de la URL>.**
- Realizado este primer paso, tendremos que acudir a la **imagen de la cámara de fotos** y hacer "clic". Lo encuentras a la derecha del buscador. Se te abrirá la opción de **<Buscar por imagen>**, en esa "caja" de texto **pegaremos la dirección** que hemos copiado en el paso anterior. Recuerda que puedes hacerlo con el botón derecho y la opción de <pegar> o con el juego de teclas <ctrl + v>. Le daremos a la tecla de **<intro>.**

Tras hacer esto, Google lo que entiende es que le estoy indicando una fotografía y que debe buscar entre todo internet (sus páginas indexadas) fotografías que coincidan con esta. Incluso derivadas de esta, imagínate que la han recortado o editado un poco. Así es de potente su algoritmo. Bienvenidos a las búsquedas inversas. Ya puedes saber dónde están las fotografías de tus hijos en todo momento y lugar.

De nuevo tienes la misma duda: "Oye Iván, he encontrado fotografías donde no deberían estar (algo muy habitual por otro lado). ¿Cómo las elimino? Recuerda que eso lo veremos en el capítulo tercero.

JUERETO 2.- BÚSQUEDAS INVERSAS

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Te propongo el segundo "Juereto". Recuerda esa palabreja que es una mezcla entre juegos y retos. En esta ocasión se trata de lo siguiente.

En primer lugar, tenéis que escoger a tres personas de la familia. Ya los tenéis, ¿verdad? Pues a continuación, con sus nombres y apellidos hacéis una búsqueda en Google imágenes **para descubrir si aparecen o no, y si tienen un "doble" o no**. Alguien que se llama como tu familiar.

Si no aparecen en Google imágenes los llamamos invisibles. **Siendo un punto por familiar invisible. Por otro lado, si localizas un "doble" (te prometo que no es tan difícil), será otro punto por doble**. En mi caso, al buscar: Iván González, me acabo de encontrar un doble mío, aunque en mucha mejor forma que yo, jeje.

La puntuación máxima en esta primera parte **será de 6 puntos**. Si encontráis tres familiares invisibles y que esos tres tengan doble.

En la segunda parte, se escogerá: **a un cantante, un deportista, un famoso y un influencer o youtuber.**

Se buscarán sus fotografías en Google imágenes. Al igual que antes, si **encontráis un "doble",** una persona que se llama igual que la persona que habéis escogido, **será un punto**. Lo máximo que podréis obtener **serán cuatro puntos.**

Y ahora, os tocará buscar "copiones". Eso significa, que la misma fotografía (que habéis utilizado del cantante, deportista, famoso e influencer o youtuber) una vez realizada su búsqueda inversa, aparezca en al menos tres lugares diferentes de internet. Pudiendo obtener también un **máximo de 4 puntos.**

Por lo que la cantidad máxima de puntuación a obtener en este

“Juereto” es de 14 puntos. Quien más puntos obtenga gana, tú decides el tiempo máximo.

Ya sabes que la mejor forma de aprender con tus hijos es jugando. Con este “Juereto” le enseñarás cómo hacer una búsqueda inversa. Este es un recurso que les puede ser muy valioso, les puede “sacar” de muchos problemas, algunos de los que le daría vergüenza decírtelo. Recuerda que tienes a tu disposición un cuaderno adicional con plantillas de estos documentos.

CONCURSANTE	

1º JUERETO
(Máximo 6 puntos)

FAMILIAR 1: _____		FAMILIAR 2: _____		FAMILIAR 3: _____	
INVISIBLE (1 punto)	DOBLE (1 punto)	INVISIBLE (1 punto)	DOBLE (1 punto)	INVISIBLE (1 punto)	DOBLE (1 punto)

2º JUERETO (Máximo 8 puntos)	1.- CANTANTE: _____		2.- DEPORTISTA: _____	
	DOBLE (1 punto)	COPIÓN (1 punto)	DOBLE (1 punto)	COPIÓN (1 punto)

2º JUERETO (Máximo 8 puntos)	3.- FAMOSO: _____		4.- INFLUENCERS/ YOUTUBERS _____	
	DOBLE (1 punto)	COPIÓN (1 punto)	DOBLE (1 punto)	COPIÓN (1 punto)

PUNTOS TOTALES (Máxima puntuación 14 puntos)	

Como me pasaba cuando te enseñaba la puerta del tiempo en el capítulo primero, me gustaría contarte algunos ejemplos reales para que veas lo útil que puede ser esto. Son cuestiones diferentes a la protección de tus hijos. Pero es que estoy seguro de que en algún momento serán un chaleco salvavidas para ti o para alguien que conozcas. Pongamos tres ejemplos:

En el primero: José Antonio está interesado en comprar una moto. Hace tiempo que busco un modelo en especial, la verdad entre tú y yo, José Antonio es un pelín "quisquilloso", más aún cuando de motos se trata. De repente, como llovido del cielo, encuentra una oferta de segunda mano, no puede ser, es la moto de sus sueños. ¿Y sabes qué? ¡A un precio espectacular!

En el anuncio se explica que es de un particular que la compró hace un tiempo pero que por motivos de trabajo ya no la utiliza, que prefiere venderla para que alguien la pueda disfrutar. Está casi nueva, con pocos kilómetros, continúa el anuncio.

Era todo tan perfecto, que José Antonio que es amigo mío desde el instituto, decidió llamarme. Tras realizar una búsqueda inversa, nos dimos cuenta de que las fotografías de la moto del supuesto particular, en realidad las había cogido "prestadas" de un concesionario oficial, el anuncio era falso. Qué decepción se llevó mi amigo. Pero mejor decepcionado que timado. Si las personas supieran hacer esta pequeña búsqueda antes de comprar muchas cosas online, las estafas se reducirían una auténtica barbaridad. Pruébalo y me cuentas. Y como decía un filósofo español, ahora vas y lo cuentas.

En segundo lugar: Yosis es el dueño de un hotel familiar que está de moda. Abrió hace menos de un año, pero se ha esforzado mucho en generar una experiencia maravillosa en todos los huéspedes que pasan por su hotel. Así lo demuestran las reseñas que les dejan cada día en uno de los mayores portales de reservas del mundo.

Pero hoy al despertarse, acaba de encontrarse con una reseña

horrorosa. Crítica al hotel con fotografías que él sabe que no son del mismo, además de unos comentarios descalificativos tanto del hotel como de las personas que trabajan en el mismo. Semáforo rojo. Esto puede ser grave para la reputación del hotel.

Tras revisar la foto del perfil de la persona que ha puesto el comentario, está seguro de que no es de ninguna persona que haya estado alojada en el hotel en esas fechas. Yosis lo sabe bien, porque hace el check in de todas las personas que llegan. El comentario es falso, pero tiene que demostrarlo para que lo eliminen.

Yosis (que es mi hermano) sabe hacer búsquedas inversas. Tras realizar la búsqueda de la foto de perfil, le lleva a una persona de nacionalidad canadiense. Más raro aún. Tras ponerse en contacto con él por Messenger, la persona de la fotografía le confirma que nunca ha hecho ese comentario. Que nunca ha tenido el placer de estar en su hotel (Yosis que no pierde una, aprovecha para invitarlo) y que no le importa ponerle esto por escrito.

Yosis ya puede acudir al portal de reservas y demostrar que el comentario era falso. Alguien ha suplantado a esta persona para hacer daño al hotel, de ahí a eliminar el comentario es un paso.

En tercer lugar: Rocío es una persona que hace tiempo que se quedó viuda. La soledad es muy mala, así que decide mitad por convencimiento y mitad por insistencia de sus hijas, darse de alta en una web de búsqueda de parejas. Allí conoce a Jesús. Su foto de perfil rápidamente capta su atención, es muy guapo. Le gustan los animales, viajar, leer y el cine. Dice que es hablador, simpático y deportista. Tiene un trabajo importante en una multinacional, lo que le hace viajar mucho. El dinero no es un problema para Jesús, tal y como él dice.

Pero hay algo que no le encaja a Rocío, para eso tiene un sexto sentido, como dicen sus hijas es medio bruja. Recuerda que hace poco escuchó una entrevista de un abogado friki, donde enseñaba a realizar búsquedas inversas. Eso es lo que hará. Tras realizar las búsquedas inversas de sus fotos de perfil, se encuentra que: ni se

llama Jesús, ni trabaja en una multinacional, sino que ha cogido una fotografía de un modelo australiano. Por lo que el perfil es falso. Este es un modo operandi muy típico en páginas de búsquedas de citas por internet. Lo que hubiera venido después de contactar Rocío con él, habría acabado con la cuenta corriente de Rocío desplumada, casi con seguridad.

Ahora entiendes por qué me encantan las búsquedas inversas. Las adoro. Pero como te decía al empezar el capítulo, las fotografías revelan mucha más información de la que te puedes imaginar. Por eso las redes sociales las aman y las fomentan. Es el momento de contarte qué información exacta revelan y cómo mirarla, vamos al siguiente apartado.

2.2.- LAS FOTOGRAFÍAS REVELAN DÓNDE VIVES: LA FICHA DEL LIBRO

¿Recuerdas la época cuando visitabas tu biblioteca más cercana? Cierra los ojos. El placer de escoger libros: hojearlos hasta decidirse por uno. Acercarte al mostrador y pedirlo prestado. Entonces el bibliotecario o bibliotecaria cumplimentaba una ficha en papel (parece que puedo verlo), donde estaban los datos del libro que te llevabas prestado. En esa ficha, se recogía: el autor, una descripción del libro, a quién se le prestaba y la fecha de devolución del mismo. ¿A que lo recuerdas?

Eras consciente que del libro que te llevabas prestado, en la biblioteca quedaba una ficha con datos adicionales del mismo. Conserva esa imagen en tu mente.

Ahora que ya estás en el contexto adecuado y con esa imagen clara en tu memoria, debo decirte que de cualquier fotografía que se sube a internet, tiene también una ficha adicional con información. Esa ficha de la que hasta este momento no eras consciente, contiene mucha información, como la que contenía la ficha del libro. Las preguntas que te debes estar haciendo en este momento son:

¿Qué información exactamente contiene? ¿Cómo puedo verla? ¿Y qué utilidad puede tener?

Genial, estamos en el punto exacto para avanzar. Para empezar te diré que ambas van juntas: la fotografía y la ficha son indivisibles. Es el reverso de una misma moneda.

Por un lado la fotografía. Por el otro sus metadatos. ¿Meta qué? Metadatos. Ese es su nombre real, aunque para ti y para mí siempre serán la ficha del libro. Esos metadatos, que son los datos de los datos, contienen información muy valiosa, de ahí que las redes sociales amen las fotografías.

La información que contienen los metadatos son las siguientes (tiene

más información que las que te voy a comentar, pero a efectos de este libro, estas son las más importantes):

- **Marca y modelo del móvil.**
- **Fecha, hora, minuto y segundo.**
- **Coordenadas GPS.**
- **Fotografía real (esto suena raro, ahora te cuento).**

¡Casi nada! ¡UFF! Me imagino que quieres que te cuente un poco más de cada uno y cómo se pueden utilizar para proteger a tus hijos. Tus deseos son órdenes, ¡en marcha!

- **MARCA Y MODELO DEL MÓVIL**

Esto puede no parecerte muy importante. Pero como siempre deja que te ponga un par de ejemplos: uno de nuestros peques y de otro de "no es lo que parece" (me encanta esa frase).

Jorge es un niño muy tímido, le cuesta hacer amigos. Y el hecho de ser nuevo en el colegio no ayuda mucho, además a Jorge no le gusta el fútbol y en su clase todos sus compañeros forman parte de un equipo. Sus padres ya temían que esto ocurriría. Los primeros días algunos niños se han metido especialmente con él, sobre todo Juanjo, Ramón y Miguel Ángel.

Uno de ellos ha realizado una fotografía de Jorge, justo cuando se agachaba a coger los lápices que le habían tirado estos niños, con tan mala suerte que se le han visto los calzoncillos que tanto le gustan, de uno de sus personajes favoritos, Bob Esponja (Jorge era fan de estos dibujos porque los veía con su abuelo, que ya se fue al cielo). Esto ha servido para que esa fotografía se comparta y se rían de él.

Gracias a la ficha del libro (los metadatos), se pudo saber el modelo exacto del móvil (porque los tres implicados negaron que hubieran realizado la fotografía), con el que se hizo la fotografía. Sin ninguna duda se hizo desde el móvil de Ramón. Tras hablar con los padres y

el centro, Ramón, Juanjo y Miguel Ángel se dieron cuenta de que no habían actuado bien y acabaron pidiendo perdón, lo hicieron de verdad. Después de unos meses, ahora todos se llevan bien. Descubrieron una pasión en común, el Fortnite (de los videojuegos, sus riesgos y los juegos *play to earn*, que es la tendencia que existe ahora donde pueden ganar dinero mientras juegan. Te hablaré en el siguiente libro, porque tengo mucho que contarte). Por cierto, Jorge es un crack en el Fornite y todos quieren jugar con él.

Pablo por su trabajo suele viajar mucho: es comercial. Hace poco se quedó a dormir en Sevilla. Pablo tiene la costumbre de mandar una fotografía a su mujer cada noche, deseándole buenas noches y diciéndole que la quiere (qué bonita costumbre). Qué buena gente es Pablo.

Ese día, como cada vez que se queda fuera de casa hizo lo mismo. Lo que no esperaba Pablo fue la respuesta de su mujer. Tras el envío de la foto, su mujer contestó como siempre diciéndole que también le quería, pero con una pregunta: "¿Me podrías explicar si tienes un Iphone porque la foto ha sido realizada con un Samsung?". La respuesta de Pablo comenzó con el clásico "no es lo que parece".

¡Que vivan los metadatos! Quizás este sea un buen momento para un disclaimer legal (advertencia legal en castellano, aunque suena mejor en inglés). Este abogado de pueblo y un pelín friki, no se hace responsable de los divorcios que esta información pueda provocar (modo ironía on o no, quién sabe, jeje). Ya sabes lo que decía el filósofo: todo gran poder conlleva una gran responsabilidad. Utiliza esto bien. En las siguientes informaciones que puedan proporcionarnos los metadatos, volveremos sobre el momento: "no es lo que parece".

- **FECHA, HORA, MINUTO Y SEGUNDO**

De las cuestiones más útiles que te puedas imaginar. Y a la vez más importantes. Tus hijos te mandan una fotografía de la biblioteca, te dicen que está estudiando mucho. Como padre piensas que la vida

de los peques no es fácil, los exámenes vienen fuerte y ellos están estudiando para ser personas de provecho en el futuro. ¡Qué orgulloso estás!

Un segundo, espera a mirar la fecha de la fotografía. Es una fotografía de hace cuatro meses.

¿Dónde está tu hijo?

¿Recordáis el ejemplo anterior de Jorge? Pues con estos datos adicionales, sabemos en qué día, hora, minuto y segundo ocurrió. Sabemos que los profesores estaban en clase en ese momento, porque ocurrió dentro del horario de clase. Toca hablar con el profesor también.

Como siempre, os cuento un par de casos más en los que podría ser útil esta información. No son de menores, pero también pueden servirte como salvavidas en cualquier momento. Pero seguro que a ti que lees este libro, se te ocurren más. Estaré encantado de leerlos:hola@metodocangurodigital.com.

Hace no mucho, en el despacho nos llegó una polémica sobre dos inmobiliarias que discutían cuál había visitado primero una propiedad. Ambas habían realizado fotografías. Las personas mienten, los metadatos no. Fue tan fácil como mirar las metadatos de las fotografías y saber sin duda quién estuvo antes.

Visitando a un cliente, me comentaba que estaba muy preocupado. Había comenzado a trabajar en la empresa una persona por recomendación de uno de los socios. Su trabajo consistía sobre todo en llevar material a los clientes. Al poco tiempo comenzaron las quejas: nunca estaba a su hora, siempre llegaba tarde. Pero al hablar con esta persona siempre decía lo mismo: yo estoy a mi hora, son ellos los que se retrasan para recoger el pedido.

La cuestión era complicada. Recuerda que comenzó a trabajar por recomendación de uno de los socios, había que estar seguro. La idea que se nos ocurrió era sencilla, pero ingeniosa. Antes de entregar el material realizaba una fotografía del mismo. La excusa que le dijimos

era saber que el material era el correcto, pero la realidad es que ya sabíamos por la fotografía la hora, el minuto y el segundo. No había duda, llegaba tarde casi por sistema. Y se había probado.

- **COORDENADAS GPS**

Si esto fuera un pastel, esto sería la guinda. Qué útil es conocer por una fotografía dónde están nuestros hijos. La cantidad de ejemplos que podría poneros sobre esto es inagotable. Estas coordenadas GPS que integran las fotografías tienen un margen de error mínimo.

Fotografías realizadas a nuestros hijos con la intención de hacerles daño, que después se hacen virales. Podemos saber exactamente: dónde se realizaron, el día y la hora. Esto puede ser tremendamente útil para que no vuelva a repetirse. Podemos saber la clase, el profesor que estaba en ese momento, los compañeros, etc…

Se hace necesario que nuestros hijos y nosotros comprendamos el alcance de esto. Como siempre, te pongo un caso real, este es uno de los que más me preocupan por cierto. Te ruego que lo cuentes por ahí a otros padres también.

Belén tiene 16 años. Está agobiada por la cantidad de tareas que tiene que hacer. Para colmo tiene varios exámenes la semana que entra, por lo que decide junto a sus padres que este fin de semana se quedara en casa y no los acompañará a la casa del pueblo. ¡Con lo que a Belén le gusta la casa en el pueblo! Pero es una chica muy responsable, siempre lo fue. Se quedará sola en casa estudiando, al fin y al cabo. ¿qué puede ocurrir? Son solo dos días. Además tiene a su abuela que no vive lejos por si hubiera una urgencia.

Después de marcharse sus padres, lo primero que hace Belén es realizarse una fotografía en el sofá de casa (es la primera vez que se queda sola en casa, está emocionada), la envía a varios amigos y la sube a internet con el texto: “Mis padres se van de finde y a mí me toca quedarme en casa sola estudiando”.

Es un gesto inocente, ¿verdad? Pero ya sabéis lo que significa.

Quizás hace un rato no, pero ahora entendéis la barbaridad que está cometiendo. Sabéis qué información contiene la fotografía. Está revelando a un montón de personas dónde vive (desde que se lo manda a sus amigos y lo sube a internet, se pierde el control), y que va a estar sola todo el finde. Sus amigos que recibieron la fotografía y también la compartieron, están ayudando a esta difusión sin saberlo. Se está exponiendo la seguridad de Belén y nadie parece tener consciencia de ello.

Cambiando de tema, estas fotografías pueden ayudarnos a localizar a nuestros hijos en caso de no saber dónde están, o al menos para saber por dónde comenzar a buscarlos. Espero que nunca tengas que utilizarlas para eso.

Las redes sociales, por las fotografías lo saben todo de nosotros (por eso quieren cuantas más mejor). Saben dónde estudian nuestros hijos, dónde trabajamos, cuándo solemos ir al supermercado y al gimnasio, qué restaurantes frecuentamos, las extraescolares de nuestros hijos y un largo etc… En el capítulo sobre las redes sociales ampliaremos más esto.

Realizar fotografías dentro de casa y subirlas o compartirlas no parece una gran idea. No solo por revelar dónde vivimos, que eso ya tiene un potencial riesgo, sino que las fotografías van a revelar cuestiones que a un ojo inexperto pueden pasar desapercibidas, pero que a los ojos de los profesionales de lo ajeno no lo harán. Analizarán nuestros muebles, televisión, cuadros, vehículos y un montón de detalles que harán que nuestra casa pase a ser un objetivo apetecible. Lo siguiente que tenemos que hacer es subir una fotografía diciendo que estamos de vacaciones. Y ya puestos, puedes dejarle la llave de tu casa puesta para ponerlo aún más fácil.

Las fotografías gritan todos esos datos y nosotros nos encargamos de regalarlos. Pocas cosas pasan para lo fácil que se lo ponemos a los malos.

Imaginaros la información que alguien podría tener sobre nosotros si encuentra nuestro móvil tan solo analizando las fotografías. Pero

sobre esto hablaremos más en el capítulo dedicado a los móviles. Ahora ya entendéis por qué mis amigos nunca me preguntan dónde están. Porque si puedo llegar a saber cómo se distribuyen las habitaciones en el hotel en el que están, podríamos contestarles con la habitación exacta donde se alojan. Algo que en el tema infidelidad, da mucho de sí.

Aunque como siempre la tecnología también se puede utilizar de forma correcta. Recuerdo un email que recibí hace un tiempo, no me quiero ni imaginar los que voy a recibir tras este libro, ya estoy emocionado por eso (hola@metodocangurodigital.com). Era de una persona que tiene un blog de viajes muy conocido. En cada uno de sus viajes llevaba una pequeña libreta donde iba apuntando cada uno de los lugares que visitaba, día, hora, etc… Si no lo hacía así, al regresar del viaje no recordaba las visitas y horarios para escribirlos en su blog. Esto de apuntar cada cosa que hacía se estaba volviendo cada vez más complicado, había llegado a un punto que le impedía disfrutar de los viajes como a ella le gusta. Tras una de mis charlas a las que asistió, descubrió que las fotografías ya hacían esto por ella (ya eran su libreta). No era necesario apuntar todo lo que hacía en su viaje de una semana, por miedo a perderlo. Las fotografías ya harían ese recordatorio por ella. Desde entonces me contaba que había vuelto a disfrutar mucho más de los viajes. Os he dicho que me encanta mi trabajo.

Otro email que recuerdo con cariño, es el de un administrador de fincas (profesión a la que le tengo un enorme respeto), que tenía que demostrar las visitas que realizaba a sus comunidades. Pero no sabía cómo hacerlo, para que fuera lo más sencillo posible. También tenía que demostrar las visitas que realizaban los proveedores de las comunidades, por ejemplo un fontanero o un electricista. Cuando descubrió que podía hacerlo a través de las fotografías, su trabajo se simplificó mucho. Y los vecinos de las comunidades siempre le agradecen que sea tan metódico con esto. La primera vez que pasó un informe, no solo era capaz de identificar el día y hora de la visita, sino que incluso ponía los minutos y segundos, jeje.

- **FOTOGRAFÍA REAL**

Existen más datos que se podrían mirar en los metadatos. Pero estos que estamos comentando son los más útiles. Este último, es la fotografía real.

Ya sé que de primeras no es muy intuitivo, pero dejadme que me explique, cuando uno realiza una fotografía es habitual editarlas después. Cuando se hacen fotografías para dañar a nuestros hijos, esto se hace con frecuencia. Esa parte que se edita, suele contener información muy importante sobre: el contexto, personas que intervienen, más información del lugar donde ocurre, etc…

Toda esa información está también en los metadatos, donde encontramos las fotografías antes de ser editadas, a eso me refiero con la fotografía real.

Sobre esto, tendría que realizar otro libro. Lo podríamos llamar cómo detectar infidelidades con la tecnología (modo ironía on). Esta parte sería uno de los contenidos estrella. Recuerdo cuando una conocida me contó el caso de una fotografía en la que se veía un señor de cintura hacia arriba, con traje y corbata, muy serio él. Tras revisar los metadatos su mujer, se lo encontró de cintura hacia abajo como Dios lo trajo al mundo. Además, por los metadatos tenía: el hotel, día, hora, etc… El marido intentó la estrategia del "no es lo que parece", pero al poco se calló. Estaba cazado.

Creo que ya puedes hacerte una idea del potencial de la ficha del libro (metadatos) y cuánta información nos puede revelar. En este momento me veo en la obligación de decirte que lo utilices para hacer el bien, recuerda aquella frase de un filósofo de nuestro tiempo: todo gran poder conlleva una gran responsabilidad :)

Vamos de nuevo con mis dotes de adivino. Apuesto a que estás pensando: "Muy bien Iván, ¿pero cómo se mira esto? Tiene pinta de ser muy complicado".

Pues la verdad es que es muy sencillo. Existen numerosas aplicaciones web para visualizar estos metadatos. Incluso una parte

podrías verlos situándose en la fotografía y con el botón derecho hacer "clic" en **<propiedades>**, para posteriormente irte a la opción de **<detalles>**. Pero tendrás una versión muy básica de los metadatos (aunque para algunas cosas puede servirte).

Por cierto, en la pestaña de **<avanzados>**, encontrarás la opción de **<quitar propiedades e información personal>**. Para eliminarlos. Enseña esto a tus hijos, porfa.

Pero nosotros queremos ser unos profesionales de los metadatos. Eso se consigue utilizando un programa con un nombre tan sugerente como: Foca.

Foca fue creada por la empresa Informática 64 en 2007, actualmente esta empresa se llama ElevenPaths. Es justamente a esa web donde acudiremos para descargarla: https://www.elevenpaths.com (esta siempre es una buena práctica, descargar desde las páginas oficiales de los proyectos).

Si bien su utilización es muy sencilla para lo que aquí vamos a necesitar, la instalación se os pueda complicar y con las decenas de tutoriales que encontraréis en Youtube, quizás no sea suficiente. En ese caso, no dudes en pasarte por tu empresa de informática de confianza, ellos lo harán en minutos. También puedes pedir ayuda a algún amigo que se le dé bien la tecnología.

Una vez instalado (es la única dificultad que encontrarás), la utilización no tiene ningún misterio:

- Tras abrir el programa **crearemos un proyecto nuevo**, puedes ponerle el nombre que quieras.
- Tras esto, en tu parte izquierda aparecen diferentes opciones. La que te va a llamar la atención es la que se llama **<metadata>**.
- Tras hacer "clic" en ella, **nos dejará cargar la fotografía que queramos**.
- Tan solo tenemos que escoger. La veremos seleccionada en

la parte inferior.

- Por último, botón derecho del ratón y darle a la opción: **<extract all metadata>**.

A partir de ahí, a divertirse. Encontrarás todo lo que hemos hablado.

JUERETO 3.- METADATOS "FICHA DEL LIBRO"

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Vamos a poner en práctica lo aprendido. Sigamos con nuestros "Jueretos". En este caso podéis competir individualmente o por parejas. Para ello iremos a la cueva de Ali Babá, que es el lugar donde acumuláis miles de fotografías (todos tenemos una cueva de Ali Babá, ¿verdad?) Es difícil de explicar, como cuando teníamos un carrete de 24 fotografías imprimiéramos más recuerdos que ahora que tenemos miles.

Una vez en la cueva de Ali Babá, escogeréis cuatro fotografías. Las que queráis. Unas más antiguas y otras más jóvenes, no me hagáis trampa.

De la primera fotografía, deberéis adivinar el año. Ganará, como en los concursos de la tele, el que más se acerque sin pasarse. El acertante se llevará **2 puntos.**

De la segunda fotografía, deberías adivinar el mes. Al igual que antes, gana el que más se acerque al mes correcto, sin pasarse. El acertante se llevará **2 puntos.**

De la tercera fotografía, deberéis adivinar tanto el mes como la hora en que se hizo la fotografía. El acertante del mes, sin pasarse se **lleva 1 punto**. Y el de la hora, **1 punto también.**

Y por último, de la cuarta fotografía, tendréis que adivinar el lugar exacto en el que estabais cuando la realizasteis. El que acierte, **se lleva 2 puntos.**

El que más puntos tenga, escogerá dónde cena la familia en su próxima salida. Y ahora como si fueras un mago, vas a enseñarles a tus hijos cómo extraer los metadatos de las fotografías. Ya me cuentas quién ganó la cena.

De esta forma, ellos van a comprender qué ocurre cuando se ceden fotografías a la ligera y qué contenido tienen las mismas. Disfruta del

juego.

Concursante 1	
Concursante 2	
Concursante 3	
Concursante 4	

FOTOGRAFÍA 1	AÑO	FOTOGRAFÍA 2	MES
Concursante 1		Concursante 1	
Concursante 2		Concursante 2	
Concursante 3		Concursante 3	
Concursante 4		Concursante 4	

FOTOGRAFÍA 3	MES	HORA
Concursante 1		
Concursante 2		
Concursante 3		
Concursante 4		

FOTOGRAFÍA 4	COORDENADAS GPS	HORA
Concursante 1		
Concursante 2		
Concursante 3		
Concursante 4		

PUNTOS TOTALES (Máxima puntuación 10 puntos)	

2.3.- RIESGOS DE COMPARTIR FOTOGRAFÍAS SIN PERMISO

En este apartado me vas a permitir que tenga que nombrar alguna ley. Lo siento. Mi alma de abogado ya me lo pedía, y por otro lado no me queda remedio. Pero te prometo que lo seguiré manteniendo todo lo más sencillo posible.

Vamos a responder a estas preguntas (que son las que más me hacen en el despacho):

¿Puedo hacer fotografías de mi hija en la función escolar? ¿Y si aparecen otros niños?

- ¿Puedo compartir esas fotografías en Facebook?
- Me han pedido en el colegio que firmen un documento de cesión de imágenes: ¿es válido? ¿que debe contener para estar correcto?
- ¿Puede el padre o la madre firmar el documento? ¿O tienen que firmar ambos?
- ¿Puedo mandar las fotografías por Whatsapp?
- ¿Qué consecuencias puede tener esto?
- ¿Puedo pedir que las retiren de redes sociales o páginas webs?
- ¿Cuál es la edad para que mis hijos puedan dar su consentimiento?

Perdón me he venido arriba con las preguntas. He tenido que parar porque se me siguen ocurriendo más, pero sin duda estas son las más importantes.

Para comenzar, ¿qué os parece un caso real? Sobre el mismo podremos trabajar y dar respuesta a la mayoría de estas preguntas.

Miguel Ángel tiene una hija llamada Alma que tiene 7 años. Alma se ha matriculado a clases extraescolares de escalada. En la inscripción además de la matrícula, a Miguel Ángel le pasaron un par de párrafos para que se le puedan hacer fotografías a su hija y puedan publicarse en la web o en Facebook.

El primer párrafo decía algo así: "Cede usted la imagen para todo tiempo y lugar, además de para cualquier medio presente o futuro que pueda estimarse conveniente". Miguel Ángel no vio problema en firmar esto. Además había un segundo párrafo en el que se indicaba que el progenitor que firmaba tenía el consentimiento del otro progenitor. A pesar de que Miguel Ángel está divorciado, no tiene una mala relación con su expareja, y pensó que eso no le importaría. Al fin y al cabo, ¿qué mal podían hacer unas fotografías en redes sociales?

Este ejemplo que se da cada día nos va a servir como guía para contestar a la mayoría de las preguntas que nos hacíamos.

Para que nadie se lleve a confusión, las respuestas son conforme a la normativa española y europea, que por cierto se aplica a las personas que viven en Europa, sean de la nacionalidad que sean. Aunque seas del país que seas las respuestas deberían ser muy parecidas.

En Europa, desde el año 2018, tenemos una normativa de protección de datos que se aplica en todos los países: el Reglamento General de Protección de Datos (esta es la primera norma que tengo que mencionarte, lo siento). Déjame que te cuente lo que es un Reglamento Europeo para que lo entiendas bien. Imagínate lo siguiente:

Mi mujer que se llama Raquel, un día de los que llegó a casa me espera en la entrada, se me queda mirando. Algo no va bien. Me mira fijamente, sé que me quiere decir algo, y me dice:

—Iván estás gordo. Hombre un pelín gordito sí estoy, dicho sea de paso.

Y a continuación me dice:

—En un mes te voy a pesar, más te vale estar más delgado por tu bien.

Como puedes leer, Raquel me ha marcado un objetivo. Pero me ha dejado libertad para escoger cómo hacerlo. Puedo ponerme a dieta, salir a realizar ejercicio, hacerme una liposucción o rezar directamente por un milagro (que lo necesitaré).

¿Pero esto qué tiene que ver con un Reglamento Europeo?

Un segundo que ya llego. Este era el sistema antiguo que teníamos en Europa. Nos marcaron unos resultados en cuanto a la protección de datos (y eso incluye las imágenes), pero cada país, a pesar de tener el mismo objetivo, tomó una decisión diferente. En mi ejemplo, todos los países tenemos que adelgazar. Pero cada país tomó una decisión diferente de cómo hacerlo. Unos a dieta, otros al gimnasio, otros sin hacer nada, en fin ya te haces una idea. Un desastre. Al final cada uno hacía lo que quería. Eso provocó que tuviéramos una normativa de protección de datos en cada país, y recuerda que esto afecta a las imágenes que es de lo que estamos hablando. Pero también afectaba a muchas otras cosas.

Por eso, en el año 2018 se decidió aprobar un Reglamento Europeo para estos temas, que sería algo así como si Raquel me dijera que estaba gordo y que tenía un mes para adelgazar (igual que antes), para a continuación añadir:

—Te he apuntado al gimnasio, tienes los lunes y miércoles. El jueves vendrá tu hermano para salir a correr, el sábado tu padre para ir en bici. Aquí tienes también la dieta para cada día.

Como puedes intuir, mi margen de maniobra es mínimo, queda un poco, pero mínimo. Esto es un Reglamento Europeo. No solo marca el objetivo sino también el camino para conseguirlo.

Ahora puedes comprender que si vives en Europa las reglas de juego son en esencia las mismas. Y también puedes apreciar la importancia de esta norma. Y por eso lo que te cuente sobre la

imagen es igual en toda Europa. Esta es la norma en la que nos basaremos en este apartado y a la que también acudiremos en otras partes del libro.

Por cierto, no es una explicación para darla en ámbitos académicos, explicar un tipo de norma jurídica con una dieta no creo que sea muy ortodoxo. Aunque sí que creo que es efectivo.

Ya estás listo para que empecemos a contestar las preguntas:

- **¿El documento que firmó Miguel Ángel, el padre de Alma, es válido? ¿Qué debía contener?**

Antes de entrar a analizar si con la firma de uno de los padres es suficiente o no, empezaremos por el contenido del documento. Los documentos de cesión de imagen son un clásico, nos lo harán firmar: cuando van al colegio, actividades extraescolares (como nuestro ejemplo), excursiones, clubes, campamentos etc…

Y lo habitual es contener frases como las que ponemos en nuestro ejemplo: "en todo tiempo y lugar", "para cualquier medio" o "sin límite temporal". Todas ellas son jurídicamente discutibles.

La imagen es un dato personal, sujeto a la normativa que ya hemos indicado. Y en estos documentos, como si fuera un check list que debes verificar, deberían recogerse al menos:

a. Quién solicita la imagen y para qué finalidad lo hace. No es lo mismo organizar una actividad extraescolar, matrículas, horarios. etc… que ser la imagen en la publicidad del colegio los próximos años, por poner dos ejemplos. Además de los derechos que tiene la persona a la que se le solicita su imagen, entre otros derechos, debe recogerse que puede retirar su consentimiento cuando quiera.

b. Adónde se va a ceder la imagen exactamente. Es probable que no nos importe que nuestros hijos aparezcan en la página web del centro de escalada o en su Facebook. Pero sí que nos importa que aparezcan en una valla en la autovía o se utilice

su imagen en flyers de publicidad.

c. Si la cesión de la imagen de nuestros hijos es gratuita o conlleva algún pago. Sí. ya sé que puedes pensar que se sobreentiende que es gratis. Pero deja de hacerlo, existen personas que viven de sus derechos de imagen: como los modelos o los futbolistas. Así que habrá que especificarlo en el documento.

d. Durante cuánto tiempo. Porque esto de "para siempre" no suena muy bien.

Te reto a pasar este check list a los documentos de cesión de imagen que has firmado de tus hijos.

Ya me cuentas qué tal resultó el experimento:

hola@metodocangurodigital.com

- **¿Puede el padre o la madre firmar el documento? ¿O se necesita la firma de ambos?**

En nuestro ejemplo solo firmaba Miguel Ángel. El centro de escalada para curarse en salud, decidía poner una cláusula en la que se recogía: que se le excluía de responsabilidad si uno de los progenitores no tenía el consentimiento del otro progenitor.

Lo cierto es que la mayoría de cesiones de imagen tan solo tienen por defecto una casilla o hueco para que sea firmada por uno de los padres, y ni siquiera suelen poner cláusulas parecidas a lo anterior. Aunque en la práctica no va a cambiar nada.

El consentimiento no es válido, la normativa europea es muy estricta con esto.

Te cuento cómo ha cambiado esto con un ejemplo de los míos.

Recordad que vivo en un pueblo de 5.000 habitantes, llamado Villanueva del Trabuco en Málaga (España).

Imaginaros la siguiente situación. Estando un día tomando algo con mi amigo Daniel en uno de los restaurantes de mi pueblo: "El

Talillas". Vemos que entra Penélope Cruz. No es raro porque allí se come de escándalo. Entonces mi amigo Daniel me dice que va a hablar con ella. Lo miró raro, pero conociéndolo es muy capaz. Se acerca a Penélope y le dice:

—Hi Pep, soy Daniel del Trabuco, te quedas a vivir aquí conmigo. Ella mira a mi amigo y le da un ataque de risa, se ríe mucho. Pero no dice nada.

Mi amigo vuelve a la mesa conmigo, e inocentemente me pregunta:

—Tú qué crees que ha dicho, ¿que sí o que no? Miro a mi amigo y le explico que va a ser que no.

Hasta aquí todo normal. Uno lee esto y ve que es lo lógico. La intención de Penélope nunca habría sido quedarse en el Trabuco y menos con mi amigo (molaría que visitara mi pueblo).

Pues ahora viene lo mejor, en la ley antigua que teníamos antes de esta europea que tenemos ahora, se podía entender que Penélope había dicho que sí. ¡Flipa! Es surrealista, ¿verdad? Pero así era. Cuando alguien no contestaba se entendía lo que quería entender el que preguntaba. Te pongo algunos ejemplos que eran válidos en la antigua normativa y hoy ya no lo son: si te mando un email y no me contestas es que quieres recibir más. Si no marcas esta casilla, significa que te puedo mandar publicidad. Si sigues navegando por esta web entiendo que aceptas las cookies (ya te explicaré lo que es esto).

Todo esto daba a entender lo que a ti te convenía, porque la otra persona no había dicho nada. Esto ya no existe. Si no te dicen nada, tienes que entender que es un no. Solo si dice de forma clara un sí es válido.

Pero Iván, ¿esto tiene que ver con nuestro ejemplo?

Pues claro que sí, esto es fundamental en nuestro ejemplo. Significa que Miguel Ángel, con toda la buena voluntad del mundo, no puede autorizar por su exmujer, no puede entender que a su mujer no le importaría. Más aún cuando hablamos de imagen donde es

obligatoria la firma de ambos**.** En palabras de un abogado sería algo así: la imagen es patria potestad y requiere la firma en conjunto.

Ahora vas y se lo cuentas a los documentos de cesión de imagen que has firmado. Te darás cuenta de que la mayoría no tiene esa opción. Puedes contar el ejemplo de Penélope a los responsables del cole de tus hijos, jeje.

¿Puedo hacer fotografías de mi hijo en la función escolar? ¿Y si aparecen otros niños? ¿Puedo compartir esas fotografías en Facebook?

Vamos a imaginar que estamos en la función fin de curso de nuestro hijo. Se aleja un poco de nuestro ejemplo, pero creo que también es importante comentarlo porque es muy habitual. A la función no han podido ir las abuelas (cosas del covid y de los límites de aforo), ni la mami que está a tope de trabajo. No pasa nada, el padre está en la primera fila, como el mejor de los reporteros, con el móvil dispuesto y preparado, a tope de batería para que no se le escape ningún detalle de su hijo, está más *ready* que Chanel cantando en Eurovisión. Está seguro de que después las abuelas y la mami podrán disfrutar de su grabación, está dispuesto a que no se pierdan nada.

Sin entrar en las normas de cada colegio que también pueden influir, allí está el padre preparado, la función está por comenzar. En ese momento se le acerca el padre de otro de los niños participantes y le recrimina que vaya a grabar la función, que ni se le ocurra grabar a su hijo. Que él no lo consiente. Que por protección de datos no se puede y que si lo hace le va a denunciar. Buen rollo como se suele decir. Para colmo ese es el niño que sale al lado de su hijo. No sabe qué hacer.

Este caso es muy habitual. Cambia la función escolar por otra actividad extraescolar y también nos valdría. Vamos con las respuestas.

La imagen es un dato personal, eso ya lo tenemos claro. Por tanto

está protegida por la normativa de la que estamos hablando, eso también lo tenemos claro. Ahora viene la novedad, las normas siempre deben guardar un equilibrio en su aplicación, no existe una súper norma que siempre gana, sino que en la mayoría de las ocasiones tenemos que buscarles su aplicación con sentido común. De lo contrario, serían abusivas.

Las grabaciones realizadas con fines particulares, no están sujetas a esta normativa, por lo tanto, la grabación de un padre de su hijo, no está sujeta a los mismos requisitos que nuestro ejemplo de la escalada. El padre puede grabar sin ningún tipo de problema (solo habría que tener en cuenta las normas del colegio o del evento, si existen). Y claro que grabando a su hijo en una función escolar van a aparecer otros menores, pero no son el objeto principal de la grabación. Es algo inevitable.

Esta grabación además se podrá pasar por Whatsapp a las abuelas y la madre. También al grupo privado de Whatsapp de la familia. Pero ojo, lo que no se podrá hacer es difundirla en Facebook u otra red social porque dejaría de estar en esos fines particulares. Nos meteríamos en un lío casi con seguridad.

- **¿Cuál es la edad para que mis hijos puedan dar su consentimiento?**

¿Recordáis hace un ratito cuando os explicaba lo que era un Reglamento Europeo? ¿Cómo se especifica el objetivo y los pasos que había que dar para llegar al mismo? Pero también os decía que, aunque no muchos, quedaban algunos pequeños márgenes para que uno pudiera decidir. En nuestro ejemplo, Raquel, si recordáis, llenaba parte de mi agenda para hacer deporte y dieta. Pero no ocupaba las 24 horas de mi día. Así que en el resto del tiempo yo podía hacer lo que quisiera, siempre que no fuera en contra del objetivo final, que era adelgazar (en nuestro ejemplo).

La edad es una de esas cuestiones en que la normativa ha dejado un margen. Y podemos encontrar pequeñas diferencias en cada uno

de los países. Para prestar consentimiento en Europa para la cesión de imagen (y muchas otras cosas), el margen es de los 13 a los 16 años. Y cada país establecerá la edad, siempre dentro de ese margen, para que sus menores presten consentimiento sin la asistencia de sus padres. En España son 14 años.

- **¿Qué consecuencias puede tener subir una imagen a las redes o webs sin el consentimiento de ambos padres? ¿Puedo pedir que las retiren?**

En nuestro ejemplo real, Rocío, (la exmujer de Miguel Ángel y madre de Alma) se dirigió al centro de escalada tras ver la fotografía de su hija en Facebook y en la web del centro. Le preguntó al centro por correo electrónico que le justificaran el momento en que ella había dado consentimiento para que se publicara la foto de su hija.

Tras recibir este correo electrónico, el centro de escalada responde en menos de 24 horas. Lo hace con el documento firmado por el padre, además indica que han procedido a borrar las fotografías de su hija de Facebook y también de su página web. Recuerda, en 24 horas.

Tras recibir la respuesta del centro, Rocío les vuelve a preguntar lo mismo. Agradece que se hayan eliminado, pero solicita el documento donde ella prestó el consentimiento. Recuerda que debieron firmar ambos padres, como ya hemos aprendido.

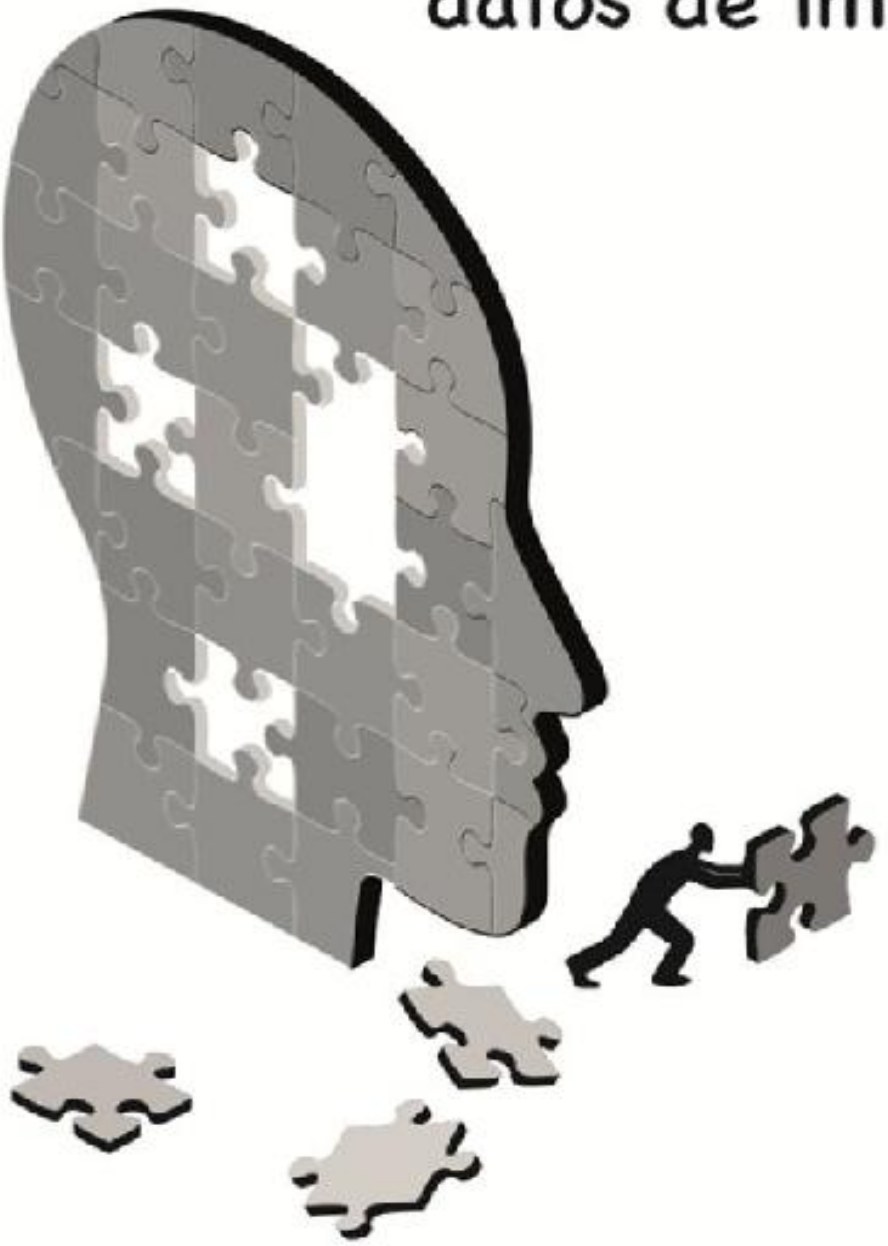
El centro de escalada no tenía ese documento firmado por ella, ni siquiera sabía que debían firmar ambos. Además, el documento no reúne los requisitos que hemos aprendido. Esto conllevó una denuncia y una sanción de 8.000 euros para el centro. ¡Uf!

Ya sé lo que piensas, que el motivo real era un mal rollo entre los padres divorciados. Y que esta "pelea" cogió al centro en mitad. Estoy de acuerdo, pero eso es lo que ocurre en la mayoría de las ocasiones y eso no exime al centro de hacer las cosas bien.

Pero, ¿qué habría ocurrido si el centro no hubiera retirado las

fotografías? ¿Qué podría hacer la madre en ese caso? Para saberlo tendrás que seguir leyendo porque en el siguiente capítulo te lo cuento todo. ¿Me acompañas?

Derecho al olvido: cómo eliminar datos de internet



3.- DERECHO AL OLVIDO: CÓMO ELIMINAR DATOS DE INTERNET

Iván enséñame a desaparecer de Internet.

Si has puesto en práctica todo lo aprendido en los dos primeros capítulos, estoy seguro de que habrás encontrado datos que quieres eliminar. Tanto tuyos como de tu familia, ya sean en texto o en imágenes, independientemente de que en su momento dieras consentimiento o no. Incluso aunque se trate de una obligación legal.

Para comenzar, siento decirte que no tengo una varita mágica con la que pueda tocar internet y eliminar publicaciones. Ojalá. El derecho al olvido, es eso, un derecho. Como tal, tiene sus requisitos y procedimiento para llevarlo a cabo. Y ya sabes porque lo hemos comentado, que no existe un súper derecho que gane siempre, y este tampoco es la excepción.

En este capítulo quiero enseñaros el paso a paso, así como los requisitos para poder desaparecer de internet. Te prometo que va a ser muy útil, porque la huella digital puede hacerte mucho daño. El pasado puede condicionar tu futuro.

¿Derecho al olvido?

En primer lugar, te diré que este es un derecho que tienen los ciudadanos que residen en Europa y que ha sido creado con la normativa que hemos visto (Reglamento Europeo de Protección de Datos). Pero que seguramente en tu país también exista algo parecido.

Antes de que sigas Iván. ¿De verdad era necesario este derecho?

Buena pregunta, necesario no, yo diría que imprescindible. ¿Preparado para un nuevo ejemplo? Pues vamos allá. Nos vamos a imaginar que eres electricista y has tenido un error importante que hace que te despidan. La verdad es que no era un error pequeño, la habías liado bien. Jo, con lo mal que están las cosas para buscar un nuevo trabajo. Por cierto, el lugar en el que trabajabas es pequeño, por ejemplo, el pueblo en el que me crié: Villanueva del Rosario, también en Málaga (España). Por lo que todo el mundo se ha enterado de que te han despedido y el motivo, así son los pueblos. Así que decides comenzar de cero. Te mudas a otra localidad mucho más grande, digamos que Marbella, donde nadie te conoce. Pero al poco tiempo, otra vez te ocurre lo mismo, mira que es mala suerte. Ahora la cosa es más complicada, porque este error es aún más importante, vaya tela. Ahora decides trasladarte a otra provincia, digamos que te vas a vivir a Madrid. Pero allí ocurre lo mismo. Ahora decides cambiarte de país, después de continente, etc…

En fin, ya vas entendiendo por dónde voy.

¿Cuál es la conclusión?

La conclusión es sencilla, ser electricista no es lo mío.

No, jeje. La conclusión que quiero que extraigas: es que la vida offline permite segundas oportunidades, aunque eso implique cambiar de localidad, provincia, país o continente. Siempre podrás comenzar desde cero.

Esto es una de las cosas más maravillosas de la vida. Tener una segunda oportunidad, poder comenzar de cero, sin la mochila de tu pasado condicionando tu futuro. Ir a otro lugar donde seas lo que quieras ser. Déjame contarte una cosa que quizás no sepas, pero en España hasta los antecedentes penales de una persona se eliminan pasados un tiempo. No quedaría rastro del delito que cometió en su pasado.

Pero si tu error no es offline, sino online. ¿Dónde te vas a

mudar?

No existe otro internet. Eso es el derecho al olvido. Es una segunda oportunidad en el mundo online. Algo que ya existe en el mundo offline. De nuevo, que tu pasado no condicione tu presente.

No reconocer este derecho sería algo así como argumentar que no existe la cadena perpetua en el mundo offline, pero que sí es legal en el mundo online.

Sigamos entonces, en este capítulo vamos a centrarnos en eliminar aquello que hemos encontrado. Lo vamos a hacer:

- **En el lugar de origen donde lo hemos encontrado**.
- Cuando esto no sea posible, lo haremos a través de **Google.**
- Y si ambos sistemas no funcionan. Lo haremos por la vía de la **Agencia Española de Protección de Datos** o el órgano equivalente que exista en tu país.
- Por último, hablaremos de **un sistema ultra rápido para quitar contenidos violentos o sexuales que afecten a menores en las redes**.

Ya sé que estás expectante para que te enseñe a hacerlo. Pero antes de entrar a explicar cómo se eliminan (que me encanta dejarte un poco con la intriga, jeje, cómo he disfrutado escribiendo este libro), déjame que te ponga tres de los ejemplos más habituales que nos llegan al despacho y donde el derecho al olvido puede ayudarte:

A. Ayuntamientos, Diputaciones, Comunidades Autónomas y Boletines Oficiales

Este punto es para cualquier notificación pública, que en su momento podía tener sentido y que hoy día ya no lo tiene. ¿Recordáis el ejemplo que pudimos ver en capítulos anteriores, sobre el albañil que pudo sacarse el carnet para conducir camiones, pero que nadie lo contrataba por una multa de alcoholemia que aparecía en un boletín? Es este supuesto.

Publicaciones de subvenciones, multas, oposiciones, cursos, adjudicación de viviendas de protección oficial, ayudas, becas, notas y un largo etc… son también notificaciones habituales.

Recuerdo un caso que fue muy sonado.

Hace unos años, Pedro estaba terminando sus estudios en la universidad para ser profesor de primaria. Tuvo que estudiar por temas de notas de corte en una provincia diferente a la suya, eso hizo que como es habitual compartiera piso con otros estudiantes. El año fue muy duro, Pedro se esforzó mucho para mantener la beca que le habían dado y lo consiguió, era además su último año. Por lo que en la fiesta de final de curso, que era también la despedida de la vida de estudiante, y la despedida de sus compañeros, Pedro lo dio todo. La cosa se volvió una locura, ¿recuerdas esas películas de desenfreno estudiantil? Pues fue así.

Pedro acabó con un par de copas de más, digo un par por decir algo, se bebió hasta las fuentes de la ciudad. Al final todo lo que entra tiene que salir, términó orinando en la vía pública, pero no en cualquier sitio, sino en uno de los monumentos más reconocidos de la ciudad. Tuvo la mala suerte que en esos momentos pasaba una patrulla de la policía local, por lo que aquello le costó una multa. En realidad no le importaba mucho, sería una anécdota para contar a los nietos, estaba feliz, en muchos sentidos. Lo que no podía ni imaginar es lo que venía a continuación.

Aquella denuncia no pudo ser notificada porque se mandó a su antiguo piso de estudiantes donde seguía empadronado, y después de un periplo de notificaciones acabó apareciendo en internet, en un Boletín Oficial. Pedro no sabía nada de esto.

Hasta que años después, algunos de sus alumnos la encontraron. Os podéis imaginar lo que ocurrió a continuación, Pedro ya era profesor, y su pasado le hizo ganarse un apodo que perdura hasta la actualidad: “Pedro el Meón”.

Tu pasado condiciona tu futuro. Derecho a una segunda

oportunidad. Se ve claro.

B. Periódicos, Blogs y otros medios de comunicación.

Habría que tener en cuenta y diferenciar lo que es un medio de comunicación de lo que no lo es. A veces se hace muy complicado.

Cualquier persona puede crear un blog y llamarlo: "El Noticiero de Málaga". Pero eso no significa que sea un medio de comunicación. Dejando este debate de lado, no es el momento ni el lugar. Solo te diré que tiene importancia para el ejercicio del derecho al olvido, puesto que un periodista puede decir cosas que no podría decir una persona de pie.

Dicho lo anterior, en los periódicos y medios de comunicación, es típico que exista una noticia que sea sexy. Pero que esa noticia nunca encuentre su final. Me explico. Imaginaros el siguiente caso, me están investigando por presunto blanqueo de capitales (Dios no quiera), y tenemos esa noticia en varios periódicos.

El abogado Iván González (friki y empollón) está siendo investigado en una trama de blanqueo de capitales, con oficina en Marbella y en diferentes localidades, se cree que es el cabecilla de una red que…. lógico de un amante de las criptomonedas… dicen que escribió un libro para ayudar a los padres a proteger a sus hijos en internet como tapadera…

Vaya historia. Eso es noticia, sobre todo en mi zona de influencia.

Pero, ¿sabes qué?, pasado un tiempo resulta que la investigación acaba.

¿Quieres saber la conclusión?

Nada de lo que se decía era cierto. Hubo una confusión con uno de mis "tocayos", que ya descubrimos en capítulos anteriores. Un pequeño error dicen.

Pensáis que se publicara una noticia que diga: "¿Recuerdan lo que publicamos hace unos meses sobre el abogado Iván González (friki y empollón)? Pues resulta que al final, tras la investigación, ha

resultado ser inocente. Se trató de un error con otra persona que tiene el mismo nombre.

Pues ya os contesto yo. Esta noticia nunca la encontrarás, porque no acaba de forma sexy. Eso no vende. Por lo que cualquier persona que ponga mi nombre en Google, seguiría teniendo una primera impresión mía pésima, aun sin conocerme y eso me hará perder clientes, sin ninguna duda. O ganar un tipo de clientes que no quiero, jeje.

Tu pasado condiciona tu futuro. Derecho a una segunda oportunidad. Se ve claro.

C. Redes Sociales.

Las reinas del daño. Las emperatrices de la viralidad. Donde el daño a nuestros hijos puede ser mayor. Aquí no tendría libro para poner ejemplos: vídeos y fotografías de niños amenazados, obligados a hacer cosas que no quieren, ridiculizados, vídeos violentos, de contenido sexual, etc…

Un verdadero problema en un medio que puede ser manipulado a nuestro antojo, como veremos en otro de los capítulos. Un medio al que nuestros hijos dan carta de veracidad. He hablado con menores que me han dicho sin ningún rubor que se creen lo que les dicen sus padres, si primero lo chequean por redes sociales y coincide.

Este es el lugar en el que más tenemos que actuar para eliminar contenido, tanto el subido por nuestros propios hijos como el subido por terceros. Hoy en día es habitual que muchas empresas antes de contratarte, hagan una revisión de tus redes sociales para ver qué tipo de persona eres. Chequearán si lo que estás contestando en la entrevista de trabajo coincide con el tipo de vida que publicitas en las redes. Esto es en algunos casos ilegal y en otros poco éticos, pero nunca lo sabrás a ciencia cierta. Tan solo te dirán el típico: ya te llamaremos…

Tras enumerar los tres casos más habituales que se dan para ejercer el derecho al olvido, estamos listos para explicar cómo eliminarlos.

Pero un segundo. Ya sé que estás expectante para que te diga cómo eliminar el contenido que ya tienes localizado. Pero poco te ayudará si no te cuento algunos criterios que se tienen en cuenta para la eliminación. Al menos enumerarlos:

- **¿Se trata de una persona pública o privada?** Ya intuyes que es más fácil eliminar cosas de una persona privada que de una pública. En muchas ocasiones, a un empresario en su actividad lo consideran persona con proyección pública.
- **¿Se trata de un contenido que sea de interés público?** Esto daría también para explicar muchas cosas. Pero en esencia, es que la publicación todavía sigue teniendo interés en que sea conocida por las personas.
- **¿Se trata de contenido veraz?** No significa que sea verdad, pero sí que esté contrastado. Se penalizan los rumores y las noticias falsas.
- **Que no hayas prestado tu consentimiento.**
- **¿Ha pasado mucho tiempo desde su publicación?** Cuanto más tiempo haya pasado menos relevancia tendrá, por tanto será un contenido que dejará de tener interés público y más fácil será eliminarlo o desindexar.

Ahora sí, vamos a explicar cómo borrar contenido. Recuerda de nuevo que esto se aplica si resides en Europa, pero que en tu país existe algo parecido o estará en vías de existir, puesto que es un derecho imprescindible en este mundo digital en el que nos movemos. Comencemos por analizar cómo "eliminar" tus datos de la propia web donde lo encontramos.

3.1.- DE LA PROPIA WEB DONDE LO ENCONTRAMOS

Esto es lo más habitual. Tras poner en práctica lo aprendido en los capítulos 1 y 2, ya tendrás un listado de cosas que quieres limpiar de internet. Así que comencemos.

Debes ir a la web donde aparecen esos datos tuyos que pueden estar allí sin permiso o pueden ser datos tuyos con permiso, pero son antiguos y otros están desactualizados. También pueden ser páginas públicas, que estuvieran obligados en su día a notificar algo. Pero esta notificación ya surtió efecto y por tanto ya no tiene sentido mantenerlas.

Haremos lo siguiente:

a. Dentro de la web buscarás y debes encontrar (digo debes, porque a pesar de que es algo obligatorio puede ser que no exista) una pestaña denominada: **Aviso Legal** (en las redes sociales directamente tendrás un botón para denunciar la publicación). Ya sé que te costará encontrarla. Estará en la parte inferior de la web. Casi escondida, es posible que tenga un tamaño de letra inferior. Pero estará. Es obligatorio. Eso espero.

b. Una vez localizada, entraremos en la misma. Entre otras cosas, en esta parte aparecerá: la persona, empresa o institución responsable de la web. Su dirección, correo electrónico, Cif o Nif. Si es una empresa, incluso su inscripción en los registros correspondientes. Si es un profesional, su número de colegiado (aunque casi nadie lo pone). Las webs no pueden ser anónimas. El Aviso Legal es contestar a la pregunta: ¿Quién eres?

c. Localizado el responsable y su correo electrónico, copiaremos el enlace donde aparece la información que queremos eliminar. Le haremos también una captura para tener constancia de lo que estaba publicado (en otro momento, seguramente en el siguiente

libro, hablemos un rato de los testigos digitales). Le remitiremos un correo electrónico con copia de nuestra identificación y le solicitaremos que la elimine. Si el correo electrónico no funciona, que debería, prueba con una carta certificada.

d. Esta petición no tiene que tener un contenido legal ni un texto exacto. Pero si quieres ponerte serio, puedes utilizar este formulario que nos facilita la Agencia Española de Protección de Datos:

EJERCICIO DEL DERECHO DE SUPRESIÓN DATOS DEL RESPONSABLE DEL TRATAMIENTO (A QUIEN LE ESTÁS PIDIENDO QUE LO ELIMINE)

Nombre / razón social: .....Dirección de la Oficina / Servicio ante el que se ejercita el derecho de supresión: C/Plaza ..... nº ..... C.Postal ..... Localidad ....., con correo electrónico ……..... (TODO ESTO LO ENCONTRARÁS EN EL AVISO LEGAL, PERO SI TE FALTA ALGÚN DATO NO TE PREOCUPES, COMPLETA LO QUE APAREZCA).

DATOS DEL AFECTADO. (TUS DATOS Y SI ES EN NOMBRE DE TU HIJO INDÍCALO TAMBIÉN)

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... (AQUÍ PONDREMOS EN NOMBRE PROPIO O EN REPRESENTACIÓN DE MI HIJO ……..) con D.N.I....., con correo electrónico…….....por medio del presente escrito ejerce el derecho de supresión, de conformidad con lo previsto en el artículo 17 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA Que se proceda a acordar la supresión de sus datos personales en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me

notifique de forma escrita el resultado de la supresión practicada. Que en caso de que se acuerde que no procede practicar total o parcialmente la supresión solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda. Que en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta supresión.

En .....a.....de.....de 20.....

Firmado

Como te decía, no es necesario un formulario en concreto, puedes expresarlo con tus palabras. Pero si utilizas este de la Agencia Española, tanto ellos como su abogado sabrán que vas en serio. Si has sabido encontrar este formulario, también sabrías encontrar el de denuncia. Están cerca uno del otro. El que avisa no es traidor.

e. El plazo que tienen para contestarte como máximo es un mes. Y no te preocupes, te contestarán bastante antes de ese plazo, es lo habitual. Te pueden contestar:

- Que eliminen lo que estás solicitando.
- Que se nieguen a ello o no te contesten. Si ocurre esto último, te explico qué hacer en el tercer punto de este capítulo. Pero se están metiendo en un problema.

Recuerda que acudir a la web de origen donde están tus datos, es el sistema más eficaz que conozco. Está por encima del 80% de probabilidades de que acepten tu petición. Si estás en los supuestos que hemos comentado, claro. Si además utilizas el formulario que te he facilitado todavía más. Pero no son pocas las ocasiones donde la web no está activa o está en el otro extremo del mundo y no tiene Aviso Legal.

Para estas ocasiones iremos a quien nos la muestra: Google.

3.2.- UTILIZANDO GOOGLE

No creo que Google sea uno de los mayores fanáticos del derecho al olvido. Cualquier abogado que nos dediquemos a estos temas, creo que pensará algo parecido. Mi impresión es que Google ha pasado por varias etapas en su vida respecto a este derecho, antes de tener que empezar a asumirlo como algo del día a día.

La primera etapa era una que siempre me imaginé así (ya sabes que tengo mucha imaginación). Tras encontrar unos datos en internet que no sabías que estaban, como por ejemplo tu nombre y apellidos y tras no poder comunicarte con la web de origen, pasabas a intentar hablar con Google. En tu caso ya que vives en Madrid intentas realizar una visita presencial. Localizabas la oficina y subías en el ascensor, pensando si estarás en el lugar adecuado o no. Hasta que se abrieron las puertas del ascensor y ahí estaba su logo, inconfundible. Tocabas a la puerta, educación ante todo. Alguien te habría. Y tú le decías:

—Perdone busco al señor Google, ¿me pueden ayudar?

—Claro que sí, pase usted. Te contestaban muy educadamente.

—Verá usted, vengo a solicitar que no indexen esta información mía, porque no he dado permiso, además bla, bla, bla…

—Disculpe caballero, se confunde, aquí no es.

Tú volvías a mirar el logo y preguntabas:

—¿Pero no son ustedes Google?

—Verá usted, sí y no. Creo que usted quiere hablar con Google Inc, y nosotros somos Google Spain. Le podemos ayudar con su publicidad, pero no con más cosas, para eso tendrá usted que preguntar en California, que por cierto hace buen tiempo en esta época (me encanta imaginarlo así).

¿A qué os parece deprimente? Pues esta era la primera etapa.

Segunda etapa, que siempre me imaginé así. De nuevo encontramos unos datos en internet que no has subido tú. Por supuesto, no puedes dirigirte a la web de origen, y de nuevo decides pasarte por la oficina de Google. Ha pasado algún tiempo desde la visita anterior, ahora ya no te contestan que no es ese el lugar adecuado. Algo hemos ganado por el camino. Resulta que allí sí era. Ya me parecía a mí que el logo se parecía, jeje. Aunque igualmente te dicen que no pueden ayudarte. La excusa ahora era más elaborada, te dicen que Google es un buscador (vaya novedad) y que por tanto es un espejo de la realidad. Solo muestra lo que existe, pero no intervienen, no priorizan y no ayudan ni penalizan. Por lo que están mostrando lo que está. Si no estoy conforme que lo discuta con el lugar de origen donde están mis datos. En fin, no entraremos a discutir que si esto fuera cierto se acabó el marketing digital, porque al fin y al cabo esta postura ya no existe.

Tercera etapa y actual. A raíz de diferentes sentencias europeas y el cambio de la normativa de protección de datos que hemos mencionado (Reglamento Europeo de Protección de Datos), a Google no le ha quedado otra que admitir este derecho, incorporando un formulario para ejercerlo. ¡Cómo ha evolucionado todo en poco tiempo!

Este formulario lo encontrarás de forma sencilla, solo tienes que escribir en el propio Google: formulario derecho al olvido Google.

Completarlo no tiene ninguna complicación. Pero déjame que te dé algunas indicaciones que creo que son importantes:

a. El propio buscador te indica que:

"Cuando Google recibe una solicitud, busca el equilibrio entre el derecho a la privacidad de la persona que la ha enviado y el derecho del público general a tener acceso a esa información, así como el derecho de otros usuarios a distribuirla. Por ejemplo, puede que Google se niegue a retirar determinada información sobre estafas financieras, negligencia profesional, condenas penales o comportamientos impropios de funcionarios públicos".

b. Debes residir en uno de los países que reconocen este Derecho. Google mantiene un listado de los mismos.

c. Si lo haces en nombre de tus hijos. Es posible que puedan pedirte documentación que lo acredite, adelántate a ellos y adjúntala.

d. No les sienta bien que repitas solicitudes ya remitidas. Pero te digo un secreto, a la misma solicitud pueden contestar que no van a desindexar, a los días la vuelves a remitir y te contestan que sí lo harán.

e. Tendrás que explicar el motivo por el que solicitas que se desindexe. Tendrás que utilizar uno o varios de los puntos que te indicaba al inicio de este capítulo: paso del tiempo, no veraz, persona privada, sin consentimiento, etc…

Tras esto, Google no tardará mucho en contestarte. Que conteste en los términos que tú esperas y no utilizando respuestas automáticas ya será otra cosa. La realidad es que Google es el buscador mayoritario en esta parte del mundo. Pero recuerda que es una empresa privada, que tienen unos intereses y una forma digamos de ver la vida (cada empresa los tiene), que no tiene por qué ser la alineada con tus valores, pero sí tiene que estar en consonancia con la ley. Por eso, no siempre estaremos de acuerdo con sus decisiones, pero sí creemos que la ley nos ampara, para eso está el siguiente apartado, no te preocupes.

Que sea una empresa privada (y no cualquier empresa) la que decida lo que es libertad de expresión, libertad de información y donde está el límite con la privacidad, es algo que a mí todavía me chirría.

Pero Iván tengo una pregunta: ¿Por qué iba a acudir a Google? ¿No me habías dicho que acudir a la fuente tenía más de un 80% de probabilidades de que se atendiera mi solicitud?

Tienes razón. Pero como hemos dicho, acudir a Google a veces es imprescindible. Sobre todo por dos motivos. El primero, es que el

mundo es muy grande.

Podemos encontrar información que nos afecte a nosotros (que indirectamente también acaba afectando a nuestros hijos), o de nuestros hijos en cualquier página web del mundo. Podría ser en la India, China, Australia o Estados Unidos. Y no en todos los lugares de este mundo, será obligatorio que aparezca la pestaña del Aviso Legal, y aun siéndolo habrá muchas webs que no la indiquen buscando un falso anonimato.

En segundo lugar, en este mundo de internet también encontramos a personas malas, que buscan hacer el máximo daño posible. Para eso han podido crear blogs o páginas webs, con el único objetivo de perjudicarnos a nosotros o a nuestros hijos. Crear un blog puede ser cosa de cinco minutos y se puede hacer anónimamente. Estos, como te puedes imaginar, tampoco tendrán el contenido legal necesario, ni identificarán a quien los creó.

Además existen webs o blogs inactivos, por lo tanto dirigirse a los mismos tampoco es posible.

Para estos casos y para más (nada impide que si nos dirigimos a la web de origen sin éxito, también podríamos probar esta otra vía) el camino es Google.

3.3.- DESDE EL ORGANISMO DE PROTECCIÓN DE DATOS

Y llegamos a la tercera opción, no la queremos pero a veces será inevitable. En esta opción es necesario acudir a un organismo público mediante una reclamación para que intervenga. Es algo así como en una pelea entre hermanos, tener que ir a quejarse a mamá para que ponga paz. Sabemos que no es lo ideal, pero es la única solución posible.

Recuerda cómo hemos tenido que llegar a esto. Bien porque la web de origen donde están nuestros datos no nos ha contestado en plazo (recordar que tenían un mes) o porque nos ha contestado negando nuestra petición. Y lo mismo, si lo hemos realizado a través de Google. Decirte como en otras ocasiones, que este es un derecho para residentes en Europa, pero que seguramente en tu país existe o existirá próximamente. Ya sé que te lo he dicho al menos dos veces más, pero es importante.

Cuando se crean estos derechos, se crean también los órganos públicos necesarios para garantizar que se cumplan. En el caso de España: es la **Agencia Española de Protección de Datos**. Que es el ejemplo práctico que pondré por cercanía.

Pero si tú resides en cualquier país de Europa, podrás encontrar el contacto de tu organismo de control en la web del Comité Europeo de Protección de Datos: https://edpb.europa.eu/. Y dentro de la web, en las pestañas superiores encontramos una denominada: **<Acerca del EDPB>.** En el desplegable una vez que hagamos "clic", tendremos la opción de ver todos los organismos públicos, sus nombres, datos de contacto, etc…

Vamos con un ejemplo real. Antonio no ha tenido una infancia sencilla. La mayoría de los niños de su edad no tenían preocupaciones que atender, pero Antonio tenía que cuidar de su hermana María José. Su padre era camionero (esta profesión sale

varias veces en el libro, ha sido la profesión de mi padre y así le rindo un homenaje) y viajaba mucho. Y su madre se pasaba el día trabajando limpiando casas, y solía llegar a casa muy tarde. Antonio tenía que estar pendiente siempre de su hermana, de sus estudios, llevarla y recogerla del colegio, actividades extraescolares, la comida, la mochila, etc… Esto no le dejaba mucho tiempo para jugar con los niños de su edad. De todas formas, Antonio siempre se sintió diferente, tampoco ayudaba mucho que fuera gordito y que no tuviera los mismos gustos que el resto de los niños de clase.

Han pasado años, Antonio en su adolescencia adelgazó mucho. Llegó al instituto y pudo comenzar desde cero (su padre ya se jubiló y su madre ya no trabaja fuera), es hasta popular, ¡quien se lo iba a decir!

Pero todavía le hace daño pensar en aquella época, las fotografías que quedan en internet no ayudan mucho a pasar página. Tras realizar búsquedas como le enseñó un abogado friki, ha podido eliminar la mayoría. Salvo un par de sitios que se resisten.

El primero, un blog que se creó para una actividad del colegio, ha intentado recordar qué compañero fue, pero hace muchos años. La actividad consistía en promocionar la localidad donde estaba su colegio. Para eso, Antonio se tuvo que disfrazar, ser como una especie de guía turístico. Cada compañero realizaba un papel diferente. En la descripción del blog, también se ponían los nombres y apellidos de los integrantes de la actividad. Este blog está ya inactivo.

Y el segundo, la televisión local del municipio. Ha recopilado fotografías por años, Antonio aparece de forma individual en muchas de ellas, con un pie de firma con su nombre y apellidos. En la mayoría no sale favorecido. Y las han subido a la web de la televisión.

Tras acudir en el caso del blog a Google (recordar que estaba inactivo) y en el caso de la televisión local a la misma, no ha logrado que se eliminen. Google ha contestado que no ve motivos para

desindexar. Antonio cree que es una respuesta automática, pero no ha logrado hablar con una persona real. Y en el caso de la televisión local, directamente ha sido ignorado, a pesar de que ha realizado la petición al menos dos veces. Antonio está realizando todos estos trámites directamente porque ya tiene diecisiete años.

Tras pensarlo varios días, decide acudir a la Agencia Española de Protección de Datos. Entra en su web: www.aepd.es. Y sigue los siguientes pasos:

- Busca la pestaña de **<Sede Electrónica>.**
- Indica que es un **ciudadano.**
- Acude a la pestaña de **<Reclamaciones Ordinarias>.**
- Encuentra un apartado denominado: **<Publicación de Datos en Internet>**. Tras marcar este apartado, tenía que especificar dónde estaban los datos. Por lo que decidió realizar dos reclamaciones: una frente a Google y otra frente a la televisión local por separado.
- Por último, le preguntaron si quería **realizarlo en papel o con firma digital**. Antonio escogió el papel. Completó los datos que le solicitaban y la dejó presentada.

Tras unos meses, tuvo conocimiento de que se habría un procedimiento contra Google y contra la televisión local. Finalmente sus datos fueron desindexados de Google y eliminados de la web de la televisión local.

Nos queda el último punto, si estás cansado o cansada, déjalo. Es demasiado importante para que lo leas si ya estás bajo de energía, te necesito a tope. Lo que te voy a contar, puede literalmente salvar la vida de tus hijos o de otros menores.

3.4.- CANAL PRIORITARIO DE RETIRADA DE CONTENIDOS DE LAS REDES SOCIALES

"Se suicidó porque su novio la grabó en un momento íntimo y se lo pasó a Rodrigo. Rodrigo se lo reenvió a sus amigos y lo subieron a un canal con más de 13 millones de suscriptores donde todos vieron el vídeo en el que aparecía".

Siento mucho decirte que esta opción, lo más probable es que no exista en tu país. En España, la Agencia Española de Protección de Datos ha sido pionera en ponerla en marcha bajo el eslogan: "No es por el vídeo o la foto, es por todo lo que hay detrás". Este es un canal para fotografías o vídeos de contenido sexual o que muestren actos de agresión. Puede utilizarlo la víctima a la que se le está provocando un daño (y estos daños son de los que dejan cicatriz para toda la vida), si es menor de 14 años lo harán sus padres, pero también lo puede utilizar cualquier persona que localice estos contenidos en internet. Limpiemos la red, es responsabilidad de todos.

¿Para qué casos está previsto?

En el caso de menores, lo más habitual es:

- Casos de acoso o agresión (en el entorno escolar o fuera)
- Vídeos de contenido sexual (en el entorno escolar o fuera)

¿Para qué supuestos no es adecuado?

- Si la difusión se realiza por mensajería instantánea como Whatsapp o Telegram o por correo electrónico, el canal no sería el medio adecuado.
- Si no son los casos excepcionalmente graves que hemos mencionado, tendrás que seguir las vías habituales (y más

lentas que ya hemos comentado en los puntos anteriores).

- Si no eres ciudadano español o no resides en España.

¿Dónde encuentro este canal?

Puedes hacerlo poniendo su nombre en Google, o siguiendo estos pasos:

- Accede a la web: www.aepd.es.
- Busca la pestaña de <Sede Electrónica>.
- Indica que eres un ciudadano.
- Pestaña de <Reclamaciones Ordinarias>.
- <Canal prioritario de retirada de contenido sensible>.

¿Cómo se actuará desde que pongas la reclamación?

Desde que se interponga la reclamación se pondrán en contacto con la red social o el lugar donde se esté difundiendo el contenido de forma inmediata. Además, si se considera que es un delito también se pondrá en conocimiento del Ministerio Fiscal. Recuerda que quien difunde estos contenidos puede estar cometiendo un delito, y aunque no fuera así, también podría tener otras responsabilidades importantes.

Esta es una vía excepcional para casos realmente muy graves. La Agencia Española de Protección de Datos pone estos tres ejemplos para que nos hagamos una idea de cuándo acudir a este canal:

> **Fue condenado a cinco años de cárcel porque grabó a Sara sin permiso** mientras mantenían relaciones sexuales, lo pasó por el grupo de amigos, que le animaron a subirlo a internet y difundió el video.
>
> **Fue acosado en el instituto porque Román le sacó una foto mientras le pegaban en el patio**, se lo pasó a Marina, ella la subió a stories y su foto se hizo viral.

Se suicidó porque su novio la grabó en un momento íntimo y se lo pasó a Rodrigo, Rodrigo se lo reenvió a sus amigos y lo subieron a un canal con más de 13 millones de suscriptores donde todos vieron el vídeo en el que aparecía.

Mientras escribo esto se me han vuelto a saltar las lágrimas. Mi trabajo no siempre es fácil. Ojalá nunca tengas que hacer uso de esta información pero, por otro lado, estoy feliz de difundirla. Desde aquí le doy las gracias a la Agencia Española de Protección de Datos.

¿sabes si alguna vez
te han **hackeado**?

4.- ¿SABES SI ALGUNA VEZ TE HAN HACKEADO?

4.1.- WEB CENTRAL DE HACKEOS

La mitad de las personas que estáis leyendo este libro habéis sido hackeadas. Pero solo una pequeña parte lo sabéis. Siento ser tan directo.

Pero Iván, entonces tengo unas preguntas:

- ¿Cómo puedo saber si alguna vez me han hackeado?
- ¿En qué plataforma ocurrió?
- ¿Qué datos míos quedaron expuestos?
- ¿Qué tengo que hacer a continuación?

Son buenas preguntas. Y son todas las que recibo cuando explico esta parte en mis conferencias.

Saber si alguna vez te han hackeado, es como decirle a alguien si ha estado enfermo. Si los síntomas han sido muy graves lo sabes. Pero si has tenido pequeños síntomas, quizás ni lo hayas notado y lo hayas achacado a otra cosa, por ejemplo, has podido pensar que ese cansancio es por la semana tan dura que has tenido. Con los hackeos pasa igual, salvo síntomas muy graves, es posible que ni te hayas dado cuenta. Y peor aún, puede ser que los síntomas todavía no se han presentado, aunque ya has contraído la enfermedad. En este capítulo vamos a realizarte un chequeo médico para que puedas estar seguro que estás más sano que una pera.

Hace años, saber si alguna de las plataformas que utilizas había sido hackeada y si tus datos habían quedado comprometidos era complicado. En muchos casos era imposible. No existía un solo lugar

al que acudir, muchas compañías acababan confesando cuando ya no podían esconder la suciedad debajo de la alfombra.

En el año 2013 un experto en seguridad, Troy Hunt, decide comenzar un proyecto que pudiera ser la página web central de los hackeos. Un lugar centralizado para tener esta información. Este proyecto se denomina: Have I Been Pwned (https://haveibeenpwned.com/).

Este proyecto ha crecido y cuenta con la colaboración de cientos y cientos de hackers buenos (éticos o de guante blanco), que cuando detectan alguna brecha de seguridad lo comunican a esta web. Haciendo esto, las personas afectadas por el hackeo tanto de una plataforma, web o red social, pueden saberlo.

Es importante antes de que te pegues el susto de verte en esta web, que aparecer no significa que nadie haya entrado a tu correo electrónico (está bien aclararlo por la afirmación con la que comenzaba), pero sí que la plataforma y donde lo tenías alojado, ha sido comprometida.

Por ponerte un ejemplo. Imagínate que se ha hackeado Facebook o Adobe (y no hay que imaginarse mucho, porque ambas plataformas lo han sido en el pasado). En estos casos, alguien ha podido tener acceso al correo con el que creaste la cuenta, a tu contraseña, quizás a los datos que introdujiste cuando te diste de alta (nombre, apellidos, domicilio, fecha nacimiento, etc…) y a algunos datos más adicionales.

Bueno Iván, entonces no es tan grave.

Está bien saber qué plataformas de las que soy usuario se han visto afectadas, pero si no han podido acceder a mi correo electrónico, tampoco es tan importante que sepan: mi nombre, apellido, domicilio, fecha de nacimiento, contraseña de esa aplicación, etc… En fin, sobre esto volvemos en un ratito, pero ve mirándote en un espejo y dite a ti mismo: “Soy muy inocente, soy muy inocente”. Así vamos ganando tiempo.

Pero volvamos al inocente, digo a la persona que está tranquila porque piensa que esos datos no son tan importantes y que lo importante es que no pueden acceder a su cuenta de correo electrónico, banco u otras aplicaciones sensibles. Pues no deberías estar tranquilo si eres de las personas que utilizan la misma contraseña en muchos servicios.

Y ahora dirás que tú no lo haces, pero por estadística 7 de cada 10 que leen este libro sí que lo hacen. Los hackers lo saben y lo comprobarán. Por lo que si esa contraseña de Facebook o Adobe la utilizas para tu Gmail, tu banco, etc… tenemos un problema serio. Y si lo que se ha hackeado directamente es tu proveedor de correos electrónicos o tu banco, esto se pone divertido.

Esta web va a ser una web de referencia para nuestra seguridad y la de nuestros hijos. Su utilización es sencilla, cuando accedes a la web te aparece un campo de texto donde podrás poner los correos electrónicos y móviles de tu familia. Uno a uno. Y en todos ellos deberá aparecer el texto: "Good news - no pwnage found".

Pero como ya te adelantaba, en internet la seguridad absoluta no existe. Cuando miras a los ojos a un hacker y le preguntas: ¿Esto es seguro? Te responde sin pestañear que la seguridad es un estado de tu mente.

Por lo que, en algunas búsquedas encontrarás otro texto diferente y no tan bonito: ¡Oh, no, pwned!

Antes de que te dé un patatús, no quiero perder lectores, jeje. Respiramos, vamos una vez más a respirar. Debajo te dirá las veces en que tu correo ha sido expuesto:

Ejemplo Pwned on 1 breached site and found no pastes (subscribe to search sensitive breach).

Queremos saber:

- en qué fecha
- plataforma

- y qué datos nuestros se han visto afectados por esta brecha. Descenderemos un poco en la web

Os pongo un ejemplo real (como todos), uno de mis correos secundarios para darme de alta en plataformas gratuitas, fue expuesto en el hackeo de Canva. Canva es un programa de diseño muy utilizado y extendido (la verdad es que está genial). Esta es la información que me aparece:

Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames.

Os pongo la traducción:

Canva: En mayo de 2019, el sitio web de herramientas de diseño gráfico Canva sufrió una violación de datos que afectó a 137 millones de suscriptores. Los datos expuestos incluían direcciones de correo electrónico, nombres de usuario, nombres, ciudades de residencia y contraseñas almacenadas como hashes de ncrypt para los usuarios que no utilizan inicios de sesión sociales. Los datos fueron facilitados a HIBP por una fuente que pidió que se atribuyeran a "JimScott.Sec@protonmail.com".

Datos comprometidos: Direcciones de correo electrónico, Ubicaciones geográficas, Nombres, Contraseñas, Nombres de usuario

Útil, ¿verdad? Si la contraseña que utilizaba en Canva no era segura o la estaba utilizando en otras plataformas, en cuanto tuve conocimiento de esto la tuve que cambiar. Así que si es tu caso, te toca cambiar las contraseñas (una de las cosas más bonitas que uno puede hacer un domingo), pero antes de hacerlo por favor lee el

apartado siguiente. Es importante.

El estar entrando en esta web para comprobar si los móviles o correos electrónicos han quedado expuestos, es una tarea que como en el capítulo primero cuando os enseñaba a bucear en internet, podríais hacerlo durante un tiempo, pero en algún momento dejaréis de hacerlo.

Por eso lo que vamos a hacer es suscribirnos, para que sean ellos los que nos avisen si nuestros correos o móviles han sido expuestos. Lo puedes hacer bajo el botón **<Subscribe>** que aparece cuando haces una búsqueda o en la pestaña de la web que indica: **<Notify Me>.** Tras esto recibirás un correo electrónico que deberás confirmar, revisa también la bandeja de no deseados. De todas formas, una vez al trimestre yo lo realizaría manual también. La insistencia aquí da puntos.

Esta web puede ayudarte mucho. Si seguimos con nuestra analogía, evitarás que los síntomas de la enfermedad que ya habías contraído lleguen a desarrollarse. Coméntalo con las personas que conozcas, ya sabes que esta es una de las misiones de este libro, conseguir que muchas personas tengan acceso a esta información minoritaria. Juntos podemos.

JUERETO 4.- WEB CENTRAL DE HACKEOS

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Seguro que ya extrañabas un nuevo "Juereto". En esta ocasión vamos a enseñarle a nuestros hijos lo fácil que es haber sido víctima de un hackeo. Recuerda que por estadística la mitad de las personas aparecen aquí.

Estas son las reglas. **Participaremos de forma individual o por parejas**.

Cada uno pondrá cinco correos electrónicos, los que quiera. Pueden ser propios o de la familia (es lo ideal), de compañeros del

colegio, páginas webs conocidas, del club deportivo, famosos, etc… Tras esto comprobaremos cuántos de ellos se han visto expuestos a un hackeo en el pasado. **Cada correo expuesto es 1 punto. La puntuación máxima es 5 puntos.**

Ahora pondremos cinco números móviles, los que quieran. Y también los comprobaremos. **Cada móvil hackeado es 1 punto. La puntuación máxima es 5 puntos.**

El que más puntos tenga escogerá la próxima película que verá la familia.

Y ahora como siempre, te toca a ti explicarles cómo saber esto y lo importante que es. Cómo pueden ayudar a todas las personas que conozcan. Diles que ahora tienen un súper poder, saber si alguna vez alguien ha sido hackeado. Recuerda que tienes un cuaderno a tu disposición con más formularios, además de otros recursos adicionales del libro, como el libro de las contraseñas padres e hijos.

Comenta con ellos los resultados, les pica la curiosidad por estas cosas, aprovecha esa curiosidad.

Por ejemplo: sabrán que esa tienda online que muchos utilizan (Shein) tuvo una brecha de seguridad:

SHEIN

In June 2018, online fashion retailer SHEIN suffered a data breach. The company discovered the breach 2 months later in August then disclosed the incident another month after that. A total of 39 million unique email addresses were found in the breach alongside MD5 password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Breach date: 1 June 2018

Date added to HIBP: 17 July 2019

Compromised accounts: 39,086,762

Compromised data: Email addresses, Passwords

Concursante 1	
Concursante 2	
Concursante 3	
Concursante 4	

	CORREOS ELECTRÓNICOS	HACKEADO (SÍ/NO)
1		
2		
3		
4		
5		

	MÓVILES	HACKEADO (SÍ/NO)
1		
2		
3		
4		
5		

PUNTOS TOTALES (Máxima puntuación 10 puntos)	

4.2.- ¿CUANTO TIEMPO SE TARDA EN HACKEAR TU CONTRASEÑA?

¿Recuerdas alguna de las películas de Indiana Jones? Siempre buscando tesoros y resolviendo misterios. Vale, eres más joven que yo. Prueba con Tadeo Jones o Dora la Exploradora, jeje. La idea es la misma, tras muchas búsquedas yo también acabé encontrando el Santo Grial: una web en la que puedas introducir tu contraseña y en la que te confirmen el tiempo exacto que se tardaría hackearla (en días, horas, minutos o segundos).

¿A que mola? (¿Todavía se dice mola? Creo que sí).

La web en cuestión se llama: https://www.passwordmonster.com/.

Es una herramienta que pone a nuestra disposición, una empresa de seguridad inglesa llamada: My1 Login. Es una maravilla.

Comienza dándote un consejo, sencillo pero útil: no utilices palabras comunes o genéricas.

A esto le añadimos que tampoco utilices ningún dato personal tuyo, por ejemplo cumpleaños, nombres de tus hijos, lugar de vacaciones, película favorita, edad, nombre de tus mascotas, etc… No sé si eres consciente, pero existen algoritmos que pueden automatizar todo lo que alguna vez has puesto en redes sociales, con esto extraen millones de posibles contraseñas. Por lo que piensa lo activo que eres en redes sociales, y te tocará ser creativo con las contraseñas. Más activo igual a más creativo. Aunque sobre esto, hablaremos más en el apartado siguiente.

Su utilización es sencilla. Tan solo tienes que escribir tu contraseña y en la parte inferior aparecerá el tiempo que se tarda en hackear. Además de indicar si es muy débil, débil, media, fuerte o muy fuerte con frases tan motivadoras como: “Fantástico, usar esa contraseña te hace tan seguro como Fort Knox.”. Y otras no tanto: “Dios mío, usar esa contraseña es como dejar la puerta de tu casa abierta de

par en par”.

Me imagino que quieres saber cuál es mi recomendación en tiempo para tu contraseña. Para una contraseña normal y que no repitas en más sitios, mínimo 100 años. Para una contraseña en redes sociales, correo electrónico o servicios bancarios, no debería bajar de 1.000 años.

Venga ya, Iván tú flipas.

No, lo digo en serio. Hazme caso por favor.

La pregunta ahora es la de siempre: ¿Cómo puedo realizar una contraseña que sea así de buena?

Y lo más importante: que sea fácil de recordar. Para eso, tendrás que leer el siguiente apartado.

4.3.- CONTRASEÑAS SEGURAS Y FÁCILES DE MEMORIZAR

¡Cuántas veces a lo largo de mi vida profesional he encontrado contraseñas escritas en un post-it y pegado a la pantalla del ordenador! ¡O cuantas veces me han confesado los clientes que tener una contraseña segura es difícil de memorizar! Por eso tienen una que utilizan para todos los sitios del mundo mundial.

En este capítulo me toca desmontar mitos, enseñaros lo sencillo que es realizar una buena contraseña y lo fácil que es de recordar.

Pero antes de hablar de las buenas, déjame que te algunos consejos sobre las malas:

1.- Para empezar vamos a ver el listado de las peores contraseñas del mundo

Nordpass es un administrador de contraseñas que cada año publica uno de los listados más virales del mundo, el listado con las peores contraseñas del mundo: https://nordpass.com/es/most-common-passwords-list/.

Qué te parece que pongamos las diez peores:

1.- 123456

2.- 123456789

3.- 12345

4.- qwerty

5.- password

6.- 12345678

7.- 111111

8.- 123123

9.- 1234567890

10.- 1234567

¿Cuánto se tarda en hackear todas estas contraseñas?

Menos de un segundo. Ya puedo verte, tienes una media sonrisa en la cara. Estás pensando que cómo pueden existir personas que todavía tengan estas contraseñas. Pues la verdad es que no son miles sino millones los que todavía tienen alguna de las contraseñas de este listado. Y seguramente conoces a alguno.

2.- ¿Tu contraseña tiene algo que ver contigo? ¿Con algo que hayas puesto en redes sociales o en internet? ¿Con datos de tu familia?

Mala idea. Una contraseña no puede ser algo personal: por lo que el nombre de tus hijos, tu película favorita, fecha de nacimiento, etc… no es buena idea. Existen programas que automatizan todas estas cosas y pueden sacar millones de variables hasta dar con la correcta, como ya os decía.

3.- ¿Recuerdas la página web de hackeos que hemos visto hace un ratito?

Pues en esta web: https://haveibeenpwned.com/, podemos encontrar en sus pestañas superiores una con el nombre de**:** contraseñas. En esta pestaña podemos comprobar si la contraseña que hemos pensado o que ya utilizamos, ha sido hackeada en el pasado. De ser así, aunque sea una contraseña fuerte tal y como hemos visto en el apartado anterior, tendrás que desecharla y buscar otra.

Ya hemos hablado de las contraseñas malas.

Pero Iván, me has prometido enseñarme a realizar contraseñas seguras y fáciles de recordar.

Exacto. Esa es mi promesa.

Podríamos utilizar diferentes métodos (en uno de mis próximos libros sobre criptomonedas, tendré que hablar de esto con mucha más profundidad). Pero vamos con los dos más sencillos.

1.- Utilizar un acróstico

Ya sé que parece que me acabo de inventar una palabra, pero los acrósticos se han utilizado desde hace cientos de años. Consiste en coger algunas letras de diferentes palabras. La forma en la que lo vamos a realizar es sencilla, piensa en la letra de tu canción favorita. Localizarla por internet debe ser fácil.

Álvaro Soler tiene una canción con el nombre de mi hija: Sofía, cuyo primer párrafo dice:

"**S**ueñ**o c**uand**o e**r**a p**equeñ**o**".

De este inicio va a salir mi contraseña, para ello pondré la primera letra y última de cada palabra, sale una palabreja como esta:

Socoeapo.1

Como ves no significa nada. Pero además yo le añado un **. y el número 1** para recordar que era el primer párrafo porque de esta misma canción sacaré más contraseñas.

Vamos con el párrafo segundo:

"**S**i**n p**reocupació**n**, **en el c**orazó**n**".

Que en formato contraseña quedaría:

Snpnenelcn.2

Ahora no me digáis que no es sencillo y que en cualquier momento no podréis buscar la misma, estéis donde estéis.

Vale ya sé que alguien está pensando que sí que es fácil, que se puede localizar rápido también, que es segura (he utilizado la web que hemos aprendido y me da que son 857 mil millones de años), pero que fácil de recordar no tiene pinta. Vale te lo compro. Vamos con el segundo método.

2.- Este método lo llamo: regreso al pasado

Imagínate dónde has pasado tu infancia o esos veranos que siempre tendrás en la memoria, retrocede en el tiempo a esa época, disfrútalo. Ahora, encuentra una comida típica que te venga a la cabeza, seguro que puedes olerla y saborearla. También me serviría que recuerdes el nombre de la calle donde jugabas, el de una fiesta donde tan buenos momentos pasaste. Recuerdas el mote de tu pandilla. Esto son cosas que no mucha gente sabrá, es tu vida, son tus experiencias.

En mi caso si hago ese ejercicio mientras escribo esto, en lo primero que pienso es en mi abuela paterna y el gazpachuelo que hacía, parece que puedo saborearlo, no habrá nadie que lo haga como ella. Estoy seguro de que no era solo la receta, sino el amor que le ponía cuando lo hacía.

¿Que no sabes que es el gazpachuelo? No sigas leyendo sin buscarlo en Google :)

Para mí esa tiene que ser mi contraseña:

Megustaelgazpachuelo.

Pero vamos a mejorarla un poco más. Para eso lo único que vas a hacer, es cambiar la última l por un 1.

En nuestro check list de contraseñas seguras, esta contraseña tendría: mayúsculas, signos (.), minúsculas, algo local y mucha extensión.

Perfecto. Y veamos qué nos dice nuestra web favorita sobre el tiempo de hackeo. Y el resultado es tachán, tachán: ¡Cien billones de años!

Ahora ya no tenéis excusa, podéis cambiar vuestras contraseñas malas por unas súper contraseñas. Vale, otra vez sé lo que piensas. Que soy muy exagerado, que al fin y al cabo no tienes nada que ocultar. Que para qué se van a molestar en hackearte a ti. Me temo que tienes que leer el siguiente apartado.

JUERETO 5.- CONTRASEÑAS BUENAS PERO BUENAS

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Vamos con otro "Juereto". En este os vais a reír mucho, lo prometo. Es muy fácil. Como siempre podéis competir entre vosotros (es la mejor forma de aprender).

Se trata de pensar en diez contraseñas. Estas son las reglas.

Las tres primeras contraseñas **tienen que ser las peores que se os ocurran, cuanto más malas mejor**. Ganará el que descubra la contraseña que menos tiempo se tarde en hackear. Esta prueba vale **por 3 puntos.**

Las tres siguientes, **serán contraseñas que ya estéis utilizando**. Aquí ganará el que tenga la contraseña más segura en tiempo de todos. Esta prueba vale por **tres puntos.**

Creareis dos contraseñas utilizando **el método de los acrósticos**. Ganará el que consiga la contraseña más segura en tiempo. Esta prueba vale por **dos puntos.**

Por último, dos contraseñas utilizando el método: **regreso al pasado**. Ganará el que consiga la contraseña más segura en tiempo. Esta prueba vale por **dos puntos.**

La puntuación máxima que alguien puede obtener **son 10 puntos.**

Aprovecha este juego donde tus hijos se reirán mucho viendo las contraseñas que utilizan sus padres y las que tienen ellos, para explicarles lo importante que es la contraseña. Diles que es igual de importante que la llave de la puerta de casa, que no es algo que se pueda dar a cualquiera, que hay que mantenerla segura.

Te aconsejo también que hayas leído el apartado siguiente donde podrás contarles cómo se paga por los datos en internet, y cómo

existen personas que comercian con ellos. Les encantará la web que te enseñé y los trucos para crear contraseñas. Anímalos a que lo cuenten a quienes conozcan.

Por cierto, te tocará decidir el premio para el ganador de este "Juereto".

Concursante 1	
Concursante 2	
Concursante 3	
Concursante 4	

CONTRASEÑAS MALAS PERO MALAS	TIEMPO DE HACKEO
1	
2	
3	

CONTRASEÑAS QUE ESTAMOS UTILIZANDO	TIEMPO DE HACKEO
1	
2	
3	

CONTRASEÑAS CON ACRÓSTICOS	TIEMPO DE HACKEO
1	
2	

CONTRASEÑAS CON EL MÉTODO REGRESO AL PASADO	TIEMPO DE HACKEO
1	
2	

PUNTOS TOTALES (Máxima puntuación 10 puntos)	

4.4.- MERCADO NEGRO DE LOS DATOS: ¿CUÁNTO VALE UN GMAIL EN EL MERCADO NEGRO?

Mira que llevo años en este trabajo y todavía me sorprende la inocencia de las personas. Para argumentar que no se preocupan por su privacidad, contraseñas, ciberseguridad, etc… te dicen estas tonterías:

- no tengo nada que esconder
- yo no soy importante
- mi vida es aburrida
- no soy famoso

Esto es una soberana estupidez. ¿Recuerdas a un tal Edward Snowden, ese muchacho que es perseguido por hacer públicos documentos clasificados como alto secreto de la Agencia de Seguridad Nacional de Estados Unidos? Pues tiene una frase maravillosa y a la que no tengo nada que añadir:

"Decir que no te importa la privacidad porque no tienes nada que esconder, es como decir que no te importa la libertad de expresión porque no tienes nada que decir. No se trata de que tengas algo que esconder, sino de que tienes algo que proteger: tu libertad".

Reflexiona sobre esto.

Cuando un hacker logra encriptar tu ordenador (y por cierto pedir un rescate en Bitcoin), ¿de verdad crees que está interesado en lo que tú tienes? No, él también piensa que tu vida es aburrida. Qué va es broma. Es peor, no sabes ni que existes. Tú no eres nadie para él. Lanzan miles de anzuelos cada día y tú eres su pesca de hoy.

No tiene interés en las fotos que tienes en tu ordenador, miles desde que tus hijos eran pequeños (por cierto sin ordenar ni hacer el

álbum que siempre dices que vas a hacer), pero es consciente de que tú sí pagarías por recuperarlas (sobre todo porque no tienes una copia de seguridad). En esas fotos están las primeras palabras de tus hijos, sus primeros pasos, el primer cumpleaños, etc…

Ese es el juego, tú quieres algo a lo que ahora mismo ya no puedes acceder y el hacker lo tiene.

En este capítulo quiero dejarte la lista de la compra.

¿Cuánto valen los datos en el mercado negro?

- Cuenta y contraseña de Gmail: entre 0,5 y 1,5 dólares.
- Cuenta y contraseña de Facebook: entre 2 y 3 dólares.
- Cuenta y contraseña de Instagram: entre 3 y 5 dólares.
- Carnet de conducir escaneado: entre 3 y 18 dólares.
- Pasaportes escaneados: entre 2 y 10 dólares.

Creo que ya te haces una idea por lo que no seguiré. Habitualmente estos datos se compran a volumen, con diversas intenciones y ninguna buena: extorsionar, suplantar la identidad, realizar estafas, etc…

Incluso existen servicios que te permiten comprar la vida completa de una persona por unos 500 a 900 dólares. Sus estudios, NIF, correo electrónico, tarjetas de crédito, etc…

Este tipo de compras, como te puedes imaginar, no se realizan poniendo en Google: "quiero comprar datos en el mercado negro". Por cierto, esta búsqueda en castellano arroja más de 50 millones de resultados, cómo somos las personas. Para estas compras se acude a la internet oculta o privada, la denominada: Deep Web.

Esta parte daría para un libro. En realidad muchos de los capítulos que estamos tratando lo harían. Mi idea es seguir escribiendo libros que de forma práctica puedan ayudar a los padres a proteger y educar a sus hijos en internet. Pero me desvío, a lo que íbamos: la Deep Web.

Si vas a Google y buscas "iceberg", verás por las imágenes que lo que emerge del agua es muy inferior a lo que se queda bajo ella. Esto ocurre con internet también, nosotros utilizamos habitualmente la parte que emerge del agua, esa es la internet pública. No creo que llegue ni a un 4% del total. Y a nosotros nos parece inabarcable, enorme.

La internet de verdad aparece oculta a nuestros ojos, es el 96% del total, eso es lo que conocemos como Deep Web.

Si de nuevo vas a Google y pones Deep Web, te vas a dar cuenta rápidamente como la publicidad no es la mejor del mundo.

Y eso es por la diferencia entre privado y anónimo. Cuando buscas algo por la internet pública, sabemos dónde estás y en función de esto tu internet se adapta a ti, en cuanto a publicidad, recomendaciones, etc… Lo habrás notado cuando buscas un vuelo en concreto. Después tendrás publicidad de ese vuelo. Esto es privado pero no anónimo.

Pero en la Deep Web es imposible saber desde dónde haces la búsqueda, eres anónimo, por lo que el sistema de publicidad en internet no funciona de forma adecuada. Si no saben dónde estás no saben qué publicidad ponerte.

La internet normal es el reino de Google y otros gigantes, la Deep Web es el salvaje oeste para bueno y para malo.

Para malo porque permite a muchos criminales aprovecharse de ese anonimato para cometer delitos e intentar salir impunes. Fíjate que he puesto intentar. Este es el lugar indicado por tanto para la venta de bases de datos ilegales, siendo el mayor mercado negro del mundo de datos robados. Las extensiones de este tipo de webs son: .onion. Ten precaución donde te metes.

Pero ese anonimato también puede ser muy bueno. Si soy periodista y estoy haciendo un reportaje de investigación, hacerlo desde la internet pública me lo complica todo si comienzo a realizar búsquedas sobre pederastia, mi navegador entenderá que este tema

me interesa y me comenzará a poner noticias y enlaces relacionado con eso. Algo que no me interesa lo más mínimo una vez termine el reportaje. Pero más importante que esto déjame que te cuente una historia que tiene algunos tintes reales.

Consuelo es una mujer valiente, con principios. Trabaja en el departamento jurídico de una multinacional de vehículos. Y desde hace tiempo está viendo una serie de prácticas que no le gustan. Por un lado, reuniones con otras empresas del sector para acordar estrategias y precios en común. Además de algunas prácticas sobre el movimiento de dinero a paraísos fiscales que también son sospechosas.

Consuelo conoce la ley, sabe que ante esas sospechas en su empresa disponen de un canal de denuncias privado, donde puede ponerlas en conocimiento del departamento de compliance. Este departamento se encargará de investigarlas. También existe un organismo público para ello que también tiene un canal de denuncias donde no se piden datos.

Aunque no lo tiene del todo claro sabe que algo tiene que hacer, su conciencia se lo reclama. Pero no estamos en Estados Unidos (esto es España). A diferencia de Estados Unidos donde si alguna de estas prácticas conllevan una sanción, a la persona que ha ayudado a destaparlas se le asigna una cantidad económica por ello. En España ella sabe que si alguien se enterara podría traerle serios problemas profesionales, incluso dificultad para encontrar trabajo en el futuro. Dirían que fue una chivata, en inglés tienen una palabra que suena mejor: *whistleblower* (el que toca el silbato).

Tras algunas semanas de darle muchas vueltas ha tomado una decisión. Decidió denunciarlo.

Sabe que la ley dice que esta comunicación es confidencial, y está un poco más tranquila porque en el formulario no le han pedido ningún dato personal. Al poco tiempo, Consuelo fue despedida, no encontrando trabajo en ninguna empresa del sector.

¿Qué ocurrió?

Pues que Consuelo no conocía la diferencia entre privado y anónimo. Efectivamente, ella no puso dato personal alguno pero lo completó desde su ordenador de trabajo, que está perfectamente identificado en la red de la empresa. Aunque en teoría su nombre debía ser protegido, la realidad es que se filtró rápidamente.

Para este tipo de cosas la Deep Web es una maravilla. Tanto es así, que la **Agencia Valenciana Antifraude (https://www.antifraucv.es/) y la Oficina Antifraude de Cataluña (https://www.antifrau.cat/es/es)** cuando vas a interponer una denuncia te advierten que:

El Buzón de Denuncias permite el anonimato y garantiza la confidencialidad y seguridad de las comunicaciones.

El buzón garantiza en todo momento la confidencialidad de las comunicaciones y la identidad del informante. Las personas pueden facilitar sus datos identificativos y de contacto o, si lo prefieren, también pueden hacer la comunicación de manera anónima.

Hay dos opciones para realizar la comunicación de manera anónima:

1. Utilizando su navegador pero sin facilitar los datos identificativos y de contacto. En este caso queda rastro de la dirección IP desde la que se realiza la comunicación, la cual puede ser requerida a la Agencia por las autoridades competentes.
2. Garantizando plenamente el anonimato de la comunicación en el entorno digital (también de la dirección IP, que puede identificar a la persona que navega por Internet), utilizando una red de anonimización. La herramienta más utilizada es la red TOR. La forma más sencilla de utilizar esta red es descargar e instalar el navegador Tor Browser, que se puede obtener desde la página https://www.torproject.org/download/download-easy.html.es.

El análisis de las herramientas usadas por otras entidades dedicadas a la denuncia ciudadana y expertos en estos temas, aconsejan facilitar esta opción de anonimato para preservar la integridad de quien informa, que a menudo puede estar en situación de vulnerabilidad.

La red TOR es básicamente un software gratuito y de código abierto que permite mejorar la privacidad y seguridad en Internet. Al conectarse a Internet con TOR, la conexión pasa a través de una serie de túneles cifrados antes de ser encaminada hasta su destino lo que dificulta rastrear la fuente de la información. Así, la identidad de la persona que se conecta al Buzón de Denuncias está protegida.

El uso de la red TOR para acceder al buzón es aconsejable o indispensable cuando se tiene el convencimiento o la certeza de riesgo, porque garantiza el anonimato de la persona en el momento de la recepción de la comunicación. No obstante, hay que recordar que quien informa debe preservar, también, el anonimato en el momento de la emisión.

En muchas administraciones públicas y redes corporativas en general, los administradores de dichas redes impiden el acceso a la página de descarga de TOR o filtran el tráfico dirigido a ella. Por ello, para utilizar este software puede ser necesario hacerlo desde un ordenador de uso personal.

Como has podido leer, se refieren en varias ocasiones a TOR.

TOR es el navegador por excelencia de la Deep Web, su puerta de entrada. Su utilización es muy similar a la de cualquier navegador de la internet pública. Puedes descargarlo en este enlace:https://www.torproject.org/es/download/

Y si lo utilizas para navegar por las webs que habitualmente utilizas, es de lo más seguro. La misión de Tor es:

"Promover los derechos humanos y las libertades mediante la creación y despliegue de tecnologías de anonimato y privacidad libres y de código abierto, el apoyo a su disponibilidad y utilización

sin restricciones y el fomento de su comprensión científica y popular". Y cuando lo utilices por primera vez, podrás ver cómo tus IP (la dirección por la que entras a internet) cambia constantemente, sería como intentar robar una casa que no para de cambiar su dirección. Por lo que la Deep Web no es mala ni buena, sino como toda la tecnología somos las personas con el uso que le damos lo que convertimos una tecnología neutra en un instrumento para hacer daño o para ayudar a otras personas.

A continuación te facilito una nueva hoja de nuestra hoja de ruta.

La hoja de control de contraseñas. Si la hubieras leído antes de este capítulo te sonaría a chino, pero ya estás en disposición de comprender todo lo que recoge la misma. Olé tú.

Ah en cuanto a la doble verificación te lo explico todo en el capítulo 7. También he creado un libro para el control de la seguridad de las contraseñas que utilizamos los padres y las que utilizan tus hijos, para aplicaciones, webs y redes sociales. Lo encuentras como material adjunto a este libro, espero que te sea útil.

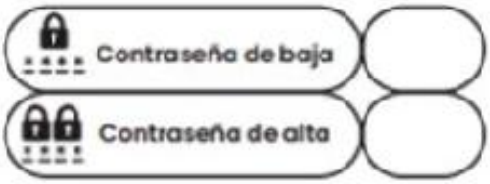
Y ahora sí, vamos al siguiente capítulo: ¿Qué sabe Google de ti y de tu hijo? Estoy deseando que curiosees conmigo. ¿Me acompañas?

HOJA DE RUTA 3.- HOJA DE CONTROL DE CONTRASEÑAS

“ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ”

HOJA DE CONTROL DE CONTRASEÑAS

FECHA	
APLICACIÓN/WEB/RED SOCIAL	
DIRECCIÓN WEB	
NOMBRE USUARIO/ID	
EMAIL REGISTRO	
MÉTODO CONTRASEÑA: - REGRESO AL FUTURO - ACRÓSTICOS	
¿SE HA HACKEADO ALGUNA VEZ ESA CONTRASEÑA? (https://haveibeenpwned.com)	
¿SE HA HACKEADO ALGUNA VEZ EL CORREO ELECTRÓNICO? (https://haveibeenpwned.com)	
¿QUE TIEMPO SE TARDA EN HACKEAR LA CONTRASEÑA? (https://www.passwordmonster.com)	
¿ESTÁ ACTIVADA LA DOBLE VERIFICACIÓN? FECHA PARA MODIFICAR CONTRASEÑA (mínimo cada 6 meses)	



5.- ¿QUÉ SABE GOOGLE DE TI Y DE TU HIJO?

Repite conmigo: Google lo sabe todo. Google lo sabe todo. Google los sabe TODO.

Vale, ya sé que puedes pensar que soy un pelín exagerado, pero no. Google lo sabe todo, pero ¡todo! Y tengo un capítulo entero para demostrarlo. Ahora vas a comprender en su profundidad la frase que ya hemos mencionado antes: "Si algo es gratis en internet el producto eres tú".

¿Preparado para abrir los ojos como platos? Pues en marcha.

Para comenzar vamos a hablar de por qué ves la publicidad que ves y no otra. Esto no es aleatorio, eso ya lo intuyes. Google te tiene perfectamente segmentado (también lo veremos en otro capítulo con Facebook) y sabe perfectamente qué te gusta y qué no, aumentando las posibilidades de compra para quien le paga por publicidad. De esto va la película. ¿Preparado para ir al psicoanalista?

Iremos a la parte de Ads Settings (www.adssettings.google.com) y recuerda estar logueado en tu Gmail. En castellano lo encontrarás como personalización de anuncios.

En mi caso tengo más de 100 criterios que se utilizan para mostrarme anuncios, esto tiene que ver con las búsquedas en Google, Youtube o sitios webs y aplicaciones en los que Google está presente, que son como te imaginas muchos.

Veamos qué me tiene que decir Google:

- 35 a 44 años. Cierto, en este momento tengo 42 años.
- Hombre. Nada que añadir.
- Idiomas: español e inglés. El inglés, regular la verdad.

- Nivel de estudios: Posgrado. Sabe los estudios que tengo.
- Mi ubicación.
- Sistema operativo y móviles desde los que me conecto.
- Y alguno de mis gustos: baloncesto, las bandas sonoras, el cine (sobre todo el de animación y humor), cómic, criptomonedas, fondos de inversión, fútbol, informática, inversión, juegos (deportivos, ordenador y de misiones), Málaga, mitos, música (latina, pop), películas (familiares y románticas) y los perros. Casi nada.

Esto es una aproximación muy cercana a lo que soy. Ya me conocéis mejor, jeje. Pero nada es perfecto, hace poco tuve que ir a Castilla La Mancha, tuve que buscar billetes, alojamiento etc… y ya me lo indica como uno de mis gustos. No digo que no me gustara, pero tanto como para que sea un gusto permanente y sobre esto reciba publicidad, va a ser que no.

¿Qué hacer con todo esto?

En primer lugar, saber que existe y que yo veo lo que veo por esta segmentación, pudiendo adaptarla a mí quitando aquellos intereses que no tengan nada que ver conmigo.

Solo tendrás que hacer "clic" sobre ellos y marcar la opción **<Desactivar>.** Si no te apetece que Google personalice nada sobre ti, puedes directamente desmarcar la opción al inicio de la página que indica: **<La personalización de anuncios está activada>.**

Tal y como indica Google, los datos que utiliza para mostrarte anuncios son:

- **Tus datos:** Información de tu cuenta de Google, como el intervalo de edad y el sexo. Tu ubicación general.
- **Tu actividad:** Tu consulta de búsqueda actual, actividad de búsqueda anterior, tu actividad con sesión iniciada en tu cuenta de Google. Tus anteriores interacciones con anuncios.

Tipos de sitios web que visitas. Tipos de actividad en aplicaciones móviles de tu dispositivo. Tu actividad en otros dispositivos.

- **Otra información:** La hora del día. Información que has proporcionado a un anunciante, como cuando te registras en un boletín informativo con tu dirección de correo electrónico.

Divertido. Lo cierto es que puedes hacer que todo esto mejore (y sea todo un poco más privado) con tres sencillos pasos. Ya sabes que no me gusta quedarme en la teoría:

1. Ya lo hemos hecho, desactivar la opción de personalizar los anuncios.
2. Vamos a eliminar al monstruo de las galletas (cookies). Te lo explico en el apartado siguiente.
3. Siempre intentaremos navegar de incógnito.

Hablemos un poco más de este último punto.

El modo incógnito o modo privado es mal entendido. Parece que cuando navegamos con esta pestaña lo hacemos de forma anónima. Y eso es falso. La única forma de navegar de forma anónima es la que ya vimos a través del navegador Tor en la Deep Web.

Pero sí que tienen algunas ventajas como no rastrear el historial de búsquedas. De esta forma cuando cerramos el navegador, estas páginas web no aparecerán en el historial de búsqueda ni como sugerencias. Tampoco se quedarán guardados los datos que introduzcamos en formularios.

Pero el modo incógnito no evita que las páginas que hemos visitado sepan que lo hemos hecho nosotros, porque tendrán nuestra IP (la dirección de nuestro ordenador), y los proveedores de servicio (incluido Google) podrán monitorizar nuestro tráfico.

¿Dónde encuentras el modo incógnito?

El modo incógnito lo encuentras arriba a la derecha donde aparecen

los tres puntitos, bajo el nombre: **<Nueva ventana de incógnito>.** Y verás como el color de tu navegador cambia. No es perfecto pero es una buena costumbre navegar así. Aunque es más importante controlar las galletas (cookies). ¿Que no sabes lo que es una cookie? No te preocupes, te lo cuento en el siguiente apartado.

JUERETO 6.- GOOGLE VS HIJOS

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Me encantan todos los "Jueretos", pero este es uno de los que más. Vamos a poner a competir a Google vs Hijos.

¿Quién ganará?

Redoble de tambores.

Estas son las reglas. **Tus hijos tendrán que completar una hoja con la información de su papá o mamá**. Esa hoja tendrá dos partes, te cuento cómo ira la puntuación:

- Edad, estudios, marca del teléfono e idiomas. Fácil, ¿verdad? Esto son **tres puntos si lo aciertan todo**. Sino un cero. Lo siento, no hay término medio.
- Gustos. Tendrán que poner 7 aficiones o gustos de papá o mamá. Cada **gusto o afición que acierten, y que además también lo tenga Google en su segmentación será un punto.**
  Si es un gusto o afición tuyo, pero que Google no tiene, **serán dos puntos.**

Y si no es un gusto o afición tuyo, **será cero puntos**. La puntuación máxima de esta parte **son 7 puntos.**

La puntuación de Google es más fácil, cada acierto de Google respecto a lo que recoge en tu segmentación es un punto.

Gana quien más puntos tenga.

Comienza la competición entre Google y tus hijos.

No olvides enseñarle cómo funciona esto, y cómo se puede interactuar para limitar lo que Google sabe de nosotros. Por cierto, cuéntame quién ganó:hola@metodocangurodigital.com

El premio te lo dejo decidir a ti. ¿Quién te conoce mejor?

HIJOS	

PADRE/MADRE		
	Datos que indican los hijos	Datos que tiene GOOGLE de ti
Edad		
Estudios		
Marca del teléfono		
Idiomas		

PUNTOS HIJOS (Max. 3 puntos)	PUNTOS GOOGLE (Máx. 4 puntos)

GUSTOS/AFICIONES QUE INDICAN LOS HIJOS

1	
2	
3	
4	
5	
6	
7	

5.1.- ELIMINANDO AL MONSTRUO DE LAS GALLETAS

No es que el monstruo de las galletas me caiga mal. Yo también veía Barrio Sésamo. El problema es que las cookies son un auténtico monstruo de internet.

Pero Iván, ¿qué son las cookies?

Antes de darte una definición, te lo explico con un ejemplo de los míos.

Manuel tiene una tienda de ropa que tiene una gran fama en Málaga. Y dentro de poco se acerca el cumpleaños de mi mujer, Raquel. Así que me acerco a la tienda de Manuel. Él es súper amable y al entrar en la tienda me pregunta si me puede ayudar. "Claro que sí", le dije. Me cuenta la historia de la tienda y me enseña unos vestidos preciosos, pero entre vosotros y yo, la verdad son un poco caros. Necesito pensarlo.

Me voy a despedir y Manuel me acompaña a la puerta, ya os he dicho que es muy amable. Todo normal. Lo raro es cuando Manuel me pregunta dónde tengo el coche, le contestó sin pensar que a unas dos manzanas. Pero va y me dice que quiere acompañarme.

Durante el camino me va contando el tipo de tela del vestido, el diseñador, lo bien que seguro que le queda a mi mujer (Manuel la conoce). Hasta que llegamos al coche. Esto ha sido raro, y el camino se me hizo eterno.

Al llegar al coche (doy gracias a Dios) porque esta aventura acabó. Pero no acaba. Cuando estoy abriendo la puerta para sentarme y me estoy despidiendo de Manuel, me doy cuenta de que ya se ha sentado en el otro asiento. Esto ya no es normal.

Manuel me dice que desde Málaga a Villanueva del Trabuco (pueblo donde vivo) es poco más de media hora. Que me va a acompañar y

así me va contando más cosas del vestido. Os puedo asegurar que fue la media hora más larga de mi vida. Al llegar a casa, Manuel decide entrar y saludar a Raquel. Mi mujer va y le invita a quedarse a comer, Manuel no tarda ni un segundo en aceptar, además me guiña un ojo.

Terminada la cena, Manuel piensa que no es hora para volver a Málaga (ya no hay autobuses) y decide quedarse a dormir. Me afirma que se volverá mañana conmigo. También me dice que si me despierto por la noche y quiero confirmar la compra del vestido o que me cuente más cosas, que allí estará. Y tanto que estará, si ya está acomodado en mi sofá…

Es la compra del vestido más surrealista de la historia.

¿Qué os parece cómo actuó Manuel?

Os parece desproporcionado y un pelín acosador, ¿verdad? A mí sí me lo pareció. Si alguno está pensando que no, que se lo haga mirar.

No es lógico que para comprar un vestido tenga que seguirme a todos lados. Saber mi coche, dónde vivo, conocer a mi familia, ¡pero es que se quedó hasta en mi casa!

Bienvenidos a lo que es una cookie. Una cookie es un Manuel pero el mundo online.

Uf, Iván, vaya tela, ¿me puedes definir porfa entonces lo que es una cookie?

Claro que sí, las cookies son como pequeños programas que se instalan en tu navegador y que permiten extraer información sobre tus hábitos de navegación que has visto, durante cuánto tiempo, etc…

Pueden seguirte durante mucho tiempo, incluso años. Ya nos parecía pesado un Manuel, pues imaginaros esto. Es cierto que existen cookies que son inofensivas. Pero a mí me preocupan las que estamos comentando, las cookies que son auténticos espías. Esto es

lo que provoca que busques información sobre un viaje y de repente te aparezca publicidad de hoteles de esa zona. No es magia, son cookies.

Imaginemos que una cookie es una empresa, que no siempre es así, porque una empresa podría ponernos varias cookies. De media a cada persona nos siguen entre 300 a 500 cookies.

En el ejemplo de antes, visualizad la siguiente imagen, entro en la tienda de Manuel y detrás mía en fila india me vienen siguiendo 280 personas (cookies), que también pasan a la tienda de Manuel para ver qué hago yo allí dentro. Cuando termino y salgo, me siguen acompañando como una procesión de cookies, a las que también se añade al final de la fila nuestro amigo Manuel. Es una locura.

Ahora comprendéis lo que siempre les digo a mis clientes, nunca estamos solos en internet, las cookies (cientos de empresas) nos acompañan siempre.

¿Pero esto se puede evitar?

Por supuesto que sí, pero antes de contaros qué podemos hacer para evitar esto, déjame explicarte un caso que me ocurrió y que nunca olvidaré. Se trata de uno de los casos más surrealistas del mundo, se podría titular: cómo una cookie descubrió el embarazo de una adolescente, antes que su propio padre.

¿Tienes curiosidad? Pues te cuento lo que ocurrió.

Noelia estaba preocupada por si podía estar embarazada, tenía un retraso de unos días y en ella eso no era normal. Por lo que empezó a buscar en internet de forma compulsiva cuestiones como: primeros síntomas de un embarazo, cambios físicos, etc… no pudo evitarlo e incluso algunas búsquedas fueron de nombres de bebés, aunque estaba segura que no podía estar embarazada.

Todas estas búsquedas en poco tiempo, produjeron una gran cantidad de cookies. Por lo que todos los anuncios que se comenzaron a mostrar en ese navegador tenían que ver con embarazos y el mundo de los bebés.

Fue en ese momento cuando Antonio, el padre de Noelia empezó a cabrearse, su mosqueo (me encanta esta palabra) crecía por día. No entendía qué le pasaba a su ordenador, se preguntaba por qué recibia tanta publicidad de bebes, si en su casa ya no había ningún niño. En su casa solo estaban su mujer y él, y Antonio ya tenía claro que no estaban en esa edad. Además vivía su hija, pero era una adolescente.

Lo hubiera dejado pasar, pero casualidades de la vida, le saltó una publicidad que le llamó la atención. Era de una tienda cercana de ropa de bebé. Y como le cogía de camino en su paseo diario se acercó a ver al dueño, al que por cierto conocía, para preguntarle por este misterio.

La verdad es que ese día Antonio se había levantado con el pie cambiado, estaba de malhumor. Cuando Antonio comenzó a preguntarle sobre esto al dueño de la tienda no lo hizo en el mejor tono posible, y la verdad es que el dueño de la tienda que se llama Álvaro, no supo qué contestarle.

Álvaro tenía contratada con una empresa de marketing digital la publicidad de su negocio, no hacía mucho que estaba probando esta nueva vía de publicidad, pero algo había que hacer, porque las ventas cada vez estaban peor. La empresa de marketing digital, un tal Samuel, le prometió que solo verían la publicidad mujeres embarazadas en sus primeros meses o mujeres cuyo interés fueran los bebés y determinadas marcas. Álvaro no tenía claro si esto era posible, pero quiso probar. Además le habían dicho que al ser una tienda física y no tener tienda online, esa publicidad estaría limitada a 40 kilómetros a la redonda de su tienda. La verdad es que a Álvaro le cayó bien Samuel.

Si te estás preguntado si se puede hacer este tipo de publicidad, ya te lo enseñaré en el capítulo de redes sociales.

Tras la desagradable conversación con Antonio, Álvaro se comenzó a preguntar si era mala idea lo de la publicidad digital y si era posible que estuviera fallando.

Al poco tiempo, Noelia confirmó que estaba embarazada. Cuando se lo contó a Antonio, este no entendía nada. Sinceramente creo que hoy sigue sin entenderlo, pero lo cierto es que pasado un tiempo, Antonio retomó su rutina y sus paseos habituales, al pasar cerca de la tienda de Álvaro sintió la necesidad de pedirle disculpas por lo mal que lo trato la vez anterior. Qué cosas tiene la vida.

Después de esto podría poner cientos de ejemplos más, pero creo que ya lo comprendes. Vigila las cookies de tu ordenador, porque también te están dando información que tienes que aprender a leer.

Como el Equipo A, tenemos una misión. Si esto lo leen tus hijos tendrás que explicarles quién era el Equipo A :) Nuestra misión es evitar las cookies (porque lo del embarazo es más complicado, dicho sea de paso). Para ello tenemos dos opciones principales:

1.- Navegar con el modo incógnito que ya hemos visto

Si recuerdas, una de las ventajas que tiene, es que no se instalan cookies. Pero antes de ello, acuérdate de eliminar todas las que tienes a día de hoy.

¿Cómo lo hacemos?

Siguiendo estos sencillos pasos:

- **Acudiremos primero a los tres puntitos** que tenemos en la parte superior de la pantalla, lo encuentras a la derecha.
- En las últimas opciones aparecerá una que se llama: **<Configuración o Settings>.**
- Tras hacer "clic" en la misma, en la parte izquierda verás la opción denominada: **<Seguridad y Privacidad>.**
- La segunda opción se denomina: **<Cookies y otros datos de sitios>**. Es el lugar al que queríamos llegar. Estas son las cuestiones que tendrás que comprobar:
    - La pestaña que dice permitir todas las cookies está sin marcar.

- La pestaña de bloquear cookies de terceros en incógnito, sí que lo está.
- La pestaña de bloquear cookies de terceros está marcada.
- La opción de borrar cookies y datos de sitios al cerrar todas las ventanas, también tiene que estar marcada.
- Y por último, la opción de enviar una solicitud de no seguimiento con tu tráfico de navegación, también tiene que estar marcada.

Felicidades. Acabas de eliminar al monstruo de las galletas. Pero fíjate en la opción justo debajo, como si no tuviera importancia dice: <Ver todos los datos y permisos de sitios>. Esa pestaña te dirá por sitio webs, por cierto clasificados por los más visitados, todas las cookies que te han instalado y podrás eliminarlas. Algunos sitios webs no recordarás ni haberlos visitado.

2.- Una segunda opción es instalar un Adblock (de esta forma mantendrás al monstruo de las galletas controlado, cuando navegues normalmente sin utilizar el modo incógnito).

Venga ya Iván, te acabas de inventar esa palabra.

Podría ser, pero no. Un Adblock es una extensión (habitualmente gratuita) que sirve para bloquear anuncios molestos, desactiva el seguimiento y bloquea sitios no seguros. Una maravilla.

Del que vamos a hablar se llama *Ghostery.*

Como decíamos es una extensión para tu navegador (son aquellos iconos que aparecen al lado de la dirección de la web). Lo descargamos siempre desde la tienda oficial. Su logo es un fantasma y desde ahora cuando entres a una web, este fantasmita te dirá cuántas cookies se están instalando. De esta forma siempre podrás saber quién te sigue y qué información está recopilando.

Tienes una vista sencilla donde únicamente te dicen la cantidad, y

otra vista detallada, donde puedes ver exactamente qué cookies y para qué te la han instalado. Dentro de la vista detallada, tienes arriba a la derecha la opción de bloquearlo todo.

Pero si quieres curiosear un poco más, ya sabes que esto a mí me encanta. Haciendo "clic" en los tres puntitos llegas a los ajustes. Dentro de los ajustes puedes marcar bloquear todo y listo. Pero si te fijas en algunos rastreadores (como ellos los llaman), verás que tienes rastreadores de publicidad, redes sociales, correo electrónico, comentarios y publicidad para adultos. Bichea esto un poco.

En fin, para no perder tiempo lo dicho: bloquear todo.

JUERETO 7.- GALLETAS

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Este "Juereto" es muy sencillo pero también muy visual y divertido.

De nuevo **es una competición padres vs hijos**, ya te habrás dado cuenta que me encantan estas competiciones.

Para esta competición necesitarás tener instalada esta extensión **de *Ghostery*** en tu navegador.

La competición consiste en que durante cinco minutos, los equipos de padres y de hijos buscarán **la web española que más cookies te instale (el que gane obtiene 5 puntos) y la web extranjera que igualmente más cookies te instale (el que gane obtiene otros 5 puntos).**

Puntuación **máxima 10 puntos.**

¿Y qué hacemos si empatamos?

Pues fácil, en caso de empate sumamos las cookies de ambas webs y el que más tenga gana.

¡Ánimo y a por todas!

Ah, no olvides aprovechar la actividad para contarle a tus hijos qué son esto de las cookies y cómo protegernos de ellas. Y por supuesto, antes de empezar a jugar os toca decidir el premio.

PADRES

Web española	Número de cookies
Web extranjera	Número de cookies
TOTAL DE COOKIES:	

HIJOS

Web española	Número de cookies
Web extranjera	Número de cookies
TOTAL DE COOKIES:	

GANADOR FINAL

PADRES	
HIJOS	

5.2.- PARTE PRIVADA DE GOOGLE

¿Cuál es la prueba de amor verdadero? Cuidado con esta pregunta cuando nuestros hijos están en la adolescencia. Existen muchos adolescentes que ven como algo normal que tu pareja tenga que conocer todo lo que haces y dónde estás en cada momento del día (modo offline).

Pero lo que necesito explicarte es que muchos adolescentes, bajo la bandera del amor y como muestra de amor verdadero, ceden su contraseña de Gmail al amigo o amiga. Tener una cuenta de Gmail compartida, que bonito e inofensivo, ¿verdad?

Pues una leche (¿Se puede decir esto en un libro? Creo que sí). No tienen ni idea de la locura que acaban de cometer. Semáforo rojo. Mi misión es que tú lo comprendas y se lo puedas explicar. Esto es una de las cosas más graves que puede hacer un menor.

Vamos con un ejemplo.

Recuerdo cuando Amalia me comentaba que su hija Radharani estaba feliz, radiante. Recordaba otras épocas en que lo había pasado realmente mal, sufrió acoso y como madre se le rompía el corazón. Pero eso había quedado atrás. Ahora Radharani estaba feliz y tenía novio. Aunque Amalia prefería llamarlo amigo. En una de mis conferencias Amalia aprendió cómo acceder a la parte privada de Google (ahora te lo explico), comenzó a ver cosas que no eran normales: lugares donde no debería estar su hija y páginas webs donde nunca había entrado en el pasado. Esto era raro y no era normal en Radharani.

Tras hablar con su hija, esta le dijo que había dado su contraseña de Gmail a su novio/amigo, porque eso era una muestra de confianza y amor verdadero. Lo que no sabía Radharani, es que cualquier persona con tu contraseña de correo tiene acceso a tu vida entera.

Amalia se sentó con su hija y le pudo enseñar lo que significaba

esto, hizo que ella lo viera con sus propios ojos.

Su novio/amigo cada noche le preguntaba dónde estaría al día siguiente, sus horarios. Radharani era feliz y siempre le contestaba. Pensaba que era lógico que su pareja supiera siempre dónde estaba, así si tenía que buscarla siempre sabía dónde encontrarla. Eso tenía que ser porque la quería mucho. Pero a veces surgían planes diferentes, aun así él siempre la encontraba, eso alguna vez le había resultado raro.

Ahora lo comprendía todo. ¿Cómo sabía siempre dónde estaba e incluso cómo le regalaba cosas que ella había estado buscando en internet? ¿Cómo había estado tan ciega? Él sabía todo lo que ella buscaba en internet.

Y todo comenzó cuando le entregó su contraseña de Gmail, su madre le había abierto los ojos. Pero, ¿cuántas Radharani seguirán por el mundo, pensando que han encontrado a su amor verdadero?

¿Quieres saber cómo se hace esto? ¿Cómo se mira? ¿Qué información se puede encontrar?

Pues no perdamos el tiempo, vamos a explicar lo que un día aprendió Amalia en una de mis conferencias. En marcha.

Para ello necesitaremos acceder a la parte privada de Google:

- Puedes poner en Google: **Mi actividad o my activity.**
- **O directamente buscar la siguiente web: www.myactivity.google.com.**

Si estás logueado con tu Gmail no tendrás que hacer nada más y aterrizarás en la parte privada de Google como elefante en cacharrería.

Pero si no lo estás te pedirá tu cuenta de Gmail y contraseña, por lo que cualquiera que tenga estos datos podrá ver lo que tú veras. Cuidado. Aquí es importante volver a los capítulos que explican cómo saber si te han hackeado, y cómo poner una contraseña

segura.

Gmail es la llave de tu vida.

I.- CÓMO RASTREAR TODOS LOS LUGARES EN LOS QUE HAS ESTADO

Google sabe dónde vives. Dónde trabajas. Dónde estudian tus hijos. Las actividades extraescolares que tienen. Qué restaurante te gusta más. Dónde has estado de vacaciones. El supermercado donde compras y un largo etc…

Y lo sabe de diversas formas. Pero sobre todo lo sabe si tienes activado el historial de ubicaciones. Así que no te digo nada y te lo digo todo. Ya estás tardando en mirar si lo tienes activado.

Cuando aterrizas en la parte privada de Google, lo primero que tiene que llamarte la atención (además está en el centro y tu vista se fijará ahí) es el historial de ubicaciones, como ya hemos adelantado.

Antes de hacer "clic" y comenzar a explicarte qué encontraremos en esa pestaña, una frase de Google muy divertida que define esto:

"Historial de ubicaciones. Guarda los lugares que visitas con tus dispositivos (incluso cuando no usas un servicio específico de Google) para que podamos brindarte recomendaciones basadas en los lugares donde estuviste, mapas personalizados y mucho más".

Gracias Google, pero no. Ya estás tardando en desactivarlo. Pero si prefieres que conserve tu historial por cualquier motivo, por ejemplo porque quieres volver a lugares que visitaste recientemente, mi recomendación es que al menos accedas a la opción de eliminación automática, y configures un plazo cercano en el tiempo. Pero bajo ningún concepto dejes marcado la opción de: **<No eliminar automáticamente la actividad>**.

Pero antes de tocar nada sigue leyendo este apartado y luego vuelves.

Veamos que encontramos en esta maravillosa pestaña (modo ironía

on).

Ve donde indica: **<Administrar historial>.**

¿Recuerdas dónde estuviste tal día como hoy hace un mes? ¿Dos meses? ¿Un año? ¿Dos años?

¿Verdad que no? Pues a partir de ahora sí lo harás.

Google podrá ser muchas cosas, pero desordenado no es una de ellas.

Delante de ti tienes un mapa donde encuentras marcado con puntos todos los lugares donde has estado. Antes de tocar nada, fíjate cómo te indica tu dirección de casa y del trabajo, lo tienes abajo a la derecha. Puedes consultar también los lugares que más visitaste, abajo a la izquierda.

Lo tienes todo ordenado en un ranking (con días, horas y número de visitas), como si se tratara de los éxitos de la radio.

Imagínate que alguien tiene tu contraseña de Gmail, pues no te digo nada y te lo digo todo.

Arriba a la derecha donde indica: **<Rutas>**. Puedes buscar por año, mes y día.

Alguno no tendrá actividad, suerte para ti.

Si te parece vuelvo a hacer de conejillo de indias para ti. Hoy es 7 de abril (cuando escribo esta parte) y soy incapaz de recordar lo que hice el 7 de abril de hace cuatro años. Veamos qué me dice Google.

Ese día caminé 1,3 km y 203 km los hice en coche. Lo habitual en mi vida laboral es que el coche sea mi segunda oficina o la primera, quién sabe.

Quizás te sorprenda saber que Google sabe si vas andando, en coche, bicicleta, motocicleta o autobús urbano. ¿Cómo lo sabe? Pues lo sabe entre otras cosas: por tu velocidad, soporte, aceleración, dirección, sentido, tipo de vía por la que circulas, etc…

Me indica que salí de casa a las 6:46 de la mañana (hora habitual

para mí), conduje hasta Marbella (puedo ver si por el camino me paré a tomar un café y dónde, como así fue). Llegué al Marbella Center donde estuve hasta las 11:15 horas (puedo ver también dónde aparqué el coche y que lo deje a diez minutos de mi cita). Después estuve visitando a mis amigos de Marbella Music School, terminé a las 12:46 horas. Así puedo seguir todo el día. Me recuerda también el restaurante en el que comí al mediodía. Terminé mis citas de ese día a las 18:15 horas. A las 20:31 horas llegué a casa. Día intenso.

Esto te parece una locura. Pues no lo es.

Si tienes activado tu historial de ubicaciones podrás ver esta información, sea el dispositivo que sea. En mi caso es un Iphone (ya hablaremos de pros y contras) pero estoy logueado con mi cuenta de Gmail, y si tienes Android estás logueado siempre.

En caso de que seas aficionado a la fotografía, Google también asocia esas fotos a los lugares donde has estado, y podrás verlas también de forma ordenada (qué buena gente es Google).

Pero veamos el lado positivo. Esta información también te puede ser muy útil en caso de tener que localizar a nuestros hijos. Incluso puedes ver que están frecuentando zonas no seguras y lugares poco aconsejables. El novio/amigo de Radharani conocía todo esto. Lo único que necesitaremos es conocer la contraseña de Gmail.

Pero Iván, no me parece bien conocer la contraseña de Gmail de mis hijos.

¿Tú mandarías a tu hijo cruzar la ciudad sin explicarle que es un semáforo en rojo? Siempre pongo el mismo ejemplo, pero creo que es uno de los más visuales. Habla con ellos, esto es un aspecto innegociable. Los padres tenemos la obligación de cuidarlos, pero puedes hacerlo desde la transparencia y el sentido común. Explícales que no tenemos ningún interés en conocer en cada momento dónde están, ni qué están viendo en internet. Pero en casos de urgencia y fuerza mayor es una información a la que podemos y debemos

acceder. Así de claro.

II.- CÓMO RASTREAR TODO LO QUE HACES EN INTERNET

Todavía estarás con la boca abierta tras descubrir la buena memoria que tiene el señor Google. Todos los lugares que has visitado y las fotografías que has realizado en los mismos. Pues yo no la cerraría. Me toca contarte que podemos encontrar en las dos pestañas que nos quedan por curiosear, las que encontramos justo a los lados de la que hemos visto de <Historial de ubicaciones>.

Comencemos por la pestaña: **<Actividad en la web y aplicaciones>.**

Encontrarás todo lo que has hecho, visto e interactuado en internet. Además ordenado cronológicamente: por días, hora, minuto y segundo. Te parece excesivo, a mí también.

Dentro de esta pestaña, localiza la opción desactivar, porque le vamos a dar uso. Pero antes de eso, y de nuevo poniéndome a mí como conejillo de indias, voy a revisar una semana de mi vida hace un año, en la misma fecha que escribo este libro, veamos qué me tiene que decir Google. Pero antes tenemos que hablar de otra cosa. Pero bueno Iván, siempre haces lo mismo, nos dejas con la miel en los labios. Pues sí. Pero antes quiero que te fijes en un subajuste que debe estar sin marcar. En la misma pestaña y que dice algo así como: **<Incluir actividad de voz y audio>.**

No te voy a aburrir contando para qué dice Google lo bueno que es que tengas marcado esa opción, sino que vamos a hacer un experimento juntos, partiendo de que lo tienes desmarcado. Este experimento lo he realizado en directo, en las radios en las que intervengo semanalmente, y la gente siempre flipa. Consiste en lo siguiente.

Piensa en una persona con la que hablas muy a menudo. Ya la tienes. Pues las próximas tres veces que hables con esa persona (avisa antes, sino va a pensar que te has dado un golpe en la

cabeza, jeje) vas a decir en mitad de la conversación: "quiero comprar comida para mascotas". Y después de eso, vas a seguir hablando con normalidad.

La próxima vez que abras Facebook por ejemplo, observa de qué vas a recibir publicidad. Y eso que lo tenemos desmarcado.

Ahora sí, vamos con lo que hice en internet hace un año en estas mismas fechas. Agobia un poco porque está por minuto y segundo. Una semana da mucho de sí, por lo que no puedo ponerlo todo, pero te voy a poner unos cuantos ejemplos reales para que te hagas una idea de lo que podemos encontrar:

- Todas las búsquedas que realicé esa semana en Google. Por ejemplo, uno de esos días a las 21:57 horas, busqué: "cómo conectar Metamask a Binance Smart Chain". Esta búsqueda sería para resolver alguna duda de mis alumnos del curso de inversión en criptomonedas.
- Además de las búsquedas, todas las webs que visité. Por ejemplo, a las 17:31 horas de uno de esos días, busqué en la wikipedia a Satoshi Nakamoto, el creador de Bitcoin. Pero la verdad no logro recordar por qué lo hice.
- Toda la publicidad que vi durante esa semana. Esta parte te la ahorro, por tu salud mental y la mía.
- Las reservas que estaba pensando hacer. A las 18:13 horas, me dice que busqué dentro de Travala.com, la reserva en el Westin Palace de Madrid.
- Me recuerda también y esto me sorprendió, los contratos de criptomonedas que he buscado dentro de la red de Ethereum (hablo un poco en chino lo sé, pero estoy por empezar mi siguiente libro donde explico las criptos de forma sencilla).
- Me muestra todas las imágenes que vi durante esa semana. Me sorprende que uno de los días desde las 16:03 horas y durante varios minutos, estuve buscando imágenes de

yamas. Ni idea de por qué hice eso. Creo que voy a pedir cita con el psicoanalista.

- Todos los vídeos que vi en Youtube, aunque sobre eso vamos a continuación con tranquilidad.
- Cada vez que accedía a Telegram o Whatsapp.
- Todas las veces que **utilic**é **el traductor de Google** y para qué.
- Y cada vez que accedí a las **Redes Sociales.**

Así podría seguir un rato más, pero ya te haces una idea aproximada de qué te vas a encontrar. Así que tienes dos opciones respecto a tus hijos y te toca tomar una decisión:

- La primera, es desactivar esta opción.
- Pero si piensas que puede ser útil como hemos comentado para nuestros peques, y desde una transparencia total con ellos, configuraremos al menos la eliminación automática cada cierto tiempo. Como curiosidad te diré que aparecen las búsquedas aunque tus hijos borren el historial.

Y ya por último, la pestaña que se sitúa a la derecha y que se llama: **<Historial de Youtube>.**

Aquí no se deja nada a la imaginación con el nombre. Encontrarás tanto las búsquedas que se hacen en Youtube, como los videos que ves. Y ya vas conociendo a Google, todo perfectamente ordenado.

Igualmente puedes desactivar esta opción o por lo menos marcar el borrado automático de esta parte.

Te puedes imaginar la información que podemos tener de una persona por los vídeos que consume. Y cómo es un primer indicativo de que a tu hijo le está pasando algo. Ellos no consumen apenas contenido en texto. Si tiene una preocupación o una duda, lo estará buscando en vídeo, ya sea en redes sociales o en Youtube.

5.3.- CÓMO NOMBRAR A UN HEREDERO DE MI VIDA EN INTERNET

¿Cómo borrar lo que existe de tu ser querido cuando ya no está? ¿Cómo recuperar sus fotografías y documentos importantes? ¿Cómo nombrar a un heredero de mi vida en Google? ¿Tengo que ir al notario? ¿Cuánto tiempo y dinero me costará? ¿Puede ser más de una persona?

En mi vida profesional he tenido que responder estas preguntas muchas veces.

Hasta hace unos años, acceder a la vida digital de un ser querido cuando este había fallecido, era una locura. No era solo el tiempo sino que también era costoso. Hoy en día es sencillo, rápido y gratis. Pero aun así, más del 90% de las personas no saben que esto existe y muchas menos han nombrado un heredero.

Siempre he pensado que el contenido de este libro debería ser una asignatura. Tanto para los peques como para los padres. Pero en concreto este punto debería ser algo obligatorio ya, no se puede demorar más. Ahorraría mucho sufrimiento y daría muchas respuestas a personas que no la tienen en el momento del fallecimiento. Y no solo por la posibilidad de conservar fotografías y vídeos de la persona querida, que esto es importante, porque imaginemos que tiene hijos pequeños, para ellos el día de mañana esto será un tesoro.

Pero además podrías tener más información sobre con quién hablaba, por dónde se movía, cómo pensaba, en fin todo lo que ya sabes que Google conoce. Esta información puede ayudar en tantas cosas que no podría ni enumerarlas, pero te pongo un ejemplo que tengo cercano estos días:

Melody siempre fue una persona apasionada por la tecnología, por eso cuando le hablaron por primera vez de la moneda de internet,

del Bitcoin, decidió que tenía que ser parte de esa nueva tecnología. Así que comenzó por el inicio, se formó, estudió y finalmente realizó sus primeras inversiones.

Melody no le contó nada a nadie de estas inversiones, quizás porque su familia no lo entendería, quizás porque sentía que este era su rincón de libertad, algo solo de ella. Con el tiempo y de forma natural, se fue preocupando cada vez más por la ciberseguridad y entre las medidas que tomó, estuvo la de nombrar un heredero para su vida en Google y en la redes sociales donde también era muy activa. Decidió que la persona más indicada sería su hermana. Tras explicarle en qué consiste esto, su hermana no dudo en aceptar.

Melody tuvo un accidente con su coche de vuelta del trabajo a casa y acabó falleciendo.

Fue una pérdida muy grande, sobre todo para su hermana, estaban muy unidas. Tras dejar pasar unos días, su hermana se puso a la tarea de cerrar todas las redes sociales y realizar una copia de seguridad. Lo mismo hizo con Google, pero aquí descubrió algo raro. Melody había dejado unos documentos a la atención de su hermana, donde detalla sus inversiones en Bitcoin y un paso a paso para que su hermana pudiera tener acceso y recuperar ese dinero.

Al final era una cantidad de dinero importante que se hubiera perdido si Melody no hubiera nombrado como heredera a su hermana, de otra forma su familia nunca lo habría descubierto.

A nivel profesional, la utilidad de nombrar un heredero también es una pasada, te cuento otro caso para que puedas verlo:

Adriana es informática de una cadena de hoteles. Es la única informática. Desde hace tiempo sabe que tiene que redactar un documento denominado: Disaster Recovery Plan.

Otra palabreja más. ¿Qué es esto?

Pues no es otra cosa que un documento donde Adriana deje por escrito qué hacer si le ocurriera algo, cómo funciona todo explicado tan sencillo que otro informático aunque fuera más torpe que ella,

podría continuar su trabajo por donde Adriana lo dejó. Lo que ocurrió es que un día mientras se desplazaba entre los hoteles con su motocicleta, Adriana tuvo un accidente porque otro coche se cruzó de carril sin señalizar. Pudo haberle costado la vida, pero gracias a Dios no fue así. Pero sí hizo que Adriana estuviera casi seis meses fuera de juego.

Afortunadamente, había desarrollado lo suficiente este documento y lo tenía en su Drive y Gmail. Además tuvo la precaución de nombrar como heredero al director de uno de los hoteles. Esto los salvó de un problema que podría haber sido brutal, porque el accidente ocurrió en plena temporada alta de ocupación de los hoteles.

Vale Iván, comprendo la importancia que esto puede tener tanto a nivel personal como profesional. ¿Me puedes explicar cómo hacerlo? Claro que sí, tus deseos son órdenes. Por cierto, en el capítulo de los móviles te diré cómo hacerlo para Apple. Porque para Android que es Google, entra dentro de lo que vamos a explicar a continuación. Y en el capítulo de redes sociales te lo explico para Facebook e Instagram, siendo muy parecido al resto. Así ya tendrás el círculo completo.

¿Estás preparado? Pues caminemos.

Como siempre, hagámoslo paso a paso:

1.- Iremos a nuestro lugar favorito. Los **tres puntitos** ya sabes dónde encontrarlos (arriba a la derecha). Buscaremos la opción que indica: **<Configuración>.**

2.- Tras esto, iremos a la opción: **<Gestionar tu cuenta de Google>.**

3.- A la derecha, encontrarás un menú. Marcaremos la opción: **<Datos y Privacidad>.**

4.- Ya estamos cerca. Si desciendes con la barra de navegador hasta la parte llamada: **<Más opciones>.**

5.- Y llegamos al destino, aquí está la opción: **<Crear un plan para tu legado digital>**. Sigamos.

6.- Antes de darle a **<Iniciar>**. Fíjate que Google te dice que puedes escoger, entre compartir los datos con personas en las que confías o eliminar tu cuenta.

7.- Primero configura el tiempo de espera para considerar que tu cuenta está inactiva. Es decir que ya no estás en este mundo, también se me ocurre que estés perdido en mitad del mar o que estés en coma. En fin, situaciones todas ellas pelín extremas. Puedes escoger entre: **<3 meses>, <6 meses>, <12 meses> o <18 meses>.**

Google entenderá que si en ese tiempo no has tocado Gmail, no has buscado nada en Google, no has visto vídeos de Youtube, tu móvil no tiene actividad, etc… puede ejecutar el testamento.

8.- Pero si eres pelín aprensivo, Google una vez pasado el tiempo que indiques antes de ejecutar el testamento (darle el control a la persona o personas que tú has indicado) intentará ponerse en contacto contigo varias veces: **por SMS o correo electrónico.**

9.- Dile a qué móvil quiere que haga estos últimos

intentos de comunicación y a qué correo o correos electrónicos.

10.- Elige ahora a tus herederos y qué quieres que hereden. **Puedes nombrar hasta diez personas**. Puedes poner un filtro más de seguridad para esas personas, añadiendo también su móvil.

11.- **Deja un mensaje a tus herederos** (una respuesta automática).

Se me ocurre: "Si estás leyendo esto es que ya no estoy a tu lado, pero…". (jo, qué mal rollo escribir esto, jeje).

Como recordarás, entre las dos opciones que tienes, una es nombrar heredero pero otra es que se autodestruya tu cuenta, como los mensajes de las series de espías.

Existen personas que no quieren que nadie acceda a su cuenta de Google. Consideran que a su cuenta no tiene por qué tener acceso nadie. Es una decisión. Para ello marcan la opción de que se elimine todo, incluido también los datos que hayas compartido públicamente como por ejemplo: vídeos de Youtube o Blogger.

Esta es la opción preferida por los espías y los infieles. Esto último es con ironía o no, vete tú a saber.

Te dejo un documento para que puedas completarlo. Este formulario te ayudará a nombrar herederos tanto para ti como para tu familia. Te animo a que enseñes a tus hijos a realizar este trámite, y les expliques lo importante que es esto. Que vayan y lo difundan entre la familia y sus conocidos. Puedes ponerle un reto del estilo: ¿A que no logras nombrar 5 herederos en una semana?

Tus hijos se van a sentir como notarios. Esto es tan importante que las personas que logréis que sepan esto, las podéis estar ayudando en uno de los momentos más difíciles que puedan afrontar de una forma que ahora ni imagináis. Ánimo.

Si necesitas más formularios ya sabes dónde encontrarlos. Y como siempre, me encantará leerte en las reseñas del libro (no te lo he dicho o sí, jeje, las reseñas son las que harán que este libro sea recomendado y llegue a muchas personas, ayúdame por favor) o en mi correo electrónico:hola@metodocangurodigital.com.

HOJA DE RUTA 4.- CHECK LIST: NOMBRANDO HEREDEROS EN GOOGLE

“ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ”

Persona que realiza el testamento:

Tiempo de espera para ejecutar el testamento	Indicar el plazo: 3 meses, 6 meses, 12 meses o 18 meses

Aviso previo antes de ejecutar el testamento	Indicar el móvil para sms y correo electrónico
	Móvil:
	Correo electrónico:

HEREDEROS	Correo electrónico herederos	Móvil herederos
	1:	1:
	2:	2:
	3:	3:
	4:	4:
	5:	5:
	6:	6:
	7:	7:
	8:	8:
	9:	9:
	10:	10:

MENSAJE PARA LOS HEREDEROS	Sé creativo y cariñoso

5.4.- DESCARGANDO UNA COPIA DE MI VIDA EN INTERNET

En realidad es una copia de tu vida en Google, pero la verdad es que no hay mucha diferencia. Esta copia puede ser por muchos motivos, pero yo te recomiendo hacerlo una vez por año. Admítelo, Google es mucho más ordenado que tú y ahora te lo demuestro, por lo que tener una copia de tu vida por año está perfecto. Puede ser que quieras hacer una copia antes de eliminar tu cuenta, eso me parece genial. O que la necesites para poder demostrar o acreditar determinadas cosas en un futuro. En fin, sea el caso que sea, te enseño cómo se hace.

Directamente en Google escribirás: **Google Takeout.**

Te aviso antes de continuar, en la copia de seguridad vas a encontrar muchas más cosas de las que yo te voy a hablar en estas páginas. Si tengo que entrar en todo lo que tiene Google de ti esto no sería un libro, sino una enciclopedia.

Una vez dentro de Google Takeout, seguiremos los siguientes pasos:

1.- Señalar los productos que quieres descargar. Google te permite descargar una copia con **44 productos (servicios)**. No te voy a aburrir relacionándolos todos porque es algo que puedes ver tu. Pero sí que te voy a comentar algunos de ellos una vez terminemos de generar la copia.

2.- Una vez marcado lo que quieres descargar, **marcaremos la extensión en la que lo quieres recibir**. Por ejemplo en pdf, csv o txt, por decir algunos.

3.- A continuación nos pedirá que indiquemos **el método de entrega**. Puedes escoger: que te lo manden con un enlace a tu correo electrónico o añadirlo a Drive, Dropbox, OneDrive o Box. Yo suelo dejar el enlace por correo electrónico.

4.- Señala la frecuencia. Puedes escoger en una sola vez o

exportar cada dos meses durante un año. Mi opción preferida.

5.- Qué tipo de fichero quieres, deberás indicarlo. Las opciones son .zip o .tgz. El .zip es el formato más habitual.

6.- A continuación te indica **el tamaño**, si indicas un tamaño inferior al que se genere no pasa nada, los dividirá en varios archivos. Las opciones son: 1 GB, 2GB, 4GB, 10GB o 50GB. Yo siempre escojo 50 GB.

7.- Por último solo tienes que marcar: **crear exportación**. Pero te pido paciencia porque esto llevará un buen rato.

Como te decía antes me gustaría comentar algunas de las carpetas que vas a encontrar en la descarga de tu vida digital. Por lo menos las que a mí siempre me han resultado más curiosas, (aunque siempre puedes comentarme si a ti te llamaron la atención otras, ya sabes: hola@metodocangurodigital.com):

- **Maps.** Carpetas con el historial de ubicaciones, pero con las coordenadas GPS. Es el código en bruto. Tendrás tus preferencias y sitios personales. Además de los registros de tus sitios destacados y tus reseñas.
- **Fit.** Historial de tus datos en Google Fit, incluidos los entrenamientos, las métricas de sueño, y otras como los pasos y distancia.
- **Drive.** Todo lo que tienes en tu unidad. Incluso cuestiones eliminadas recientemente.
- **Correo**. Mensajes y archivos adjuntos de tu cuenta de Gmail.
- **Calendar**. Los datos de tu calendario.
- **Contactos.** Los contactos y las fotos de los contactos que has añadido, así como los contactos que se han guardado durante tus interacciones en productos de Google, como Gmail.

- **Hangouts**. Tu historial de conversaciones y archivos adjuntos de Hangouts.

Entre muchas otras cosas. Al menos las fotos te las va a ordenar por años.

De nuevo me veo en la obligación de recordarte que cualquier persona con tu contraseña de Gmail puede tener acceso a esto, por lo que debes extremar la precaución para asegurarte que esta cuenta no se haya hackeado y que la contraseña sea segura. Ya sabes cómo.

Te dejo también un formulario para poder realizar las copias de seguridad de la familia, esto es bueno hacerlo una vez al año mínimo. Aquí existe mucha información que puede ser necesaria. Es importante.

HOJA DE RUTA 5.- CHECK LIST: DESCARGANDO UNA COPIA DE MI VIDA EN INTERNET

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

CHECK LIST: DESCARGANDO UNA COPIA DE MI VIDA EN INTERNET

PRODUCTOS Y SERVICIOS A DESCARGAR	Indicar los productos o servicios a descargar	Extensión	
		PDF	
		CSV	
		TXT	

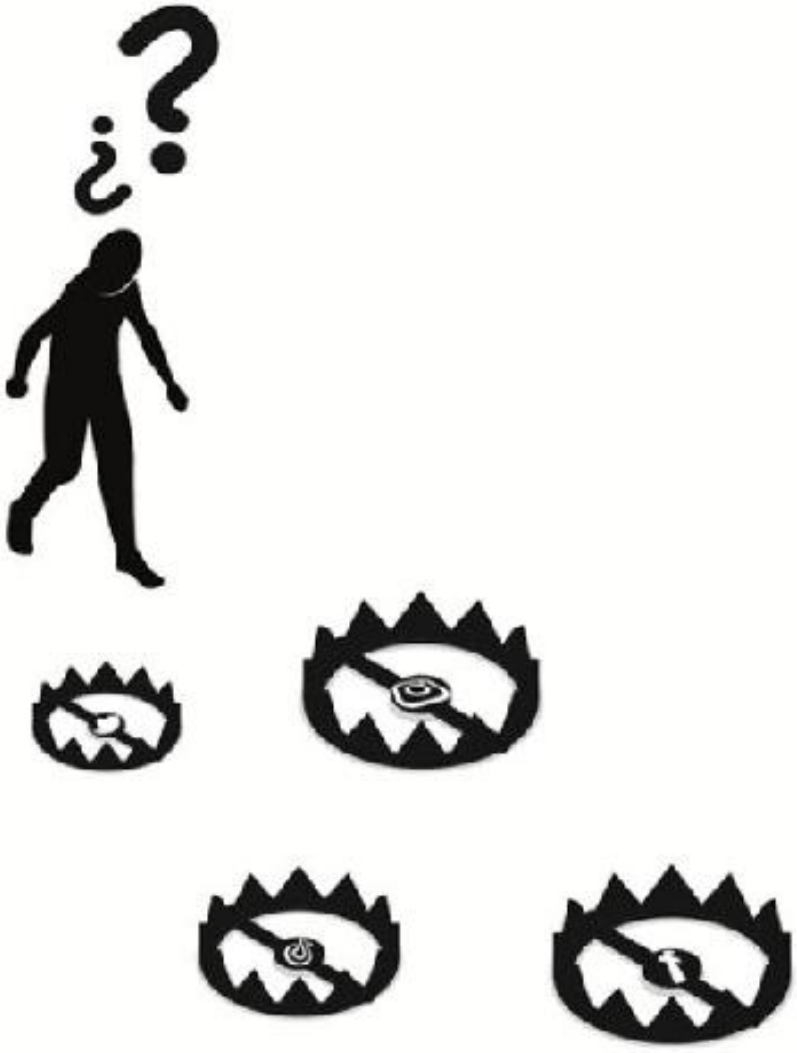
MÉTODO DE ENTREGA	ENLACE POR CORREO ELECTRÓNICO	
	DRIVE	
	DROPBOX	
	ONE DRIVE	
	BOX	

FRECUENCIA	1 SOLA VEZ	
	1 SOLA VEZ	

FICHERO	TIPO		TAMAÑO	
	ZIP		1 GB	
			2 GB	
	TGZ		4 GB	
			10 GB	
			50 GB	

POSTUREO

Y riesgos en redes sociales



6.- POSTUREO Y RIESGOS EN LAS REDES SOCIALES

¿Quién crees que te conoce mejor?: ¿Tu mujer o marido? ¿Tu madre? ¿El Gobierno?

Vale, si ya has leído el capítulo de Google, dirás que Google. Pero recuerda que el adn de las redes sociales es ponerte en contacto con personas con las que tienes intereses comunes, (aunque tú no sepas cuáles son). Y esa palabra "intereses" lo cambia todo. ¿Preparado para abrir la boca de nuevo? Espero que te haya dado tiempo a cerrarla.

Antes de divertirnos, déjame que te recuerde dos frases que ya te dije, pero que aquí quiero que las tengas presentes:

- "Hay dos palabras que son mentiras en sí mismas, fácil y gratis. No hay nada en la vida que merezca la pena que sea gratis y mucho menos fácil".
- "Si algo es gratis en internet, el producto eres tú".

Recuerda que Facebook compró hace unos años Whatsapp por 21.800 millones de dólares, una aplicación que es gratuita. Será por algo. Dale una pensada.

6.1.- QUE SABE EL MUNDO FACEBOOK DE TI (FACEBOOK, INSTAGRAM Y WHATSAPP)

Comencemos imaginando algo hipotético o no tanto.

Si lo recuerdas soy de Villanueva del Trabuco, un pueblecito de Málaga. Mi pueblo es del interior, y es habitual que algunas personas tengamos un apartamento vacacional en la costa. En nuestro caso es típico tenerlo en un pueblo costero, llamado Torrox. Hace un tiempo que Raquel y yo también compramos un apartamento allí. Torrox está a más de una hora de camino desde mi pueblo, por lo que no vamos tan seguido como me gustaría. Te tengo que confesar algo, últimamente cada vez estoy más preocupado. Y eso Iván, ¿qué ocurre?

Pues que cada vez que abro mis redes sociales, me suelen aparecer noticias relacionadas con el aumento de los robos en pisos vacacionales. En estas noticias comentan, que uno de los motivos es que los dueños pasan largas temporadas sin visitarlos. Uf como es nuestro caso. Para colmo, el otro día me apareció una noticia que decía que estaban aumentando los robos precisamente en Torrox.

Menos mal que cuando mi nivel de preocupación subía y el de mi mujer también (curiosamente le aparecían noticias muy parecidas), nos aparece publicidad de una empresa de alarmas que trabaja por aquella zona y que había sacado una oferta. No dudamos ni un segundo en contratarla. Como está el patio no podíamos dejar pasar esa oportunidad.

Venga ya. Estás intuyendo lo que ocurre. Las noticias de robos en apartamentos vacacionales son cíclicas, van y vienen. Pero "casualmente" solo se están mostrando a las personas que tenemos un apartamento vacacional. No son noticias inventadas pero sí teledirigidas a quienes les van a afectar. Posteriormente adaptamos esas noticias a tu zona. Y tu estado anímico ya está listo para consumir el producto que resuelve el problema que, por otro lado,

siempre ha existido, pero que a ti te lo han mostrado como algo urgente y que puede ocurrir inmediatamente. Vaya tela.

Ahora olvídate de este ejemplo y piensa que ocurriera con elecciones políticas. Pues ya ha ocurrido, ahora comprendes perfectamente el escándalo de Facebook y Cambridge Analytica.

Este es el poder de influencia o persuasión de las redes sociales. Algo que ni siquiera los Gobiernos podrían hacer con todos los datos nuestros que tienen.

Facebook y su mundo tienen muchas formas de saber cosas de nosotros. Una sencilla sería a través de las fotografías. ¿Recuerdas el capítulo donde hablamos de la ficha del libro (metadatos)? Pues no tengo mucho que añadir, ya sabes cómo funciona.

Una fotografía subida varias veces desde mi apartamento de Torrox, habla más alto que unas escrituras de propiedad.

Pero no es la única forma que tiene Facebook para recabar datos tuyos, lo pueden hacer: cuando estás logueado, cookies, Wifi abiertos, Gps/antenas, Bluetooth cercanos, Mac Address, Teléfono, Imei, Ip, Browser Fingerprint, etc… De muchas de esas cosas hablaremos en este capítulo y en otras partes del libro.

Pero me gustaría contarte una curiosidad (que podría ser ficción o no), te lo dejo a tu imaginación y a lo que puedas buscar en Google, jeje.

Jesús está de vacaciones con Sofía en Mallorca. Ambos son amigos desde pequeños, pero en muchas cosas no pueden ser más diferentes. Jesús es un poco aprensivo con el tema de las nuevas tecnologías e intenta proteger su privacidad siempre que puede. Eso hace que tenga la precaución de tener el Bluetooth desactivado, al igual que la Wifi y el Gps.

Sofía es todo lo contrario, esto de la privacidad no va con ella, no le preocupa nada de nada, como ella misma suele decir. Jesús sabe que tiene que tener una conversación tranquila con Sofía un día de estos, y enseñarle un libro que escribió un abogado de un pueblecito

que le abrirá los ojos.

Jesús le pide a Sofía que le haga una fotografía, siempre es él quien se las hace a Sofía, pero esta le hace ilusión, el lugar es maravilloso. Están de visita en Pollenca. Al final de un dique hay un asiento de piedra que parece sacado de una película, parece que estuvieras en el mar.

Jesús le pide que se la haga desde su móvil, porque así cuando la suba a Facebook para que la vean sus amigos esta red social no podrá saber dónde estaba. Así lo hacen. Pero resulta que Jesús comienza a recibir publicidad de restaurantes de la zona en Facebook tras subir la fotografía.

De alguna manera la red social ha sabido que estaba allí. ¿Pero cómo lo han podido saber?

La curiosidad le puede a Jesús y a Sofía, tras hacer unas cuantas búsquedas llegan a una noticia con este titular: "Facebook puede determinar tu ubicación por el polvo en la lente de la cámara de tu smartphone". Ambos flipan. La conversación de Jesús con Sofía es cada vez más urgente y la lectura del libro también.

Esto es real, creo que te divertirás con esta lectura. Siempre he pensado que lo que hoy nos parece ciencia ficción, es simplemente una ventana a lo que será nuestro futuro.

Por cierto, estos restaurantes que le han aparecido a Jesús en nuestro ejemplo de antes, son restaurantes que a Jesús le van a encantar. Facebook ya lo sabe.

Venga ya Iván. Ya solo te falta decirme que Facebook sabe aquellos sitios que me van a gustar sin que haya estado nunca.

Exacto, así es. Además sabe los que no te gustarían. Igual que sabe qué personas te van a caer bien antes de conocerlas y cuáles no. Y muchas otras cosas.

Como sé que puedes no creerme, por eso te lo voy a demostrar.

Nuestras madres siempre nos han dicho lo especiales que somos,

que somos únicos (gracias mami por decírmelo tantas veces, te quiero). Y podrá ser cierto en el mundo offline, pero no lo es en el online.

Facebook y su mundo nos han generado un archivo personal.

Visualiza un mueble de tu casa o de la oficina con tu nombre, ábrelo mentalmente, puedes ver que están todos tus intereses. Pues Facebook tiene un archivador digital con todo lo que la red social sabe de ti, por cierto todo bien ordenado que ya sabes que para estas mega empresas el orden es importante.

Ese archivo eres tú. Están tus gustos, aficiones, creencias, forma de pensar, etc… Pero no eres único, compartes gustos, aficiones, creencias y forma de pensar con muchas otras personas en el mundo "similares a ti". Por lo que cuando un "similar a ti" ha estado por ejemplo en Córdoba, Facebook sabe: dónde comió, qué visitó, por dónde paseó y qué opinión tiene de todos esos sitios. Por lo que yo, que tengo un ⅞ muy elevado de parecido, no debo ser muy diferente. Y si a mi "persona similar" le gustó, lo más probable es que a mí también te guste. Así funciona esto.

Facebook tiene esa categoría de "personas similares", que las empresas pueden utilizar para hacer publicidad.

Por otro lado, si mis "personas similares" se llevan muy bien con una persona o muy mal, es muy probable que yo también me lleve bien o mal. No somos tan especiales en el mundo online.

¿Sientes curiosidad por abrir tu archivador de Facebook y saber que contiene? ¿Hasta qué punto ese archivador influye en el mundo Facebook que yo veo?

Vamos a ello:

- Una vez entres en tu perfil de Facebook buscarás la opción con tres puntitos (ya sabes todo lo divertido siempre comienza por aquí). Está a la derecha de **<Ver más>.**

- Tras esto iremos a la configuración de **perfil y etiquetado.**
- Y dentro de la configuración, a la opción de: **<Tu información de Facebook>.**
- Nos quedaremos en la primera opción: **<Acceder a tu información>.**

Hemos llegado, ya estamos en tu archivador personal.

Como Facebook es muy fan del orden, te tendrá por cajones dentro de tu archivador.

Tenemos 8 cajones que se llaman así:

1.- Tu actividad en Facebook.

2.- Información Personal.

3.- Conexiones.

4.- Información Registrada.

5.- Información de inicio de sesión y seguridad.

6.- Aplicaciones y sitios web fuera de Facebook.

7.- Preferencias.

8.- Información sobre anuncios.

A su vez cada uno de estos cajones puede tener pequeños apartados o separadores sobre ti. Si recuerdas cuando hablamos de Google en el capítulo anterior, te decía que tenías una tarde o una mañana divertida para ir abriendo pestaña a pestaña (cajón a cajón). Pues lo mismo para Facebook.

Nosotros aquí vamos a ir abriendo los diferentes cajones de mi archivador (de nuevo de conejillo de indias) y nos vamos a asomar, pero no vamos a leer folio a folio de lo que contiene, porque de nuevo este libro se convertiría en una enciclopedia.

Te voy a comentar lo que más me llama la atención a mí. Pero puede que a ti te llamen la atención otras cosas, ya me lo cuentas

(hola@metodocangurodigital.com).

1.- TU ACTIVIDAD EN FACEBOOK (1º cajón de mi archivador)

Aquí encontramos más de 40 separadores o apartados dentro de este cajón. Flipa. Lo que más me ha llamado la atención a mí de este cajón es:

- **Las fotos.** Tanto las fotos en las que apareces, como las fotos que has subido. Como podrás ver todas tienen un icono de un lápiz que te permite acceder a modificar algunas opciones. Encontrarás la fecha, podrás modificar la dirección e incluso verás el texto alternativo que Facebook le ha dado para las personas con poca visión. Por supuesto, puedes eliminar y descargar.
- **Encuestas en las que has votado.** No te imaginas cómo se incentiva esto. Una encuesta permite conocerte y que bajes tus defensas ante determinadas preguntas.
- **Tus vídeos (sería algo parecido a tus fotos)**, pero mira qué curioso que también están todos los vídeos que has visto, ordenados por días. Esto también ayuda a Facebook a conocer tus aficiones e intereses.
- **Comentarios** que hayas puesto a quien sea y donde sea dentro de la red social. Por supuesto ordenados. El orden ante todo, jeje.
- **Messenger.** Todo lo que has hablado con todo el mundo y desde siempre.

Te dejo el resto de opciones para ti. Quizás te llame la atención la parte que habla de los grupos en los que estás, los eventos en los que has participado o los pagos efectuados dentro de Facebook. Solo con este cajón, como puedes intuir, Facebook y su mundo te conocen muy bien. Vamos por el segundo.

Pero antes de eso (ya estas otra vez Iván, cierto *sorry*), es que me acabo de acordar que he tenido que acceder varias veces a esta parte con un notario o un testigo digital, esto nos ha sido muy útil cuando hablamos de nuestros hijos. Algunas veces nos ha pasado que se han editado e imprimido fotografías donde aparecen nuestros hijos, o se han imprimido supuestos comentarios que los mismos han realizado, incluso conversaciones de Messenger. Hablas con tu hijo y afirma que nunca ha realizado esa fotografía, que nunca ha realizado esos comentarios o que nunca ha tenido esas conversaciones por Messenger. Que se han manipulado. Facebook tiene la respuesta a esto y podemos saber si ha sido real o no. Necesito que recuerdes que estas opciones existen, y que pueden y son muy útiles en muchos casos. Ah, recuerda que los mundos Facebook e Instagram son casi idénticos.

2.- INFORMACIÓN PERSONAL (2º cajón de mi archivador)

Otros 16 separadores más que encontramos en este cajón para seguir conociéndote. Veamos cuáles me llaman la atención a mí:

- **Información del perfil.** Esta debería ser la información que tú has proporcionado a Facebook. Aquí encontrarás: tu información general, trabajo y formación académica. Lugares de residencia, información básica y de contacto, familia y relaciones, detalles sobre ti y acontecimientos importantes. En lo que quiero que te fijes (además de revisar los datos), es que dentro de la información básica y de contacto, no esté completado la parte de intereses, creencias religiosas e ideología política. Es importante.
- **Fabebook Assistant**. Si utilizas esta opción aquí tendrás los audios. Yo no la utilicé nunca, así que en mis opciones no aparece nada. Pero compruébalo.
- Y ahora vamos con una de las partes que más me molesta de Facebook. **Tu libreta de direcciones**. Párrafo literal de Facebook:

"Si la subida continua de contactos está activada, Facebook subirá de forma automática los contactos de tu teléfono o tableta siempre que inicies sesión en tu cuenta de la plataforma".

Algunas frases más:

"Ten presente que si eliminas la información de esta pantalla, pero la función "Carga de contactos continua" sigue activada, la información se subirá de nuevo automáticamente".

"Al desactivar la subida de contactos en la aplicación de Facebook, esta no se desactiva de forma automática en la aplicación de Messenger".

"Si usas la aplicación de Facebook en más de un teléfono o tablet, tendrás que desactivar la subida continua de contactos en todos ellos". IMPORTANTE, IMPORTANTE, IMPORTANTE.

Uno preocupado porque al cambiar de móvil o cuando te lo roban (sobre esto hablaremos en otro capítulo, pero te hago un adelanto. A la mitad de los que estáis leyendo el libro os han robado ya el móvil o lo harán, así que leed el capítulo de los móviles tranquilamente) has perdido tu agenda de contactos, y resulta que Facebook la tiene completita. Pero no solo de tu terminal, sino de todos los teléfonos y tablets que hayas utilizado.

Así que si se te ocurre consultar tu Facebook desde el teléfono de tu amigo, ya tienes la libreta de direcciones de tu amigo subida también. Olé. Lo consultas desde el de tu pareja, pues también la agenda de tu pareja se sube. Otro olé. Y así podría seguir, no doy ideas, pero esto a veces ha generado cuestiones de fuga de información divertida, y es una forma de poder tener acceso al móvil y correos electrónicos de personas que nunca te lo hubieran dado de forma voluntaria. Olé, olé.

Ahora eres consciente de por qué hackear el Facebook de un famoso puede ser algo muy goloso para los malos. Entre otras cosas se van a hacer con una base de datos de móviles de otros famosos.

En cuanto a nuestros hijos, al igual que lo hacíamos con la cuenta de

Gmail (Google) también tendremos que tener la contraseña de acceso a sus redes sociales para casos de urgencia. Ya hablamos sobre esto, ¿verdad? Puedes utilizar el libro de contraseñas que he creado y que acompaña a este libro como material adicional.

Puedes imaginarte que saber qué personas tienen entre sus contactos nuestros hijos, puede ayudarnos a saber muchas cosas.

Te voy a dar la ruta para que compruebes que esta opción la tienes desactivada o activada. Y de no ser así, ya tienes los conocimientos para saber qué hacer. Es tu decisión, la mía es clara. Lo tengo desactivado. Ah por cierto, como ya te avisa Facebook tendrás que hacerlo tanto en Facebook como en Messenger.

- **Activar o desactivar la subida continua de contactos en Facebook (hazlo en el móvil):**
- Como siempre todo comienza por las tres barritas.
- Desplázate hacia abajo y toca: **<Configuración y Privacidad>.**
- A continuación toca: **<Configuración>.**
- Después buscaremos **<Permisos>.**
- Dentro de los mismos buscaremos: **<Subir Contactos>.**
- Ya puedes activar o desactivar.
- **Activar o desactivar la subida continua de contactos en Messenger (hazlo en el móvil):**
- Abre Messenger.
- En Chats, **toca tu foto del perfil** en la parte superior izquierda.
- **Busca contactos telefónicos.**
- Ya puedes **activar o desactivar.**

Este cajón de tu archivador tiene mucha información de ti, como todos, la verdad. Pero me importa mucho, porque con este cajón

sabemos todas las personas que forman tu vida. Recuerda que tu listado de contactos son tu familia, amigos, trabajo, hobby, lugares que frecuentas, etc… Si reflexionas un poco sobre esto, irás comprendiendo cómo Facebook te conoce.

Siguiente cajón, este siempre me ha resultado curioso.

3.- CONEXIONES (3º cajón de mi archivador)

Este es uno de los corazones de las redes sociales. Estas se basan en establecer relaciones entre personas que comparten algo en común o que se conocen. Aquí encontraremos tu lista de amigos y enemigos (amigos eliminados), por fecha y como siempre ordenado. A mí me resulta curioso.

Por cierto, también es habitual que te digan dos personas que no se conocen, y por aquí puedas ver en qué fecha se hicieron amigos y por el cajón primero (tu actividad en Facebook) puedas ver sus comentarios y conversaciones por Messenger. Facebook de nuevo sabe si mientes o no.

Os detallo que encontrareis:

- **Amigos:** personas con las que estás conectado actualmente.
- **Amigos eliminados:** personas con las que ya no estás conectado en Facebook.
- **Solicitudes de amistad enviadas**: solicitudes enviadas a otras personas para ser amigos en Facebook.
- **Personas y páginas que sigues**: personas, organizaciones o empresas cuyo contenido y publicaciones has decidido ver (aunque quizás no recuerdes ni cuándo).
- **Solicitudes de amistad recibidas**: depende de tu número de seguidores tendrás una colección de robots y personas con poca ropa.
- **Personas que te siguen**.

4.- INFORMACIÓN REGISTRADA (4º cajón de mi archivador)

Este es quizás mi cajón favorito. Son 9 separadores los que tiene este cajón de nuestro archivador personal. Espero que te haya dado tiempo a cerrar la boca de la sorpresa. Porque ahora toca abrirla de nuevo, prometido.

En marcha:

- **Descripción de la etapa vital de tus amigos en Facebook.** Esto siempre me resultó muy curioso. En mi caso se establece que la edad de mis amigos es: vida adulta. (aunque en algunos lo de adultos es discutible, jeje)
- **Tu historial de búsqueda**. Aquí encontrarás todas las frases, nombres y palabras que has utilizado para realizar búsquedas por fecha. Te puedes hacer una idea de lo importante que es saber qué busca una persona y a quién, con esto te acercas mucho a la personalidad de alguien. También tienes el historial de vídeos que has buscado y por supuesto, las búsquedas de voz.
- **Ubicación.** Tanto tu ubicación principal, como el historial de ubicaciones (Facebook sabe que esto es importante y por eso te vuelve a solicitar una contraseña para acceder), te mostrará un mapa y los lugares. Dentro del mapa podrás comprobar que lo has desactivado. Aunque ya sabes que puede ser muy útil para nuestros hijos. Aunque Facebook también nos dice esta frase que nos tranquiliza:
  "Si los servicios de ubicación y el historial de ubicaciones están desactivados, podremos seguir calculando tu ubicación de forma aproximada mediante, por ejemplo, las visitas, los eventos y la información sobre tu conexión a internet".
- **Categoría de anuncios.** Si alguna vez te has preguntado por qué tu Facebook es diferente al de tu pareja, o por qué tus anuncios no tienen nada que ver con los de otra persona, es por esto. Facebook se basa en la publicidad, vive de la

publicidad. Para esta red social y la mayoría, conocerte bien lo es todo. Deben hacerlo para que cuando alguien pague por publicidad y la quiera segmentar, llegue a las personas que más probabilidades tienen de comprar. Facebook no caza a cañonazos, sino que es un francotirador.

Siempre me ha resultado curioso saber qué creen estas redes sociales que me gusta, cuáles son mis aficiones, mi forma de ver la vida, etc… porque en función de eso me van a enseñar publicidad.

¿Quieres saber qué dice Facebook de mí? Ahí va de nuevo el conejillo de indias. Facebook dice que tengo más de 500 intereses (que es como los llama Facebook, estos intereses pueden ser cosas tan diferentes, que hasta las personas que se dedican al marketing digital se sorprenden de los intereses que existen), vamos a poner unos cuantos ejemplos. Ya sabes que si los modificas, tu Facebook y tu publicidad será diferente:

- Padre Rico, Padre Pobre (un libro).
- Kris Carr (lo he tenido que buscar, es una autora de Estados Unidos que no tengo conciencia de conocer).
- Amazon Kindle (plataforma de Amazon para autopublicar libros).
- Inversiones inmobiliarias.
- MetaTrader 4 (un software para invertir en acciones).
- Yoga.
- Emprendedores.
- Motocicletas (no están entre mis aficiones, aquí creo que han patinado también).
- Perros.
- Acondicionamiento físico (creo que Facebook me quiere decir algo, no sé si darme por aludido, jeje).

- Cerveza (en fin, creo que la probé una vez en mi vida pero desde luego no es uno de mis intereses).
- Familia.
- Jack Canfield.
- John C. Maxwell.
- Vino (tampoco diría que sea un interés para mí).
- Ikea (en fin, no diría que sea un interés, pero sí que me toca ir de vez en cuando).
- Casa rural.
- Comida rápida (más de lo que debería).
- Netflix.
- Liga de Campeones de la UEFA.
- Seguridad de la información (obvio).
- Retorno de la inversión.
- Naturaleza.
- Psicología.
- Carne.
- Fuengirola (me encanta esta localidad, pero no tanto como para que sea un interés).
- Estepona (lo mismo).
- Tel Aviv (ni idea de por qué aparece en mis intereses).
- Marbella (con esta localidad, sí tengo algo especial).
- Historia.
- Diversión.
- Derecho público.
- Lectura.

- Agua (uno de mis intereses es el agua, qué curioso, le aparecerá a mucha gente esto, ya tengo curiosidad).
- Google (motivos obvios).
- Constitución de los Estados Unidos (no creo que haya buscado esto en mi vida).
- San Juan (Puerto Rico) (no creo que tenga nada que ver conmigo, pero quizás a mis similares sí les gusta y Facebook ya sabe que a mí también me gustaría).

Suficiente para que te hagas una idea. De mis 500 intereses los he dejado en poco más de 80, el resto los he eliminado.

¡Qué a gusto me he quedado! Me hago una nota mental para hacer esto más seguido. Coméntame qué cosas curiosas has encontrado en tus intereses:hola@metodocangurodigital.com.

Siguiente cajón, por favor. Pero antes, otra de las frases maravillosas que nos deja Facebook para el recuerdo:

"Es posible que te sigamos mostrando anuncios relacionados con esas categorías si consideramos que pueden resultar relevantes".

5.- INFORMACIÓN DE INICIO DE SESIÓN Y SEGURIDAD (5º cajón de mi archivador).

Este cajón de tu archivador es más concreto.

Y te servirá para identificar quién puede estar accediendo a tu cuenta sin permiso**,** como siempre ordenado por fechas, tipo de dispositivos, sistema operativo, IP, etc…

Aquí encontramos tres separadores que, como nos dice Facebook, son:

- **Dónde has iniciado sesión**. Periodos de tiempo en los que has iniciado sesión y la has mantenido activa en Facebook.
- **Inicios de sesión autorizados**. Ordenadores y teléfonos móviles que has guardado en tu cuenta de Facebook.

- **Inicios y cierres de sesión**. Historial de tus inicios y cierres de sesión en Facebook.

Útil para saber si alguien está entrando a tu cuenta sin tu conocimiento.

6.- APLICACIONES Y SITIOS WEB FUERA DE FACEBOOK (6º cajón de mi archivador)

En este cajón necesito que revises: qué aplicaciones y sitios webs están facilitando información sobre lo que haces dentro de ellos. Es importante. **Revisa y quita permisos**. Esta parte es tan importante que te vuelve a pedir contraseña. Y no me voy a extender, porque quiero que únicamente hagas esto. De nuevo, es importante.

7.- PREFERENCIAS (7º cajón de mi archivador)

Como nos dice Facebook, son acciones que has realizado para personalizar tu experiencia en Facebook. Para nosotros este cajón es el menos importante. Vámonos al último que también tiene cosas para divertirnos.

8.- INFORMACIÓN SOBRE ANUNCIOS (8º cajón de mi archivador)

Cualquier cosa que comienza por anuncios y tiene que ver con redes sociales, despierta mi interés de inmediato. Si en el cajón 4 (información registrada, y dentro de ella la opción categoría de anuncios) hemos aprendido a mirar qué intereses tenemos, siempre según Facebook. Y eso era lo que provocaba los anuncios que vemos. Este cajón es el reverso de la moneda. Aquí sabremos qué empresas están utilizando esos intereses para hacerme llegar publicidad. Y más importante, no solo las empresas para las que soy sexy por mis intereses, sino cuáles han subido a una base de datos donde estoy incluido. Porque eso me ayudará a saber por qué esa empresa tiene mis datos si en muchos casos yo nunca he sido

cliente y nunca se los he facilitado. Miremos los míos.

He recibido publicidad de Tik Tok, Civitatis o el Marca, y el motivo es que: es posible que hayas interactuado con su sitio web, aplicación o tienda.

Pero existen al menos 20 empresas de las que no tengo ni idea de quiénes son y de las que he recibido publicidad. El motivo es que: el anunciante ha subido o utilizado una lista para mostrarte anuncios. Aquí tengo que extremar la precaución.

Primero las estoy bloqueando, además en un par de ellas les he remitido un correo electrónico para que me expliquen por qué tienen mis datos, ya tengo curiosidad.

Con esto hemos acabado todo mi archivador, casi nada, esta forma de funcionar de Facebook es la misma que utilizan todas las redes sociales. Cuanto más te conocen, mejor hacen la publicidad y más podrán cobrar por ello, por lo que más dinero ganan. Y oye, no les va nada mal.

Estas son las reglas del juego, y en esta parte te he enseñado cómo aprovecharlas en tu beneficio y como protegerte, me encantaría que la gente conociera esto.

JUERETO 8.- FACEBOOK VS FAMILIARES

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

¿Recuerdas el "Juereto" que hicimos con Google? Pues haremos uno parecido.

Lo haréis por parejas, puedes incluir a alguien más de la familia: pueden ser los primos, abuelos, tíos o incluso algún amigo.

De los presentes, uno será el juez. Este no jugará pero tendrá la misión más importante.

Vamos a intentar adivinar sus intereses (los del juez) y ganarle a Facebook. Ah, si no tiene cuenta de Facebook, no nos vale como juez. Obvio.

Cada pareja escribirá:

- **Tres libros, canciones o películas** que crean que le gustan al juez.
- **Dos localidades** que le gustan.
- Dos lugares donde le gustaría **ir de viaje.**
- **Tres aficiones.**
- **Dos famosos** que le gustaría conocer.

Tras terminar de escribirlos, el juez (recuerda el adulto que no jugaba y sobre el que estamos adivinando sus intereses) **dará un punto por respuesta correcta**. La puntuación máxima que se puede **tener son 10 puntos**. Es fácil para el juez saber si le gusta o no lo que habéis puesto. Una vez sumados los puntos sabremos la pareja ganadora y la que se enfrenta al reto definitivo, competir contra Facebook.

Ahora, le enseñaremos al juez y al resto de personas cómo se miran estos intereses en Facebook**. El juez puntuará también en**

función de los intereses que Facebook tiene de él. Completamos los intereses, cada respuesta correcta, recuerda que es un punto. Ahora suma, y tenemos el ganador final.

¿Quién ganará, Facebook o la familia?

Cuéntamelo en hola@metodocangurodigital.com.

PAREJA 1

LIBROS, CANCIONES, PELICULAS	1.- 2.- 3.-
LOCALIDADES QUE LE GUSTAN	1.- 2.-
LUGARES PARA VIAJAR	1.- 2.-
AFICCIONES	1.- 2.- 3.-
FAMOSOS	1.- 2.-

PUNTUACIÓN TOTAL PAREJA 1	

PAREJA 2

Libros, canciones, películas	1.- 2.- 3.-
Localidades que le gustan	1.- 2.-
Lugares para viajar	1.- 2.-
Aficiones	1.- 2.- 3.-
Famosos	1.- 2.-

PUNTUACIÓN TOTAL PAREJA 2	

FACEBOOK

Libros, canciones, películas	1.- 2.- 3.-
Localidades que le gustan	1.- 2.-
Lugares para viajar	1.- 2.-
Aficiones	1.- 2.- 3.-
Famosos	1.- 2.-

PUNTUACIÓN TOTAL FACEBOOK	

PUNTUACIÓN FINAL

MEJOR PAREJA	
FACEBOOK	

6.2.- CÓMO NOMBRAR UN HEREDERO DEL MUNDO FACEBOOK

Ya sabes lo importante que es esto, lo hemos visto cuando nombramos un heredero para Google. Y te puse varios ejemplos, ¿recuerdas a Melody y Adriana?

Pero si tengo que ser sincero, los casos más graves siempre los he encontrado en redes sociales, por eso este apartado vuelve a ser fundamental. Recuerdo uno que se me quedó marcado:

Manuela nunca quiso que su hija Carla se comprara una motocicleta, por lo que intentó retrasar ese momento lo máximo posible. Pero sabía que Carla no pararía hasta comprarla, era su ilusión desde pequeña. Por eso cuando empezó a trabajar y tuvo el dinero suficiente, tenía claro qué hacer con él. Se compró una motocicleta roja, estaba orgullosa de ella, por eso su Facebook se llenó de fotografías con ella, no te lo he dicho pero a Carla le encantaban las fotografías y está un pelín "pillada" con las redes sociales.

El destino es cruel y quiso que un día Carla tuviera un accidente que le costó la vida con su motocicleta. El dolor para su familia debió ser indescriptible, pero tampoco ayudaba que la última fotografía en redes sociales fuera de Carla con la moto, justo unas horas antes de fallecer. Manuela en cuanto tuvo algo de fuerzas quiso, por un lado eliminar todo eso, y por otro conservar las miles de fotos de Carla y sus vídeos. Sabía que no era el momento, pero más adelante era consciente de lo importante que serían estos recuerdos.

Casos extremos como el de Carla se complican y sobre todo se retrasan, a no ser que se tenga nombrado un heredero para el mundo Facebook. Por eso, este punto es fundamental con todos los usuarios de la familia que utilicen estas redes sociales (si son otras, la mayoría ya tienen opciones parecidas y no te costará hacerlo tras saber cómo se realiza en esta). Además recibir recordatorios, cumpleaños o sugerencias de amistad de alguien fallecido, como te

puedes imaginar tampoco es agradable.

Pues hagamos de nuevo testamento en cinco minutos, gratis y sin pasar por el notario (ya tendríamos Google y Facebook, solo nos quedaría Apple):

1.- Dentro de tu perfil de Facebook buscarás los tres puntitos (todo comienza siempre por aquí). Ya sabes justo a la derecha de la opción: **<Ver más>**.

2.- Una vez que hagas clic en los tres puntitos, la última opción es: **<Configuración de perfil y etiquetado>.**

3.- Tras entrar en esa opción, aparece la de **<Configuración>**. La primera opción será **<General>.**

4.- Y ya hemos llegado. Como puedes observar dentro de la Configuración General de la Cuenta, tienes una opción que se llama: **<Configuración de cuenta conmemorativa>.**

Esta opción es explicada por Facebook diciendo: que es el lugar para que decidas qué quieres que ocurra con tu perfil principal de Facebook cuando fallezcas. Facebook lo llama **Contacto de Legado.**

5.- Tan sólo tendrás que darle a editar y señalar la persona que **quieres que sea tu heredero (contacto de legado).**

Facebook te pone como requisito que tiene que ser tu amigo en esta red y mayor de edad.

Tu contacto de legado (tu heredero) seguramente te pregunte (tendrás que hablarlo antes con él) qué implica esto, hazlo antes de designarlo. Ahora lo vemos. Una vez lo nombres como heredero, Facebook se lo va a notificar con este mensaje:

"Hola, ….: Ahora Facebook permite a las personas elegir un contacto de legado que administre su cuenta si le ocurre algo:

https://www.facebook.com/help/1568013990080948

"Te he elegido porque me conoces bien y confío en ti. Ponte en

contacto conmigo si quieres hablar de este tema".

Es algo muy frío, para una persona puede tener una importancia tan grande en tu vida. Escribe algo desde el corazón. Dile porque cuando leíste esta parte del libro fue la primera persona que te vino a la mente, porque le tienes confianza plena y que no podría existir otra persona mejor para hacer esto.

Pero recuerda, háblalo antes de que reciba el mensaje. Porque sino va a ser unos de los Messenger más raros que reciba en su vida.

No te lo he dicho pero también podrías decidir que tu cuenta se elimine y nadie conserve nada, igual que con Google. En cuanto Facebook tenga conocimiento de tu fallecimiento ejercerá tu última voluntad, y lo eliminará todo.

¿Qué implica ser tu contacto de legado (heredero)?

Esa pregunta te la va a hacer la persona que quieras que sea tu legado (heredero). Deberás explicarle qué significa esto y por qué lo has escogido. Lo importante que es esto, puedes utilizar el ejemplo que yo te he puesto o cualquier otro que se te ocurra. Como contacto de legado existen cosas que no podrá hacer (tal y como nos indica Facebook):

- Seguir aceptando amigos y eliminando amigos.
- Entrar en tu cuenta, como si fueras tú.
- Leer los mensajes.

Pero sí podrá (y esto es lo importante):

- Fijar una publicación en tu perfil, con la fecha del funeral o un último mensaje de despedida por ejemplo.
- Decidir quién puede ver y publicar homenajes, en caso de que se haya establecido un apartado en la cuenta conmemorativa para ello.
- Actualizar foto de perfil y portada.

- Solicitar la eliminación de la cuenta.
- Descargar una copia de tu vida en Facebook, pero con ciertos límites.

Esto es importante, es uno de los motivos por los que hacemos el nombramiento de un heredero (contacto de legado) en Facebook**,** por lo que no olvides marcar la casilla que nos dice que: *"permitir a mi contacto de legado una copia de lo que he compartido en Facebook. El contenido descargado incluirá publicaciones, fotos, vídeos y datos de la sección "información" de mi perfil, que pueda ser contenido que originalmente no era visible para tu contacto de legado. No se incluirán los mensajes".*

En Instagram tendrás que hacerlo a través del siguiente enlace:

https://help.instagram.com/contact/1474899482730688?helpref=faq_content&fbclid=IwAR1q3BhNXwKMyiB9nxkxdUnCafnjVDI0nxbmkfpmwiA9Ngn4rygIPTOHnxI

(No te preocupes, al final del libro en la sección de enlaces te dejo código QR. Igualmente lo encuentras si pones en Google: "Solicitud de eliminación de persona fallecida en Instagram)".

HOJA DE RUTA 6.- CHECK LIST: NOMBRANDO HEREDERO EN FACEBOOK

“ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ”

CHECK LIST: NOMBRANDO HEREDERO EN FACEBOOK

PERSONA QUE REALIZA EL TESTAMENTO:	

RUTA PARA NOMBRAR HEREDERO	... - Configuración de Perfil y Etiquetado - Configuración - General - Configuración de Cuenta Conmemorativa
PERSONA QUE SE DESIGNA HEREDERO (recuerda que tiene que ser mayor de edad y amigo tuyo en Facebook)	Correo electrónico
MENSAJE QUE RECIBIRÁ, que sea cariñoso :)	

Llamada explicando qué significa esto	SÍ	
	NO	
Copia de seguridad	SÍ	
¿Debe cambiar foto de perfil?		
¿Quiere que se publique un último mensaje?		

6.3.- DESCARGAR UNA COPIA DE TODO LO QUE EL MUNDO FACEBOOK SABE DE MÍ

Descargar una copia de seguridad de Facebook y su mundo de forma periódica, es igual que llevar una rueda de repuesto en el coche. No tendremos que recurrir a ella frecuentemente, pero cuando sea necesario nos salvará de un problema importante. Ya lo vimos en Google, ahora toca Facebook. Aunque todas las redes sociales suelen tener una opción parecida a esta.

Donde encontramos esa opción:

1.- Pues ya sabes, todo comienza por los tres puntitos, en tu perfil.

2.- Una vez que hagas clic en los tres puntitos, la última opción es: **<Configuración de perfil y etiquetado>.**

3.- Tras entrar en esa opción, aparece la de **<Configuración>.**

4.- Ahora busca: **<Tu información de Facebook>.**

5.- Dentro encontramos la que estamos buscando: **<Descargar tu información>.**

6.- Primero escoge el formato de archivo: **Html y Json.**

El primero te será más fácil de visualizar, el segundo más fácil de importar si fueras a importarlo a otra aplicación.

7.- La calidad del contenido multimedia.

Decide si lo quieres **con calidad alta, media o baja.** Como te puedes imaginar esto afectará al tamaño del archivo.

8.- **Selecciona el intervalo de fechas** que quieres. Estas son las opciones: la semana pasada, el mes pasado, últimos 3 meses, últimos 6 meses, el año pasado, últimos 3 años, desde el principio o personalizar).

9.- Por último, **escoge de tu archivador personal qu**é **cajones y qu**é **separadores quieres descargar**:

- Tu actividad en Facebook
- Información Personal
- Conexiones
- Información Registrada
- Información de inicio de sesión y seguridad
- Aplicaciones y sitios web fuera de Facebook
- Preferencias
- Información sobre anuncios

Ahora paciencia. Déjale un tiempo, sobre todo dependiendo del intervalo que hayas escogido y del rango de fechas. Será en esta misma página donde tendrás la opción de descarga, en una pestaña adicional llamada: **<Archivos Disponibles>**. Pero ojo, no estará disponible indefinidamente, sino tan solo unos días.

HOJA DE RUTA 7.- CHECK LIST: DESCARGAR UNA COPIA DE TU VIDA EN FACEBOOK

“ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ”

CHECK LIST: DESCARGAR UNA COPIA DE TU VIDA EN FACEBOOK

RUTA PARA DESCARGAR UNA COPIA DE TU VIDA	**... - Configuración de perfil y etiquetado- configuración - tu información de facebook - descargando tu información**

FORMATO DEL ARCHIVO	**HTML**	
	JSON	

CALIDAD DE LA IMÁGEN	**BAJA**	
	MEDIA	
	ALTA	

INTÉRVALO DE FECHAS	**La semana pasada**	
	El mes pasado	
	Últimos 3 meses	
	Últimos 6 meses	
	El año pasado	
	Últimos 3 años	
	Desde el principio	
	Personalizar	

ESCOGE CAJONES Y SEPARADORES		
	Tu actividad en facebook	
	Información personal	
	Conexiones	
	Información registrada	
	Información de inicio de sesión y seguridad	
	Aplicaciones y sitios web fuera de facebook	
	Preferencias	
	Información sobre anuncios	

6.4.- COMPRA DE SEGUIDORES, COMENTARIOS Y RESEÑAS. MANIPULACIÓN O INFLUENCIA

Piensa en alguien que de verdad admires. Puede ser un actor, cantante, influencer, escritor, etc… ¿Tiene redes sociales? La mayoría las tendrá. ¿Cuántos seguidores tiene? Ya lo has mirado.

¿Cuántos son de verdad?

Venga ya Iván, ¿me quieres decir que cualquiera de las personas que admiro es posible que haya comprado seguidores? Justamente eso te quiero decir.

Pero antes, vamos a plantearnos cómo ven nuestros peques las redes sociales. Para ellos es un territorio de veracidad. Que algo aparezca en redes o lo diga el influencer o youtuber de turno, es sinónimo de que es verdad absoluta, no es discutible. A mí me han llegado a decir en algunas charlas que solo se creen lo que dicen sus padres o profesores, cuando lo chequean con lo que dicen las personas que siguen en internet. Flipa. ¿Pero qué ocurriría si le enseñamos lo sencillo que es manipular esto? Lo fácil que puede ser comprar seguidores, comentarios o reseñas, y cómo funciona ese mundo. Haremos que reflexionen más la próxima vez, los haremos personas críticas y que duden de sus gurús. Ese es el objetivo de este apartado.

Cuando termines de leer estas páginas, lo importante no será el ranking de los más seguidos, sino el ranking de los "realmente" más seguidos.

Por cierto, esto no se aplica solo a nuestros peques sino que los adultos no somos mucho más listos. Te voy a contar un caso real.

Hace no mucho, un señor visitó un restaurante de Málaga. Se presentó como un gurú en marketing digital, un avanzado a su época. Tenía el secreto para hacer que ese restaurante, a pesar de

llevar abierto solo unos meses, pudiera tener más seguidores que algunos de los restaurantes más conocidos de la ciudad. El dueño del restaurante lo miró con desconfianza. Pero en ese momento el gurú hizo su oferta (lo tenía todo bien preparado): "Te prometo 200 seguidores nuevos cada día, y en menos de un mes serás uno de los restaurantes más seguidos de Málaga. Ahora no me pagarás nada, y cada semana vendré a verte y me pagarás 800 euros cuando confirmes que es así. Al mes, cuando seas uno de los restaurantes más seguidos de Málaga me pagarás 3.000 euros más".

El dueño del restaurante pensó que no tenía nada que perder, solo pagaría cuando viera el crecimiento de los seguidores, 200 seguidores nuevos cada día implican muchas reservas. Eso compensa de sobra lo que tendría que pagar. Dijo que sí.

Pasó la primera semana, el dueño del restaurante no podía creer cómo estaba creciendo su cuenta, todavía no habían aumentado mucho las reservas, pero era cuestión de tiempo. Estaba feliz, por lo que recomendó el gurú a varios negocios más, en diferentes localidades. En pocas semanas todo el mundo de la restauración conoce al gurú, y quería trabajar con él. Todo iba bien, hasta que un día la cuenta de la red social del restaurante fue suspendida temporalmente por infringir las normas de uso de la red social. De golpe perdió todos los seguidores que habían llegado.

El dueño del restaurante pensó en un primer momento que se trataba de un error. Intentó contactar con el gurú, pero este ya no cogió el teléfono, era raro. Insistió, pero había desaparecido. Eso sí, desapareció con los bolsillos llenos. Se cambió de zona y me imagino que seguirá haciendo lo mismo a día de hoy. Lo único que hacía este gurú era comprar seguidores y reseñas.

Comprar seguidores, reseñas o comentarios, es uno de los caballos de batalla de las redes sociales. Todas lo prohíben en sus términos y condiciones. Recuerda que las redes sociales viven de la publicidad y para que la gente contrate publicidad tiene que darle credibilidad a la misma. Las cuentas falsas no ayudan en nada a esto.

Sin entrar al daño que esto puede hacer a tu marca, y a que te expones a una suspensión temporal o permanente de tu cuenta, está el debate antiguo de si es mejor cantidad o calidad. Y si la cantidad ayuda a vender más.

Actualmente existe una profesión que consiste en ser seguidor de redes sociales, o dejar comentarios o reseñas. En este caso ya no son cuentas falsas, sino personas reales que a cambio de una cantidad de dinero ofrecen estos servicios. Incluso existen plataformas que los agrupan. Para la red social perseguir estos casos (que siguen infringiendo sus términos y condiciones) se hace más difícil, porque en este caso son personas reales.

He realizado una búsqueda en Google: **"comprar seguidores"**. Estas son algunas de las ofertas que he encontrado en la primera página. En la mayoría me dan la opción de segmentar por países a los seguidores, lo que hace que el precio varíe. También puedo decidir si los quiero recibir en bloque o unos poquitos cada día. Veamos estas ofertas:

- La primera opción me ofrece **1.000 seguidores de Instagram por 9,99 euros.**
- La segunda opción me ofrece 100 seguidores en Instagram **por 4,20 euros**, 100 likes en TikTok **por 2,50 euros**, o 250 suscriptores en Youtube por **30 Euros.**
- También existen packs: tengo uno básico por **12,99 euros** que incluye 500 seguidores y 500 likes en tu perfil de Instagram. O el profesional: que **por 44,99 Euros** me ofrecen 2.500 seguidores y 2.500 likes.

Creo que ya te puedes hacer una idea de cómo funciona el tema. Puedes aumentar la información si buscas en Google: Granjas de Clicks.

Ahora vamos rizar el rizo, para colmo existen personas que compran seguidores a la competencia.

En la mayoría de estas páginas que os comentaba para comprar seguidores solo te piden el perfil, por lo que cualquiera puede hacerlo. Y una vez que lo han comprado para la competencia, denuncian el perfil a la red social para que chequee que son falsos y suspenda o cierre la cuenta. En fin, buena gente (modo ironía on).

Las redes sociales intentan limitar estos comentarios falsos, incluso han intentado valorar más los comentarios geolocalizados. Es decir, el comentario que haces sobre un restaurante se valora más si se geoposiciona. Se sabe que has estado en el restaurante. Pero como la creatividad humana no tiene límites, no han faltado las compañías que tienen a personas en motocicleta parándose delante de los restaurantes, y realizando comentarios. Así el algoritmo no pueda diferenciarlo de los comentarios reales.

Necesito que le acerques este mundo a tus hijos, y para eso vamos a ser: detectives de seguidores falsos.

Vamos a seguir una metodología sencilla para ello:

1.- Revisa unos cuantos seguidores de ese perfil, si tiene muchos seguidores **sin fotografía en su perfil desconfía**, estos suelen ser falsos.

2.- **Revisa algunos comentarios**. Algunos pueden no tener ningún sentido. Otra señal.

3.- Otras veces es muy evidente, porque entre los seguidores del perfil están **cuentas de compra de seguidores.**

4.- Escoge **cinco o diez seguidores con nombres que te parezcan curiosos**, y revisa sus biografías, esto te dará una pista clara.

5.- Utiliza herramientas como Hootsuite (para ver el crecimiento por meses de la cuenta, unos picos de crecimiento son sospechosos) o Hypeauditor (dónde te dará la calidad de la audiencia de ese perfil).

6.- No tiene sentido que una cuenta tenga más de un millón de seguidores, suba una fotografía y tenga 500 likes. Esto no es creíble.

¿Cómo analizamos la influencia real de la cuenta sobre sus seguidores? Para de esta forma saber si tiene muchos falsos o no. Fácil.

Cogeremos las últimas diez fotografías, y sacaremos la media de "me gusta". Ese número lo dividiremos por el número total de seguidores. Después lo multiplicaremos por 100. **Eso nos dará el Ratio de Influencia.**

Para que te hagas una idea (estos números se van actualizando): si la cuenta tiene menos de **1.000 seguidores, un ratio de un 8%** de "me gusta" o más está correcto. Si tiene entre 1.000 y 10.000 seguidores, un ratio de un **4%** de "me gusta" o más es correcto. Está entre 10.000 y 1.000.000, un **2%** de "me gusta" o más es correcto. Y por último, más de 1.000.000 un **1,5%** o más.

Ahora toca ponerlo en práctica. Comenta con tu hijo lo sencillo que es comprar seguidores, comentarios y reseñas en internet. Enséñaselo con una búsqueda en Google. Tras esto, pídele que te diga el primer cantante que se le ocurra, el primer actor, el primer deportista y el primer youtuber. Y tras esto, realizar el análisis que hemos visto sobre su cuenta y sacar conclusiones. Suerte y espero que no se lleve muchas decepciones.

Te dejo como siempre un modelo para que te sea más fácil hacerlo. Si necesitas más, ya sabes dónde encontrarlos. ¡Vamos, detectives!

HOJA DE RUTA 8.- CHECK LIST: DETECTIVE DE SEGUIDORES FALSOS

“ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ”

LA PRUEBA FINAL	Media de los me gusta de las últimas diez fotografías o publicaciones	Media de los me gusta dividido por el número de seguidores	Ratio influencia (multiplica el número anterior x 100)

INTERPRETACIÓN DEL RATIO DE INFLUENCIA (% HABITUALES)

Menos de 1000 seguidores	8% o +
Entre 1000 y 10000 seguidores	4% o +
Entre 10.000 y 1.000.000 seguidores	2% o +
Más de 1.000.000 seguidores	1,5% o +

CONCLUSIONES DEL DETECTIVE DE SEGUIDORES FALSOS	SI TIENE SEGUIDORES FALSOS		NO TIENE SEGUIDORES FALSOS	

6.5.- RETOS VIRALES (CHALLENGE) Y CONFIGURACIÓN DE LA PRIVACIDAD

La mayoría de los retos que se convierten en virales son divertidos e inofensivos. Pero tenemos que hablar de un término que quiero que conozcas: la tiranía del like. El intentar encajar con tu grupo de amigos, parecer guay (no sé si se sigue diciendo esta expresión, jeje), provoca que puedan llegar a realizar retos virales muy peligrosos para su salud.

Antes de contarte alguno de los peligrosos, debo advertirte que esto cambia constantemente y son como tormentas que descargan, pasando a continuación de largo. Por lo que no tiene mucho sentido hacer una recopilación de los actuales, porque seguramente cuando leas esto ya tengamos otros en marcha (aun así te contaré alguno para que reflexionemos juntos).

Por lo que prefiero que hablemos, de qué podemos hacer para prevenirlos:

- Parece de sentido común, pero lo primero es hablar con ellos. Que tengan la confianza para hablar contigo de este tipo de retos virales y de cualquier desafío o curiosidad que encuentren por internet. Siguiendo los ejercicios de este libro, ya estáis creando esa confianza.
- **Controlar**. De nuevo, esa palabra que parece tabú para los padres. Sí, nos toca estar pendientes, supervisar, ayudar, pero nunca y digo nunca, desconectarnos. Con este libro y los siguientes que vendrán no podrás hacerlo, esa es mi misión.
- **Configurar adecuadamente la privacidad de las diferentes redes sociales**. En un segundo te pongo el enlace de todas ellas.
- **Seguir cuentas de redes sociales que nos mantendrán actualizados**, en España por ejemplo: OSI (Oficina de

Seguridad del Internauta), INCIBE (Instituto Nacional de Ciberseguridad), Grupo de Delitos Telemáticos de la Guardia Civil. Nosotros también podemos ayudar tanto en la cuenta de mi despacho: Privacidad Global, como en la cuenta: Método Canguro Digital.

La red social estrella para viralizar contenidos es Tik Tok. Es una red social que literalmente ha explotado en su crecimiento. Nació para ser un lugar donde realizar karaoke, cantar e imitar las coreografías de sus cantantes favoritos, y eso ya dio algún problema a nivel de nuestros peques.

Imagínate unas niñas de 14 años realizando coreografías tan subidas de tono como las de Becky G por ejemplo, mientras cantan alguna de sus letras: *"A mí me gusta que me traten como dama. Aunque de eso se me olvide cuando estamos en la cama. A mí me gusta que me digan poesía. Al oído por la noche cuando hacemos groserías".* Pura poesía.

Este tipo de problemas y otros derivados con los contenidos no adecuados, llevó a que esta red social haya sido prohibida en diferentes países. Aun así, su crecimiento ya es imparable.

Hoy en día es mucho más que karaokes y coreografías. Es en esta red social donde nacen la mayoría de retos virales. Por lo que ya te puedes ir haciendo una cuenta. Pero Iván es que… No hay excusas, donde están tus hijos tienes que estar tú. Es así.

Quizás uno de los primeros retos peligrosos que saltó a la prensa fue Momo, una mujer con aspecto de la película del exorcista que iba marcando retos cada vez más peligrosos. Después llego la Ballena Azul, reto que incluía cortes en el brazo y en última instancia el suicidio. Actualmente tenemos retos virales que, como la moda, siempre acaban volviendo a la actualidad:

- **Reto de la canela**. Buscando el efecto: "el aliento del dragón". Consiste en tomarse una cucharada de canela en polvo, esto hacía que expulsaras las canela por la nariz y la

boca provocando irritaciones de garganta y problemas respiratorios.

- **Ice and salt Challenge.** Se trata de poner sal en la piel, para luego presionarla con hielo. Esto hace que se produzca una reacción química que provoca quemaduras.
- **Condom Challenge.** En este caso introducen la cara dentro de un condón, como si fuera una bolsa de plástico. Puede provocar asfixias.

La estupidez humana no tiene límites. Y no se trata de ser moralista, sino de pensar en lo que es capaz de hacer una persona por sentirse integrado. La presión de tus supuestos amigos, puede acabar provocando daños o incluso la muerte. Es imposible ponerse en la piel de unos padres que han perdido a su hijo porque este estaba saltando de un balcón a una piscina. Y lo han perdido por solo unos likes, o simplemente porque varias personas que no llegan a la inteligencia de un primate le puedan decir algo bonito.

Actualmente, tenemos retos virales como los siguientes (pero ya te digo que cuando leas esto, la estupidez humana habrá dado un paso más):

- **Caza del pijo.** Consiste en agredir a jóvenes que ellos califican como "pijos", grabarlo en vídeo y subir las imágenes a redes sociales.
- **Lamer tapas de váter**. Ni lo comento.
- **Rompe Bocas.** Alguien se acerca por detrás para hacerle la zancadilla, o te envuelven los tobillos con cualquier prenda. El objetivo es que te caigas de boca mientras otro lo graba.
- **Tide Pod Challenge**. Comer, cocinar o morder cápsulas de detergente como si fueran dulces.
- **The Shell Challenge**. Comer cualquier alimento con su propio envoltorio o cáscara. Creo que no han entendido lo de comer más fibra.

Además de lo que hemos comentado anteriormente. Recuerda (es importante) que ya explicamos el canal prioritario, del que dispone la Agencia Española de Protección de Datos para retirar este tipo de contenidos. Vuelve a revisar esa parte por favor. Además de eso, la propia Agencia Española de Protección de Datos dentro del proyecto educativo denominado: "Protege tus datos en internet", tiene videotutoriales en los que explica paso a paso cómo configurar las opciones de privacidad de las redes sociales más comunes: Facebook, Twitter, Instagram y Tik Tok.

Videotutoriales de la Agencia Española de Protección de Datos para configurar la privacidad:

https://www.aepd.es/es/guias-y-herramientas/videos

Con esto, terminamos el capítulo de redes sociales. Se podría profundizar en más cosas, pero creo sinceramente que esto es lo más importante que tienes que dominar para poder protegerte tú y proteger a tus hijos.

Ahora vamos con los móviles. ¿Me acompañas? Siguiente capítulo.

¿qué sabe tu Móvil de ti y de tu hijo?

7.- ¿QUÉ SABE TU MÓVIL DE TI Y DE TU HIJO?

Cada vez que visito a un cliente me ocurre igual. Le pregunto: ¿cuál es tu antivirus? Una pregunta inocente, ¿verdad? Y me responden con el antivirus del ordenador de sobremesa o con el ordenador portátil. A continuación, les digo que lo que necesito es el antivirus del móvil.

Cara del gato de Shrek. Cuando reaccionan, lo primero que me dicen es que no sabían que existen antivirus para el móvil. Me toca explicarles que la mayoría de los ataques de los malos, están centrados en los móviles. Es lógico. Los móviles ya no son móviles, son ordenadores. Mucho más potentes que los que yo tenía no hace mucho tiempo. En el móvil encontramos tu correo electrónico, tus aplicaciones del banco, Whatsapp, contactos, fotografías (y ya sabes qué significa eso, si no lo recuerdas revisa el capítulo de los metadatos), etc… es decir, tu vida, y eso que todavía no te he contado qué sabe tu móvil de ti. En marcha.

Para comenzar te vas a bajar una aplicación (si tienes Android) llamada: Conan Mobile, es una maravilla. Es una aplicación gratuita. Sí, ya sé que estás pensando que si es gratis, el producto eres tú. Buen alumno. Pero en este caso, es una aplicación desarrollada dentro de un proyecto europeo por parte de Incibe (Instituto Nacional de Ciberseguridad), por lo que ya la hemos pagado indirectamente con nuestros impuestos.

Conan Mobile, es una auditor/antivirus que va a realizar una comprobación integral de tu smartphone y tableta. Es una pasada, ah que eso ya lo había dicho. Obligatoria para nuestros móviles y los de nuestros hijos. Te hará una auditoría de tu configuración y de los riesgos de seguridad que puedes tener. Seguirá por las aplicaciones y sus permisos (y en este capítulo hablaremos más de eso). Y te alertará de comportamientos anómalos y potencialmente peligrosos.

¡Guau!

Ya tienes tarea, descargar Conan Mobile y revisar sus conclusiones para todos los móviles Android de la familia. Vale ya sé lo que estás pensando. Pero bueno Iván, esto es solo para Android. ¿Qué ocurre con IOS (Iphone)? La verdad es que acabarán desarrollando también una versión para IOS, pero lo cierto es que existen más riesgos para Android, luego te cuento el motivo.

Tras esto, vamos por la segunda tarea. ¿Tienes apuntado el NIF de tu móvil?

¿Que no? Pues sigue leyendo.

7.1.- EL N.I.F. DE TU MÓVIL

Te van a robar el móvil.

No es que yo sea un cenizo, lo siento pero es pura estadística. A lo largo de nuestra vida nos van a robar el móvil al menos una vez. Si esto va a ocurrir: ¿qué precauciones tienes que tener?

Pues varias que te voy a contar en este capítulo. Pero la primera sin duda es saber el N.I.F. de tu teléfono.

¿Para qué sirve el N.I.F. del teléfono? ¿Existe uno por país? ¿Dónde lo miro? ¿Eso cambia? ¿A qué huelen las nubes? Ah no, esa pregunta era de otro libro, jeje.

Como me imagino que quieres saber la respuesta a todas estas preguntas, vamos a por ellas.

¿Qué es el código IMEI (conocido como el N.I.F. del teléfono)?

El código IMEI (International Mobile Equipment Identity) es un código de 15 cifras único en el mundo, no existe otro teléfono que tenga la misma numeración que el tuyo. No depende de tu país, como sí lo hacen los documentos nacionales de identidad.

El IMEI está normalizado por EGPP, que agrupa a todas las asociaciones de telecomunicaciones del mundo. Y ya a título de curiosidad, te diré que estas 15 cifras identifican la marca, modelo y operadora, casi nada.

En realidad de esas 15 cifras, las seis primeras cifras entre otras cosas identifican el país de fabricación del móvil. La cifra 7 y 8, identifican al fabricante. De los números 9 al 14, identifican el número de serie del móvil. Y el último número es un validador, que confirma que el IMEI es correcto.

Vale Iván, esto es interesante, ¿pero para qué me puede servir a mí?

¿Recuerdas lo que te acabo de decir, que en algún momento te van a robar el móvil? Incluso podrían suplantar tu tarjeta SIM y hacer un

duplicado, pudiendo suplantar tu identidad. También te podría pasar como le ocurrió a Richelle.

A Richelle le prepararon una cita a ciegas sus amigas, en principio no le pareció buena idea, pero sin saber por qué aceptó. En esa cita conoció a Eliot. Le pareció un buen chico, por lo que quedaron varias veces más para salir. Efectivamente Eliot era un buen chico, pero no había conexión y ambos decidieron seguir como amigos.

De vuelta a casa, Richelle pensó que de aquella cita a ciegas no había salido una pareja pero sí un buen amigo, no estaba mal. Al día siguiente de esa decisión: Richelle tenía 100 llamadas perdidas de Eliot. Esto no era normal. Llamó a Eliot y le pidió explicaciones, le salió del corazón hacerlo así porque no le había parecido ese tipo de chico.

Eliot le prometió que él no había llamado ni una sola vez, Richelle dudó, pero al día siguiente volvieron las 100 llamadas. Richelle perdió la confianza, su número estaba en el móvil, no había error posible. Esto era insoportable. Richelle volvió a llamar a Eliot, esta vez muy enfadada. Él seguía diciendo lo mismo. No sabe por qué, pero Richelle en ese momento le creyó. Entonces, ¿cómo era posible esto?

Decidieron acudir juntos a la comisaría más cercana, esto ya no tenía sentido. En la misma, tras realizar algunas indagaciones, le explicaron que cuando dos teléfonos se llaman entre sí transmiten el número y el código IMEI, por lo que se podría saber si esas llamadas salieron del móvil de Eliot.

Justo así fue. El número era el de Eliot, pero no tenían el código IMEI. Seguramente esto se debía a que alguien estaba utilizando un software que imita su número de teléfono, pero que no podía imitar el código IMEI. Suerte que Richelle creyó en este caso a Eliot, sino hubiera estado en un serio problema.

El código IMEI sirve para evitar estas suplantaciones, pero también para cuando te roban el teléfono y necesitas localizarlo o bloquearlo.

Si te lo roban y llamas a tu operadora con el código IMEI, tu móvil pasará a ser un bonito pisapapeles. No podrán utilizarlo para hacerte daño. En la denuncia que pongas, no será importante ni la marca ni el número de teléfono, lo que necesitará la policía será el código IMEI. Recuerda esto cuando llegue el momento.

Me has convencido Iván. ¿Cómo lo miro? ¿Y ese número cambia?

Empecemos por la segunda pregunta. Ese número es único y no va a cambiar nunca para tu móvil. Y en cuanto a la primera pregunta. Tienes cuatro formas de mirarlo, te adelanto que mi preferida es la última. Veamos todas las opciones:

1.- Mirar la caja del móvil. Ahora mismo te estás preguntando dónde la has dejado. Te cuento un secreto, existe un gran agujero negro que engulle las cajas de los móviles, por lo que no te preocupes. Pero si acabas de comprar el móvil y la tienes localizada, en la caja aparecerá. Si el móvil permite tener dos ranuras para tarjetas, tendrás que apuntar ambos números porque tendrás dos códigos IMEI.

2.- Si tu móvil te permite quitar la batería. Debajo de la misma encontrarás también el código IMEI. Suerte porque esto es poco probable. Eso me recuerda, aunque me vaya a otra cosa (ya llevamos un tiempo juntos y sé que me lo permites), que el hecho de no quitar la batería puede comprometer la información del teléfono y de los que están a su alrededor. Te lo digo más claro, es posible extraer información de un teléfono apagado si tiene la batería puesta. Flipa. De ahí que el muchacho que se llevó unos cuantos documentos (modo ironía on) el señor Edward Snowden, cuando quería tener total privacidad dejaba su móvil en la nevera, para que funcionara como jaula de Faraday.

3.- Sigue la ruta:

Iphone. <Ajustes> - <General> - <Acerca de / Información>

Android. <Ajustes> - <Información del dispositivo>

4.- Pero como esto puede cambiar con cada móvil, mi opción

preferida es que te vayas al móvil y como si fueras a poner un número de teléfono para llamar, en el teclado pulses las siguientes teclas: ***#06#.** Y por arte de magia aparecerá el código IMEI. Este juego de teclas es universal por lo que funcionará en cualquier teléfono del mundo, esté en el idioma que esté.

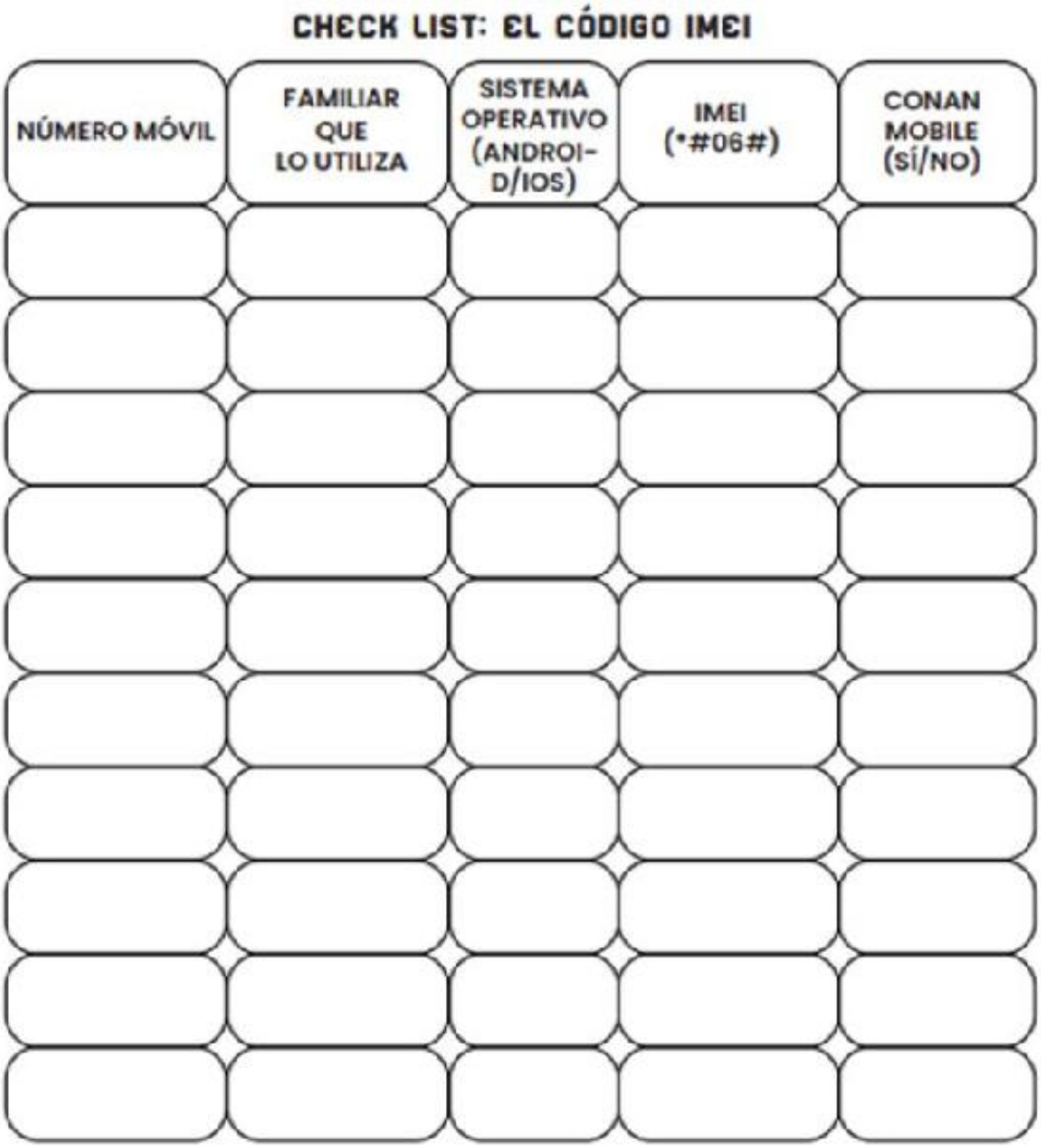
Ahora te toca lo más importante, apúntalo. Espera que lo repito. Apúntalo. Si no lo haces ahora, como si el destino conspirara contra ti cuando lo quieras buscar no lo encontrarás. La opción de llamar cuando te lo roben, y que se ponga el ladrón para pedirle que te lo mire, va a ser pelín complicada.

Ahora vamos a poner lo aprendido en práctica. Explicarás a tus hijos lo importante que es el código IMEI y la descarga de Conan Mobile.

Otra vez dándome deberes Iván. Ser unos padres digitales, unos auténticos Canguros Digitales no es fácil, pero tú puedes. Completa este documento con los móviles de la familia, ya sabes lo importante que es. Recuerda que a día de hoy Conan Mobile solo está para Android.

HOJA DE RUTA 9.- CHECK LIST: EL CÓDIGO IMEI

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"



7.2.- TU MÓVIL SABE DÓNDE VIVES Y CUÁNDO VAS AL SUPERMERCADO

¿Qué te parece no tener que pagar ninguna comida más con tus amigos? Para eso vamos a realizar un truco de magia, magia tecnológica claro. El truco consiste en adivinar qué hicieron alguno de tus amigos el miércoles pasado, hora de llegada al trabajo, supermercado, gimnasio, a tu casa o lo que sea que hagan un miércoles. También podríamos adivinar dónde estuvieron de vacaciones (el nombre del hotel incluso).

Todo esto lo sabe tu móvil. Esto y mucho más. Si tu móvil es Android, ya sabes que perteneces a Google, y tuvimos un capítulo completo para aprender a manejarnos por la parte privada de Google. Recuerda que en ese capítulo analizamos qué sabe Google de ti. Por tanto, si tienes Android tienes Gmail. Recuerda que todo eso lo encontrabas en: https://myactivity.google.com/.

Pero hasta este momento si eras usuario de Iphone, estabas muy tranquilo. Yo diría que hasta relajado, porque pensabas que al no estar logueado con Gmail en tu Iphone estabas a salvo de todo esto.

¿De verdad piensas que Apple no lo hace?

Por mucho que se esfuerce en su publicidad en transmitir las emociones de la seguridad y la privacidad (de vender saben un rato, eso está claro).

Por supuesto que lo hace, es cierto que la información es más reducida (al menos la que podemos ver). Y no podremos saber si llegaste por la ruta habitual o por una diferente, si llegas en coche o en bici y por último si hiciste alguna parada por el camino. Algo que con Google sí sabemos. Pero tu Iphone te dirá localidades, calles en las que estuviste, número de visitas y horario.

¿Dónde está eso? Fácil, sigue la siguiente ruta:

- **<Ajustes>** - **<Privacidad>** - **<Localización>** (si está sin activar Game Over) - **<Servicios del Sistema>** - **<Lugares importantes>.**

Como esta pestaña es importante y pelín comprometida, te volverá a pedir tu sistema de seguridad (pin, huella o reconocimiento). Mira lo que dice mi móvil, para que te hagas una idea: en mi caso estuve en Antequera, en la calle Fresca, el 12 de abril y el 7 de abril. El día 12 de abril llegué tras andar 6 minutos. Y el 7 de abril llegué tras conducir 32 minutos. El 12 de abril estuve de las 19:14 horas a las 19:49. Y el 7 de abril desde las 16:19 a las 18:32. Además me lo marca en un mapa.

El móvil te delata. Ese es uno de los motivos por los que la policía siempre intenta localizar el móvil de los desaparecidos. Te cuento algo que me pasó.

En una de las charlas que yo daba (a estas alturas del libro, ya sabes que me han pasado muchas cosas en las charlas, por eso me encantan), solía sacar a alguien del público y le pedía permiso para revisar su teléfono. Era muy espectacular poder adivinar dónde vivía, a qué hora llegaba a trabajar o a qué restaurante suele ir.

Pero un buen día, nunca lo olvidaré, saqué a una persona y le dije que había estado en Nerja el día 14 de mayo. De repente noté que se le cambiaba la cara, miré donde estaba sentado y había una mujer mirándolo muy muy fijo. Fue un momento como las películas del oeste antes del duelo final. Él no dijo nada y empezó a ponerse de un color muy pálido. En ese momento solía decir dónde estuvo y las horas, no lo hice, cambié de tema y dejé caer que a veces esto tenía un margen de error (mentira cochina).

Luego con el tiempo supe que era su mujer, y que sin querer estaba revelando una infidelidad en público, algo que ya intuía ella pero que allí confirmó. Desde entonces, lo que hago es que sean las propias personas las que revisen su teléfono y comenten en voz alta lo que quieran. Sigue siendo chulo, pero desde luego es menos

espectacular.

En fin, creo que ya sabéis interpretar esta parte también. Y recordad que a esto se le puede añadir la información que tienen las fotografías de tu móvil, recordad la famosa ficha del libro (metadatos).

Tras todo lo que hemos explicado, tanto en este capítulo como en los capítulos anteriores, creo que eres consciente de la importancia que tiene tu móvil. Si además por estadística sabemos que en algún momento nos lo van a robar y por eso tenemos apuntado el código IMEI, no estaría mal aumentar la seguridad del mismo, más allá de que nos pida nuestra huella, cara o pin al arrancarlo.

Me parece bien Iván, ¿cómo lo protegemos?

Sigue estos pasos y protegerás tu móvil como un auténtico profesional.

1.- UTILIZA UNA CONTRASEÑA EN LAS APLICACIONES

Aquellas aplicaciones más importantes, vamos a hacer que nos vuelvan a pedir una verificación de seguridad (independientemente de las que nos puedan pedir dentro de ella), solo para poder abrirlas.

En Android depende del móvil, pero la ruta habitual es: **<Ajustes>** - **<Privacidad y Seguridad>** - **<Bloqueo de aplicaciones>.**

En Iphone, es un poco más complejo:

- Dentro de **<Ajustes>**, deberás buscar la **<Opción Tiempo de Uso>.**
- Antes de decidir qué aplicaciones son las más sensibles, para bloquearlas, deberás poner una contraseña en la opción: **<Usar código para Tiempo de Uso>**. Acuérdate de poner una contraseña segura, tendrás que confirmar.
- Ya estamos preparados para bloquear aplicaciones. Busca aquellas que creas más sensibles: bancos, correo electrónico,

mensajería instantánea, etc… Una vez localizada, haz clic en el **círculo a la izquierda y pulsa siguiente.**

- Ahora establece el límite de tiempo: **por ejemplo 5 minutos**. Tras pasar ese tiempo verás como la aplicación aparece como apagada, con un reloj de arena.
- Tras esto, si necesitas utilizarla más tiempo puedes añadir un tiempo adicional, pero deberás volver a poner la contraseña que estableciste.

2.- UTILIZA LA VERIFICACIÓN EN DOS PASOS (2FA): GOOGLE AUTHENTICATOR

En todas las aplicaciones que nos permitan tener un doble factor de identificación, vamos a activarlo. Es uno de los métodos más seguros que existen. Estarás acostumbrado a que cuando ejecutas una operación en tu banco, te llegue un código por SMS. Eso es una verificación en dos pasos. Pero el SMS no es el mejor sistema posible, nosotros vamos a utilizar Google Authenticator.

Esta aplicación creada por Google (de ahí el nombre), nos proporciona códigos de seis cifras, que te serán solicitados por las aplicaciones una vez introduzcas tu usuario y contraseña. Estos códigos cambian cada 30 segundos, y son totalmente aleatorios. Esta aplicación funciona para IOS y Android. Parece un poco de película de detectives, jeje, códigos que cambian cada 30 segundos. Pero es una maravilla, hazme caso.

Una vez instalas la aplicación, no deja de ser un llavero donde puedes tener diferentes llaves. Primero te descargas el llavero, la aplicación de Google Authenticator. Y después puedes ir configurando (añadiendo) diferentes llaves. Eso quiere decir que cada aplicación que le configure el doble factor de verificación, tendrá sus propias claves que cambian cada 30 segundos. Te parece raro, no lo es. Tú tienes llaves diferentes en el mismo llavero: las de tu casa, el garaje, el coche, etc… pues esto es lo mismo. Hagamos dos ejemplos y así lo veras más sencillo. Vamos a configurar dentro

de Google Authenticator dos llaves diferentes: la llave de Facebook y la de Amazon. En cuanto lo hagamos, para entrar a Facebook o Amazon ya no bastará el usuario y contraseña, sino que tendrás que añadir también el código que te dará Google Authenticator. En marcha.

FACEBOOK

- Ya sabes que todo lo importante en Facebook comienza por los tres puntitos. Tras esto, ve a la última opción: **<Configuración de perfil y etiquetado>.**
- En la izquierda, tendrás un menú. Busca la segunda opción: **<Seguridad e inicio de sesión>**.
- Aquí encontrarás la opción de: **<Autentificación en dos pasos>.**
- La primera opción que te permite, es usar una aplicación de autentificación.
- Cuando le hagas clic a esa opción aparecerán dos cosas: **un código QR y un código numérico.**
- **Importante, es muy importante.** He dicho que es importante. Pues eso, que a este código QR y al código en letras y números tienes que hacerle una captura de pantalla. Guárdalo en un lugar seguro. Si algún día te roban el teléfono (que lo harán), aunque la persona tuviera tu usuario y contraseña necesitará estos códigos (que no los tendrá).
- Igualmente puede que tengas que volver a instalarlo en otro móvil y necesitarás volver a instalar el llavero (Google Authenticator) y todas las llaves (en este caso la de Facebook), por lo que necesitarás este código QR o el código numérico.
- Tras esto, solo nos queda añadir esta llave a nuestro llavero, ve a tu aplicación de **Google Authenticator y dale al signo de más.** A continuación te dará las opciones de

escanear el código QR o introducir la clave de configuración. Listo.

Ya tienes tu primera llave en el llavero, felicidades.

AMAZON

- Dentro de Amazon tendrás que acudir a la pestaña que está situada arriba a la derecha: **<Cuenta y listas>.**
- La primera opción será: **<Mi cuenta>.**
- Tras esto buscaremos la opción: **<Inicio de Sesión y Seguridad>.**
- Y una de las opciones será: **<Configuración de la verificación en dos pasos (2SV)>.**
- Tendrás que editar la opción que tienes registrada (si es que tienes alguna, habitualmente está el móvil). Como puedes leer te dará la opción de añadir un nuevo teléfono o app de verificación. Esa es la opción correcta.
- Tras esto aparecerá **el código QR**. No olvides realizar una captura y guardarlo en un lugar seguro. Cuando lo escanees se te añadirá otra llave del llavero, está con el nombre de Amazon. A continuación verás que ya te está generando códigos diferentes a los de la llave anterior, que era Facebook.
- **Añade el código actual en el último recuadro**, y ya hemos configurado la doble verificación también en Amazon.

Ya no tienes excusa. Debes añadir una capa de protección a aquellas aplicaciones más importantes, haz que crezca tu llavero y el de tus hijos.

Por cierto, puedes realizar una exportación completa de tu Google Authenticator por seguridad a otro móvil. Si tocas los tres puntitos (ya sé, no son creativos con esto, jeje), tendrás la opción de <Exportar Cuentas>. Podrás tener una copia de tu llavero y tus

llaves (nunca está mal esto) en otro equipo o móvil que tengas en casa y no utilices. Además, ya que estamos en los ajustes aprovecha y dentro habilita la opción de privacidad, así te pedirá que uses tu huella para abrir la aplicación. Olé tú, ánimo que puedes.

Se lo estamos poniendo difícil a los malos. Pues todavía podemos mejorar nuestra seguridad, para eso nos vamos a comprar un Condom.

Iván, creo que te has equivocado, has escrito Condom. Debes estar pensando eso. Pero está bien, sigue leyendo.

3.- CONDOM USB

Existen muchos tipos de pendrive. Permitidme que antes de hablaros del bueno (Condom), os hable de otro que no lo es tanto. Hablemos del USB Killer.

Recuerdo cómo te conocí. Estábamos en otoño. Un cliente mío me llamó para pasar a verlos por sus oficinas, algo raro había ocurrido, aunque no sabían cómo. Tras llegar me estaban esperando, muy raro todo. Me llevaron al departamento de administración donde trabajaban tres personas, y digo tres porque acababan de despedir a una de ellas. Lo curioso, es que el día siguiente a dejar de trabajar en la empresa, al intentar arrancar el ordenador este se apagó con un ruido muy raro. Y ya no arrancó. Estaba frito.

Pensé que esta misión era más para un informático que para un abogado friki y empollón como es mi caso, ¿que tenía que ver yo con la muerte de un ordenador? Pero el dueño, que además de cliente es amigo, algo intuía y por eso me llamó. Pasaba algo raro y quería saber el qué.

Entonces lo vi. Era un pendrive aparentemente normal, pero algo extraño. Le pregunté a los compañeros si ese pendrive era de la empresa. Me dijeron que no. Me confirmaron que era del trabajador despedido. Les recordé lo importante que era no insertar pendrive externos en ordenadores del trabajo, me pusieron cara de póquer,

no entendían de lo que les hablaba.

Así que fiel a mi forma de ser, les conté una historia que nos sucedió en mi despacho.

Por cierto, ¿se puede dentro de una historia contar otra? No lo sé. Y no tengo a ningún autor de guardia para preguntarle, así que vamos a intentarlo.

Les dije a esos trabajadores y al dueño de la empresa que estaba presente (ya que me había desplazado les iba a enseñar alguna cosa más, a través de esta historia), si conocían a la empresa X (aquí no puedo poner el nombre, sorry). Por supuesto todos la conocían, es una de las empresas más grandes de mi ciudad. Les conté que un día en un networking, conocí a uno de sus gerentes (ahora se dice CEO), tras una pequeña charla que di se me acercó, y me dijo que estaría bien que algún día trabajáramos juntos. Pero que lo veía difícil, porque su empresa era muy segura.

Esto para un abogado friki y digital como yo, es como si te tocaran las palmas. Así que no me quedó otra que bailar. Le pregunté si estaba seguro de que era segura. Me contestó sin dudarlo, que estaba 100% seguro, que gastan mucho dinero en software de seguridad anualmente (esto era medio farol). Volvía a tocarme las palmas. Con una sonrisa y la mirada fija, le propuse algo: "¿Si puedo comprometer vuestra seguridad en menos de 3 días me contratarías?".

La respuesta fue un apretón de manos. El trato estaba cerrado.

El motivo por el que sabía que podía hacerlo (en una negociación siempre hay que tener el máximo de información posible), era que tenía y tengo amigos que trabajan en esa empresa. Y jamás, y digo jamás, nadie les había explicado absolutamente nada de la seguridad en internet y en sus equipos. Por lo que sabía que el gerente de la empresa, no estaba entendiendo algo que es básico. La seguridad no es un tema de gastar dinero en software (por lo menos no solo eso). Esto es tan absurdo como pensar que por tener

un Ferrari llegarás antes en una carrera. El problema viene cuando el que tiene que conducirlo no tiene carnet.

Este era el caso. La seguridad en el ámbito digital, es una unión entre recursos y personas. Ambos se necesitan. En algún momento leí que una cadena es tan fuerte, como su eslabón más débil. Tenía claro que el eslabón más débil de esa empresa eran las personas. Y lo sabía seguro, mis amigos trabajan allí. Los siguientes pasos fueron sencillos.

Sabía que en esa empresa tienen turno partido, y que muchos trabajadores aprovechan el descanso para ir a un gimnasio que está cerca. ¿Pero Iván, cómo podrías saber eso? Tan solo tuve que buscar un poco en las redes sociales. Os habéis fijado que nos encanta subir fotografías dentro del gimnasio, haciendo posturitas.

El caso es que escogí tres víctimas. Los motivos no vienen al caso, pero tras analizar un poco sus redes sociales sabía que eran los correctos. Eran tres hombres (otro día os explico por qué). Dos llegaban al gimnasio en coche, y el tercero en moto. Esperé a que entraran. En ese momento me acerqué a la rueda de sus coches y su moto, dejando un pendrive a la vista y preparado para que una vez se insertara en el ordenador, pudiera comprometer su seguridad (sin hacer daño). Así le demostraría al gerente de la empresa que no era tan segura como él pensaba.

Al salir del gimnasio los tres recogieron el pendrive. En uno de ellos (por asegurarme) escribí fotos en Cancún. Dos de ellos, al llegar a su lugar de trabajo pincharon el pendrive. Premio. El tercero tardó diez minutos más, pero también lo hizo. Olé.

Recuerda esto, es más fácil hackear a una persona que a una máquina.

Existen muchas técnicas de ataque a las personas, se denominan ingeniería social (que es una palabra maravillosa, para decir que a alguien le han tomado el pelo). Entrar en estas técnicas, que deben ser transmitidas también a tus hijos, nos llevaría muy lejos. Prometo

hablarte más de esto en mi siguiente libro.

Volvamos a la historia original. Tras contarles esto, los tres me miraban fijamente, había comprendido esta parte y en el futuro serían más prudentes. Pero el caso del ordenador frito no parecía que tuviera que ver con esto. No era un virus o un malware, literalmente el ordenador había muerto. Yo tampoco entendía qué ocurría, para qué te voy a engañar. Les pedí llevarme el pendrive. Tenía que averiguar qué había ocurrido, ya era algo personal.

Tras acercarme a visitar a un amigo hacker (pero de los buenos), le conté lo que me había ocurrido. Al hacerlo noté cómo sus ojos se iluminaban. Conocía la respuesta. Me dijo que lo acompañara. En su guarida (que así lo llama él), abrió el pendrive y me explicó que dentro tenía unos condensadores de electricidad, que tras cargarse completamente soltaban una descarga que inutiliza el ordenador. En ese momento me dijo el nombre de este pendrive, nunca lo olvidaré: USB Killer.

Tras investigar más, encontré cosas curiosas sobre el mismo, como por ejemplo: que su precio es ridículo y que algunas webs lo venden, como el mejor regalo para tu expareja y tu exjefe. Las personas nunca dejarán de sorprenderme.

Pero si recuerdas el inicio, hablábamos de comprar un Condom. El Usb Condom, es un pendrive bueno. Muchas veces digo, que me he convertido en un yonki de enchufes y wifi, escojo una cafetería porque tiene un enchufe cerca y una buena wifi. Lo sé, soy un desastre. Después de eso preguntó qué puedo tomarme. Es triste. Pero teniendo en cuenta que mi maravilloso Iphone no es capaz de aguantar un día completo de batería, no me queda otra.

Asumo que esto nos pasa a muchos, lo que nos obliga a tener que cargar nuestros móviles: en lugares públicos, hoteles, restaurantes, estación de tren, aeropuerto, etc… Lugares donde no tenemos control de los enchufes.

¿Control de los enchufes? ¿Pero qué me estás contando Iván?

No sé si alguna vez te has parado a pensarlo, pero las carreteras tienen doble dirección. Pues vaya novedad, Iván. Espera, sigue leyendo. Mientras tú cargas tu móvil, alguien podría estar llevando tus datos, van por la misma carretera pero en sentido contrario. Ah.

Pero es que además hacer esto no es complicado. Tampoco es plan que te cuente cómo se hace, pero es fácil, créeme. Y no me vengas de nuevo con el cuento de para qué van a querer tus datos, eso ya lo hablamos en el capítulo cuarto, donde te expliqué cuánto valen en el mercado negro.

La pregunta debe ser: ¿cómo me protejo?

Y como para otras cosas en la vida, necesitarás un condón. Más concretamente un Condom USB.

Un Condom USB es un pendrive bueno, como ya hemos dicho. Está creado para protegerte (el nombre es bastante descriptivo). Lo insertamos entre tu cargador y el enchufe, de forma que filtra, será como poner en la carretera un puesto de peaje, que solo dejará pasar a la electricidad y le prohibirá el paso a los datos.

De esta forma, cuando lo utilices solo pasara lo que tú creías que pasaba (antes de saber que esto existía), que es que tu móvil cargara, pero nadie podrá extraer datos mientras eso sucede. Pero Iván, ¿esto tiene que ser muy caro? Estos USB son muy económicos. Entre 2 y 4 euros los puedes encontrar en la mayoría de plataformas de venta online que te vengan a la cabeza ahora mismo.

Nosotros en el despacho los regalamos a los clientes, serigrafiados con nuestro logo. Es un regalo original, verdad. Esto debería ser algo obligatorio para todos los profesionales que constantemente estamos en la calle, y que tenemos que cargar nuestro teléfono en cualquier sitio. Y es un regalo que puedes hacerle a tu hijo, estoy seguro que aunque sea solo por el nombre él se encargará de difundir para qué sirve. Hasta que lo compres para la familia, adviértele que si tiene que cargar el teléfono lo haga apagado. Otra opción que también es segura, es que cargue una batería externa, y

después con la batería recargue su móvil. Así evitamos riesgos.

7.3.- DETECTIVE DE APLICACIONES FALSAS (QUE HACEN COSAS QUE NO DICEN)

¡Guau! Una aplicación que permite ponerte unos cuantos años encima, y ver tu aspecto cuando seas mayor. Qué chulo. Y es gratis. ¿En serio? Sentido Común.

No parece muy lógico que alguien se haya puesto a desarrollar una aplicación, con el coste que eso tiene en recursos y tiempo, para posteriormente regalarla a la humanidad. ¡Qué buena gente!

Pues ahora piensa cuántas aplicaciones gratuitas tienes en tu móvil. Y vuelve a leer el párrafo anterior en voz alta. Y de estas, cuántas veces te has descargado una aplicación que en realidad nunca has utilizado, o que has utilizado muy pocas veces. Pues tu hijo multiplica esto por mucho.

Los menores descargan de forma compulsiva aplicaciones, la mayoría por recomendaciones de amigos o influencers. Por cierto, estos últimos con sus propios intereses, ya que muchas veces promocionan aplicaciones previo pago. Por lo tanto, esta habilidad que vamos a aprender, esta nueva profesión de detective de aplicaciones falsas, debe ser desarrollada cuanto antes, tanto para ti como para tus hijos. Descargar una aplicación falsa (que son todas aquellas, que dicen una cosa y hacen otra), tiene una serie de riesgos:

- La aplicación puede suponer la descarga de un **virus o un malware**. Que acabe haciendo más o menos daño.
- **Hacerse pasar por aplicaciones oficiales**. Muchas las imitan a conciencia (la realidad es que encontramos más en la tienda de Android que en la de Iphone), con diversas intenciones. La más habitual es robar datos.
- **Darle excesivos permisos**. Con la excusa de que son gratuitas, acaba poniéndonos en riesgo tanto a nosotros

como a nuestros hijos. En un ratito te pongo algunos ejemplos.

Estos son los principales riesgos. ¿Pero existen más? Claro que sí, pero estos son los principales.

¿Cómo me protejo entonces?

Para eso estoy yo, vamos con los siguientes pasos:

1. Descargar aplicaciones solo desde las tiendas oficiales. Es posible que haya problemas, pero desde luego hemos reducido mucho el riesgo. Para subir una aplicación tanto al Play Store de Android, como sobre todo a la App Store de IOS, requiere pasar determinados filtros de seguridad.

2. Existen probabilidades (muchas en Android menos en IOS) **que aun estando en las tiendas oficiales pueda ser falsa** (ya sabes, que haga cosas que no debería). Para asegurarnos deberemos seguir los siguientes pasos. Ojo a todos y cada uno de ellos, no algunos por separado:

- En primer lugar, vamos a buscar el **número de descargas.** Esto no es infalible, pero somos muchas personas, muchos ojos sobre una aplicación. Por lo que tener muchas descargas nos hace pensar que estamos ante una aplicación fiable. Tendréis que seguir chequeando el resto de pasos, porque la aplicación que nos hace envejecer fue una de las más descargadas en su día.
- Lo siguiente será **revisar las valoraciones o reseñas en IOS**. **Las puntuaciones y opiniones si estamos en Android.**
  Todas las aplicaciones pueden tener algún comentario negativo, hasta este libro tendrá comentarios negativos y como autor ya estoy preparado para ello. Por cierto, ¿qué tal si me dejas una reseña bonita, porfa? Por lo que algunas reseñas negativas son normales, es así cuando se adquiere

cierta relevancia, son las reglas del juego. Pero si son muchas o por el tipo de reseña que es, te darás cuenta rápidamente si es una aplicación falsa.

- **Permitir o no permitir, esa es la cuestión.**
  Los permisos son una de las claves. Nosotros los aceptamos y ellos se aprovechan. Estarás de acuerdo conmigo, leer no es el deporte favorito de nuestra época. Y si uno es menor de edad, todavía menos. Reconozcámoslo, los menores no leen. Y tienen el dedo muy rápido, muy rápido, por lo que suelen aprobar casi cualquier cosa. Las aplicaciones falsas lo saben y se aprovechan de ello. Con la excusa de que son gratis, te hacen aprobar permisos que la aplicación no necesitaría para nada. Dos ejemplos:

  a. Muchas personas suelen descargar una linterna para su móvil. Algo que es bastante inocente, esa linterna en teoría solo debería servir para encenderse o apagarse. Punto. Pero para ello, te suelen pedir permisos de geolocalización, acceder a tus contactos o incluso tus fotografías. Ese es nuestro verdadero pago por lo gratuito.

  b. Recuerdo hace poco, que me contaba un padre que le había descargado a su hijo una aplicación muy inocente (fíjate que es la segunda vez que utilizo esta palabra en dos párrafos, no es casualidad), estaba entre las más descargadas. Se trataba de un monito, cuando su hijo tocaba la pantalla el mono saltaba. El juego consiste en sortear obstáculos. Algo sencillo. Tras escucharme hablar de Conan Mobile, descargarlo y analizar el móvil, se dio cuenta que tenía acceso a los contactos, fotografías, geoposicionamiento y unas cuantas cosas más. El padre es abogado y era su teléfono profesional. En fin, ya te puedes imaginar.

Recuerda que Conan Mobile es solo para Android. Pero revisar los permisos en IOS es sencillo: debes ir a **<Ajustes>,** y descender

hasta encontrar **las aplicaciones instaladas**. Pulsando en cada una de ellas verás los permisos que tienen asignados.

- Y por último, **revisar el dueño de la aplicación.**
  De esta forma verás rápidamente si es una aplicación que quiere hacerse pasar por otra. ¿Dónde encuentras esta información? En Android en el apartado **<Contacto del Desarrollador>**. En IOS la encuentras en **<Ficha Técnica>**. En ambos casos vas a encontrar: el nombre de la empresa, la dirección, pero sobre todo el sitio web del creador. Y aquí vamos a revisar algunas cuestiones. Ponte la gorra de detective, jeje. ¿Preparado? Pues en marcha:

  a. Primero quiero que veas el **nombre de la página web**, y si tiene algo que ver con el desarrollador o la aplicación.

  b. En segundo lugar, vamos a mirar cómo comienza la dirección de la web. Debe ser así: **"https". Para que te hagas una idea, esa S, piensa que es segura.** Esto lo que significa es que en algún momento una tercera empresa verificó que esa dirección era segura. Es una auditoría por un tercero. Y eso da tranquilidad. Al menos un poco.

  Lo cierto es que los malos ya saben esto. Saben que si quieren engañarnos tiene que tener esa S, que va acompañada de un candadito. Y para eso no dudan en comprar los candados. Por cierto la auditoría de esa tercera empresa, ni es gratis ni para siempre.

  Debemos por tanto comprobar ambas cosas, si pulsas en el candado deberás buscar la opciones del certificado, así sabremos si está en vigor y hasta qué fecha. Y lo más importante a quién se ha emitido y por quién. Todo debe coincidir. La armonía es fundamental en la vida.

  Con estos sencillos pasos, acabas de quitarte de en medio a la mayoría de aplicaciones falsas.

c. **Busca también la pestaña del Aviso Legal en la web**. El Aviso Legal es lo mismo que preguntar: ¿quién eres? Revisa que coincida con el autor de la aplicación, la dirección, datos completos, correo electrónico. El país en el que esté te dirá mucho de la seriedad de la aplicación. Europa para esto es el lugar más seguro en cuanto a privacidad. Este filtro ya lo pasarían muy pocos.

d. Y por último, **revisa si la web está descuidada, tiene faltas de ortografía, errores gramaticales, etc...** si los tiene es una mala señal. ¿Quién dejaría su casa sin ordenar cuando espera visitas? Y además los malos no han estudiado ortografía y gramática, nunca lo olvides.

Si haces esto, serás un auténtico detective de aplicaciones falsas, y lo más importante podrás enseñarle a tu hijo a que también lo sea. Anímalo a que transmita esta información. Te dejo un documento con los pasos que hemos seguido para que puedas aplicarlo a cualquier aplicación. Sobre todo las gratuitas.

HOJA DE RUTA 10.- CHECK LIST: DETECTIVE DE APLICACIONES FALSAS

“ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ”

APLICACIÓN QUE ANALIZAMOS	

TIENDA OFICIAL	Descargada desde tienda oficial	
	No descargada desde tienda oficial	

NÚMERO DE DESCARGAS	
VALORACIONES O RESEÑAS	

REVISIÓN DE PERMISOS	ANDROID (CONAN MOBILE)	IOS (AJUSTES, APLICACIONES INSTALADAS, PULSANDO EN LA APLICACIÓN)

DUEÑO DE LA APLICACIÓN	ANDROID (CONTRATO DEL DESARROLLADOR)	IOS (FICHA TÉCNICA)

DUEÑO DE LA APLICACIÓN

NOMBRE DE LA WEB	Si tiene que ver con el desarrollado	
	No tiene que ver con el desarrollador	
HTTPS	SÍ	
	NO	
CANDADO	Si está en vigor	
	No está en vigor	
CANDADO	Si coincide con la empresa	
	No coincide con la empresa	
AVISO LEGAL	Si está identificada la empresa	
	No está identificada la empresa	
AVISO LEGAL	Se encuentra en europa	
	Se encuentra fuera de europa	
ORTOGRAFÍA Y GRAMÁTICA	Existen errores evidentes	
	Esta correcto	

7.4.- CÓMO NOMBRAR UN HEREDERO EN APPLE (CERRANDO EL CÍRCULO)

Ya hemos visto cómo nombrar un heredero en Google, también cómo hacerlo en Facebook y su mundo. Sabemos nombrar heredero si tenemos Android (a través de Google).

¿Pero qué ocurre con la manzana (Apple)? ¿No tiene esa opción? ¿Cómo se hace? ¿A qué podrán acceder y a qué no? ¿Tienen que tener un Iphone al que nombre?

Todas estas preguntas las vamos a resolver en esta parte. Comenzamos.

1.- ¿Si tengo Apple tengo la posibilidad de nombrar un heredero?

Sí. Pero esta opción está disponible solo si tienes tus dispositivos actualizados. Otra ventaja más para mantener actualizados tus dispositivos, además de la que ya conocemos que es para mantenerlos seguros. Esta opción se introdujo en: **IOS 15.2, IPAD 15.2 y MACOS 12.1.**

2.- ¿Dónde localizo esa opción?

Fácil. En Iphone, Ipad e Ipad:

- Ve a la opción de **<Ajustes>** y toca tu nombre.
- Después busca la opción: **<Contraseña y Seguridad>.**
- Si tienes tu dispositivo actualizado, localizamos la opción de: **<Representante Digital>.**
- Listo. Ahora toca **<Añadir representante digital>.**
- **Escoge una persona o varias** de tus contactos (ahora te cuento qué ocurre si no son usuarios de Apple).

- Imprime la clave de acceso, **entrega y explica a tus herederos qué implica esto** (es muy importante). Te reproduzco lo que dice el documento:

Clave de acceso del representante digital

Propietario de la cuenta: IVÁN GONZÁLEZ MORENO

ID de Apple del propietario: hola@metodocangurodigital.com

Representante digital: Raquel

Como representante digital de IVÁN, tras su fallecimiento ***podrás acceder a los datos de la cuenta y eliminar el bloqueo de activación de sus dispositivos Apple.***

Para solicitar acceso a los datos de la cuenta de IVÁN, deberás entrar en digital-legacy.apple.com y proporcionar la clave de acceso junto con una copia de su certificado de defunción.

Una vez aprobada la solicitud, podrás consultar los datos de IVÁN en icloud.com o descargar una copia en privacy.apple.com. También podrás consultarlos desde un dispositivo Apple.

Para obtener más información, visita support.apple.com/digital-legacy.

Y a continuación encuentras el código **QR y el equivalente numérico.**

Ah, ni qué decir tiene que este documento es confidencial. Por otro lado, no te agobies que siempre podrás ir a tu representante digital y volver a consultar su clave de acceso. Así como eliminar a tu heredero y nombrar otro. Si nombras a más de uno ten en cuenta que cada uno tendrá una clave diferente.

- **Revisa que tu fecha de nacimiento es correcta en los Ajustes, puesto que la solicitarán**.
- **Confirma la edad de tu heredero**. La edad mínima tiene que ser 13 años, esta es la habitual. Pero existen países que pueden requerir una edad diferente, te los indico:

    - 14 años: Austria, Bulgaria, China continental, Chipre, Italia, Lituania y España.
    - 15 años: Francia, Grecia y la República Checa.
    - 16 años: Alemania, Brasil, Croacia, Eslovaquia, Eslovenia, Hungría, Irlanda, Kosovo, Liechtenstein, Luxemburgo, Países Bajos, Polonia, Portugal, Rumanía y Singapur.

En el Mac lo localizas: dentro del **<Menú>** - **<Preferencias del Sistema>** - **<ID de Apple>** - **<Contraseña y Seguridad>**.

3.- ¿ A qué pueden acceder y a qué no pueden acceder mis herederos?. Apple nos contesta:

- Pueden acceder:
    - Fotos en Icloud
    - Notas
    - Email
    - Contactos
    - Calendarios
    - Recordatorios
    - Mensajes en Icloud
    - Historial de llamadas
    - Archivos almacenados en Icloud Drive
    - Datos de salud
    - Notas de voz
    - Lista de lectura y favoritos de Safari
    - Copia de seguridad de Icloud, que puede incluir apps descargadas del App Store; fotos y vídeos almacenados en el dispositivo; ajustes del dispositivo y

otros contenidos de los que se haya realizado una copia de seguridad en Icloud.

- No podrán acceder:
    - Contenidos con licencia: películas, música y libros que haya comprado el titular fallecido.
    - Compras dentro de las App.
    - Información de pago.
    - Información almacenada en el llavero (contraseñas).

4.- ¿Qué ocurre si no son usuarios de Apple?

Nada, no es necesario ser usuario de Apple para ser heredero (representante digital). Eso sí, recuerda disponer de la copia de la clave, confirmar la fecha de nacimiento de quien te nombró y tener la edad adecuada. Cuando llegue el momento necesitarás también el certificado de defunción.

Como siempre, te dejo una hoja de ruta para que te sea más sencillo el procedimiento. Háblalo con tu hijo. Difundid esta información por favor. Es importante. Y que toda la familia que tenga Apple (al igual que Google y Facebook) dejen sus herederos nombrados. Tardarás cinco minutos, no más. Pero esto puede solucionar muchos problemas.

HOJA DE RUTA 11.- CHECK LIST: NOMBRANDO HEREDERO EN APPLE

“ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ”

CHECK LIST: NOMBRANDO HEREDERO EN APPLE

PERSONA QUE REALIZA EL TESTAMENTO:

RUTA PARA NOMBRAR HEREDERO	**AJUSTES- CONTRASEÑA Y SEGURIDAD - REPRESENTANTE DIGITAL - AÑADIR REPRESENTANTE DIGITAL**	
PERSONAS QUE SE DESIGNAN HEREDEROS	1.- Nombre y apellido	Móvil
	2.- Nombre y apellido	Móvil
	3.- Nombre y apellido	Móvil
IMPRIMIR CLAVE DE ACCESO	SÍ	
	NO	
Llamada explicando qué significa esto + entrega clave de acceso	SÍ	
	NO	
Confirma la edad del heredero (confirma que dispone de la edad requerida)	SÍ	
	NO	
Fecha de nacimiento que aparece en los ajustes de tu teléfono (y que se le pedirá a tus herederos)		
Indica aquí si quieres que se tenga algo más en cuenta por tus herederos ej. que entreguen copia de las fotografías a alguien.		

PROTEGER A TU HIJO

EN WHATSAPP Y TELEGRAM

8.- PROTEGER A TU HIJO EN WHATSAPP Y TELEGRAM

Una de las últimas cosas que quiero contarte, son algunos "trucos" de las dos aplicaciones de mensajería instantánea más descargadas del mundo: Whatsapp y Telegram. En mi siguiente libro profundizaré en esto lo prometo y trataré cosas como:

- Las principales estafas en estas aplicaciones.
- Cómo se pueden manipular mensajes.
- Aplicaciones falsas que suplantan a estas.
- Qué valor tienen a efectos legales.
- Como parar las informaciones virales, etc…

Pero Iván, ya me ha dicho eso en varias partes del libro, lo sé. Pero si intentara escribirlo todo en un solo libro, estoy seguro que solo conseguiría que te doliera el estómago (como en una gran comilona) y que no consiguieras hacer bien la digestión. Quiero que saborees el libro. Y además esto se convertiría en una enciclopedia. Por experiencia sé que los libros muy largos no se leen. Así que para el siguiente.

Dicho esto, existen algunas cosas que tengo que contarte y no pueden esperar.

8.1.- CONFIGURAR WHATSAPP PARA QUE SEA SEGURO

Te pongo en antecedentes, Whatsapp es una de las aplicaciones más descargadas del mundo. Comprada por Facebook por unos 22.000 millones de dólares. Una aplicación gratuita (modo ironía on). Y que tanto tú como tus hijos estáis utilizando ahora o lo haréis. Se usa tanto a nivel profesional como personal, aunque de esto también debería hablaros en otro momento.

Con estos datos, no me queda otra que darte algunos consejos de configuración tanto para ti como para tus hijos. Esto es lo que mi experiencia me dice que deberías hacer:

- **COMPRUEBA QUE NO HAYAN HACKEADO A TUS HIJOS (NI A TI).**

Hablemos un poco de esto. Existen diversas formas de comprometer Whatsapp, pero esta es la más sencilla y con consentimiento de tu hijo o no, esto se hace mucho. Bajo el amor se disfraza el control.

Así se hace: tan solo necesitas el acceso al móvil de tu víctima (aunque la mayoría de las veces lo hacen con consentimiento como te decía). El atacante, que en este caso es el amor de su vida y la persona que más la comprende (de nuevo ironía on), le pide que compartan cuenta de Gmail (ya sabes lo que eso significa por el capítulo 5) y el acceso permanente a Whatsapp.

Para ello, abrirá el navegador en su móvil (todos los navegadores tienen la posibilidad en sus opciones de abrirse como versión de escritorio, es decir como si fuera en el ordenador). Tras esto, abrirá Whatsapp Web y le mostrará un código QR para vincular otro Whatsapp. Ahora irá al Whatsapp de tu hijo y vincular su Whatsapp.

Se tardan segundos. De esta forma ya tiene control total sobre el Whatsapp de la víctima. Podrá acceder a chat, fotografías, borrar

mensajes o escribirlos (en fin un arma de destrucción masiva).

Flipo Iván. ¿Pero cómo evito esto?

La forma de evitar esto, es cada cierto tiempo (una semana es buena idea) entrar a: **<Configuración>** - **<Dispositivos Vinculados>**. Y revisar todos los dispositivos que están vinculados, tocando en los mismos y cerrando sesiones.

- **LAS FOTOGRAFÍAS DEL PERFIL**

Lo sé, soy un desastre. Pero yo no recuerdo a muchas personas que tengo en mi Whatsapp por el nombre, pero ahí está el perfil de Whatsapp para ayudarme. Tengo conocidos que se entretienen revisando las fotografías de los perfiles de Whatsapp. Como si fuera una red social, se enteran de cambios en sus vidas, nacimiento de hijos, cambios de pareja, etc…

En mi vida profesional, he visto cómo el perfil de Whatsapp era utilizado para subir fotografías con la única intención de hacer daño a un tercero y difundirlas de forma indirecta (ya hemos hablado de la creatividad humana para tocar las narices).

Mi recomendación es que utilices fotografías neutras, no utilices fotografías de tus hijos o muestres aspectos comprometidos. Pero mejor aún, oculta tu foto de perfil.

Genial, ¿cómo lo hago?

De nuevo acudiremos a la **<Configuración de Whatsapp>** y dentro de la misma a la pestaña de **<Cuenta>**, ahora nos moveremos por las **<Opciones de Privacidad>**. Aquí vamos a estar un ratito configurando la mayoría.

En este caso, busca la opción: **<Foto del Perfil>**. Como puedes leer, puedes modificar las opciones para que la fotografía sea vista por todos, tus contactos o nadie. Ya sabes qué escoger.

- **NO DEJES QUE LE METAN PRESIÓN A TU HIJO**

Elimina el doble check azul y oculta la última sesión. Entre los menores esta presión es brutal. Lo había leído pero no me contestó. Sé que lo ha leído. Está conectado y no me contesta. ¿Pero qué se cree? Mañana no le hablo. Le voy a escribir de nuevo, etc…

Eliminamos y ocultamos esto: **<Configuración>** - **<Cuenta>** - **<Privacidad>** - **<Ult. Vez>**.

Podemos desactivar las confirmaciones de lectura (nadie sabrá que tú lo has leído, pero tú tampoco lo sabrás). Puedes escoger quién quieres que vea tu última sesión, las opciones vuelven a ser: todos, tus contactos o nadie. Ya sabes qué escoger.

- **OCULTA LA BIOGRAFÍA**

Nuestros hijos son creativos por naturaleza, por lo que suelen aprovechar la información/biografía para añadir mucha información: qué les gusta y qué no, datos de webs, correos electrónicos, redes sociales, etc…

Información que en algunos casos puede ser utilizada en su contra. Evitémoslo. Esta es la ruta: **<Configuración>** - **<Cuenta>** - **<Privacidad>**. Busca la opción de info. y ahora modificarla.

- **LOS GRUPOS DE WHATSAPP**

Uno de los mayores peligros para nuestros hijos, y para nosotros. Déjame que te explique un poco más de esto. En el capítulo 2 y 3, te hablaba de una norma de protección de datos, el Reglamento Europeo de Protección de Datos. Un abogado hablando de una normativa, qué raro, jeje.

Allí te lo mencionaba respecto a las imágenes que se pueden subir de nuestros hijos a internet, y también de cómo eliminarlas.

Los grupos de Whatsapp también tienen que cumplir esa normativa. Estos grupos requieren el consentimiento de la persona que se incluye. Si son menores de 14 años, ese consentimiento lo deben prestar los padres o tutores legales.

Ok Iván, una pregunta: ¿vale cualquier tipo de consentimiento?

Pues no. Ese consentimiento tiene que ser libre, específico, informado e inequívoco. Eso significa que no es válido entender que (recuerda el ejemplo que pusimos con Penélope Cruz y mi amigo):

- me dijiste que sí
- creí que no te importaría
- intuía que te apetecería
- como no me dijiste que no, pues te incluí
- me dijiste de palabra que sí

Cuidado con esto, porque es la persona que crea el grupo quien tiene que demostrar que tiene el consentimiento de todos los integrantes.

Un Grupo de Whatsapp puede suponer algo muy inocente, a priori, imagínate un grupo de senderismo donde se incluyen a 200 personas de Málaga, por supuesto sin pedirles permiso. Y casualidades de la vida, en ese grupo de Whatsapp está Esteban y el abogado que le llevó el divorcio a su mujer (David), al que por cierto no aguanta. Lo sabe, porque ha visto su foto de perfil, es él no hay duda. Ahora tiene su móvil personal. Por fin. Lo siguiente que hizo Esteban, fue suplantar su identidad con ese número móvil, y acabó creando un problema serio. En este caso no te cuento cómo lo hizo para no dar ideas.

Además los Grupos de Whatsapp también pueden servir para "comer el coco" a nuestros hijos. Cada vez más, existe un riesgo para nuestros hijos con la palabra libertad financiera, no tengo nada en contra de esa palabra, pero si la sumamos a criptomonedas, es un cóctel difícil de aguantar. Aunque sobre este mundo y sus riesgos e innumerables ventajas, dedicaré al menos dos capítulos en mi próximo libro (ya estoy otra vez, jeje). Sí que tengo que contarte algo en este momento.

Mario sabía que algo le ocurría a su hija. Susana estaba cada vez

más desconectada de su día a día, estaba cambiando el grupo de amigos, incluso su forma de hablar era diferente. Parecía que había perdido su alegría, se la habían robado. Mario sabía exactamente cuándo comenzó esto.

Todo comenzó el día que su hija le comentó que con otras compañeras acudiría a una conferencia. No sabía mucho de qué iba el tema, pero era algo sobre una nueva profesión, una forma de ganarse la vida diferente y que utilizaba internet como vehículo para ello.

Tras esa conferencia Susana venía entusiasmada, le habían hablado de cómo invertir en criptomonedas. Se podía ganar mucho dinero, dedicando muy poco tiempo al día. Le hablaron por primera vez de la palabra "libertad financiera". Mario recuerda la conversación con su hija (la había recordado mucho últimamente), esta le había pedido matricularse en una academia. Esa academia le había prometido enseñarle todo lo necesario para que pudiera lograr la libertad financiera en poco tiempo, las personas que dieron la charla estaban todas felices.

Mario no tenía claro si aceptar, pero su hija le dijo que era la oportunidad de su vida, le dijo muchas cosas que dolían, pero entre otras que no quería ser como él, que nunca estuvo cuando lo necesitó. Mario había sido camionero toda la vida. Él tenía esa cicatriz, por culpa de su profesión se había perdido muchas cosas, lo sabía, pero también sabía que tenía que sacar su familia adelante.

Susana le dijo que no quería cambiar el tiempo por dinero, que eso se hacía en la economía antigua. Que con esta nueva profesión no necesitaba trabajar más de dos horas al día, que podría hacerse rica y trabajar desde cualquier lugar del mundo. Invertir en criptomonedas era el futuro. Algo le decía a Mario que esto no estaba bien, pero a la vez también se decía a sí mismo que si era cierto y su hija dejaba pasar esta oportunidad, siempre se lo reprocharía. Quizás él fuera de otra época, se decía. Quizás no comprendo este mundo, se repetía. El motivo final que decantó la

balanza, y llevó a Mario a pagar la matrícula de la academia, era que Susana le prometió que no abandonaría sus estudios. Con el tiempo se dio cuenta del tamaño error que fue esto.

Ese día (habían pasado unos meses desde la matrícula), Mario sabía que tendría que afrontar una conversación complicada con su hija. Había abandonado los estudios y eso incumplía la promesa que le había hecho, antes de matricularse. Susana se pasaba todo el día creando grupos de Whatsapp y convenciendo a otras personas (la mayoría también menores de edad como ella), para que se apuntaran también a esta academia. Mario ya sabía que le pagaban a su hija por cada persona que convencía. Era un trabajo encubierto. Y su hija ya no estaba tan preocupada por aprender a invertir, ahora era prácticamente un comercial de esta academia, pero sin dar de alta ni tener un sueldo. Había cambiado de grupos de amigos. Incluso le había llegado a decir a sus padres, esto le dolió en el alma a Mario, que eran pobres porque querían, que nunca se habían esforzado lo suficiente. Que no se gana dinero de verdad trabajando tantas horas como lo habían hecho ellos. Que eso era de ser muy torpes.

A medida que avanzaba la conversación, Mario sabía que no iba bien. Susana parecía un robot que estaba programado para responder en piloto automático. La academia ya conocía que estas conversaciones se producen, y la habían preparado para responder todas y cada una de las preguntas que Mario podía hacer. Ese día Susana se fue de casa.

Me temo que esto que os cuento es cada vez más habitual. Estas sectas, que tienen los mismos métodos sean del tipo que sean, han crecido como setas. Todo comenzó porque a Susana la metieron en un grupo de Whatsapp donde se enteró de las primeras conferencias. Y continuó por los innumerables grupos que Susana creó, para seguir convenciendo a otras compañeras de la increíble oportunidad que era el mundo de las criptomonedas. La academia sabía todos los pasos que se daban. Era una estrategia bien pensada. Una estafa piramidal.

Pero a lo que vamos en este punto, los grupos de Whatsapp. Quizás hubiera ayudado en casos como este que no hubieran podido añadir a tus hijos con tanta facilidad a un grupo de Whatsapp.

¿Dónde está esa opción Iván?

Sigue esta ruta: **<Configuración>** - **<Cuenta>** - **<Privacidad>** - **<Grupos>**. Y modifica las opciones para que sólo puedan añadir a tus hijos a grupos las personas de sus contactos, o quien tú decidas de sus contactos.

Como últimas medidas de seguridad:

a. **Añade la opción de seguridad de verificación en dos pasos, mediante un PIN de seis dígitos**. Para ello ve a <Configuración> - <Cuenta> - <Seguridad> - **<Verificación en dos pasos>.**

b. **Y el bloqueo de pantalla también**, de forma que te requiera Touch Id para desbloquear. Lo encuentras en: <Configuración> - <Cuenta> - <Privacidad> - **<Bloqueo de pantalla>.**

JUERETO 9.- WHATSAPP SEGURO

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Y ahora vamos por uno de nuestros "Jueretos". Este me encanta (como todos, jeje). Nos sentaremos de nuevo todos los integrantes de la familia.

Y completaremos el **check list de seguridad de Whatsapp.**

Cada uno lo hará sobre su propio Whatsapp.

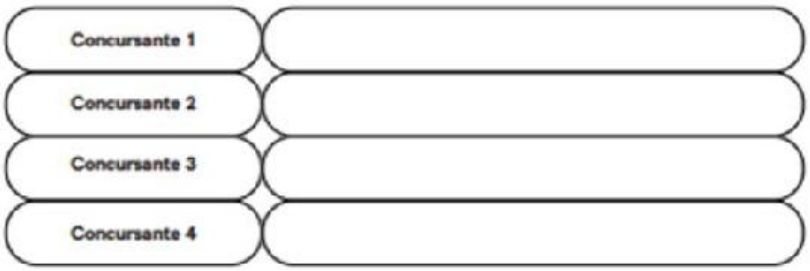
Cada opción posible **tiene indicados los puntos que otorga.**

¿Quién gana? Fácil, el que más puntos tenga.

La decisión sobre qué premio daréis la tomáis entre todos, pero es importante que haya premio.

Ánimo. Ah, recuerda contarme quién ganó:

hola@metodocangurodigital.com



CONCURSANTE 1

DISPOSITIVOS VINCULADOS	Conoces todas las sesiones iniciadas y lugares (1 punto)	
	No reconoces todas las sesiones iniciadas y lugares (0 puntos)	
FOTOGRAFÍA DEL PERFIL	Todo el mundo puede ver la fotografía del perfil (0 puntos)	
	Sólo los contactos (1 punto)	
	Nadie puede verla (2 puntos)	
DOBLE CHECK AZUL	Activado (1 punto)	
	Sin activar (0 puntos)	
ÚLTIMA SESIÓN	Todos pueden verla (0 puntos)	
	Solo los contactos (1 punto)	
	Nadie (2 puntos)	
BIOGRAFÍA	Todos pueden verla (0 puntos)	
	Solo tus contactos (1 punto)	
	Nadie (2 puntos)	
GRUPO DE WHATSAPP	Todos te pueden añadir (0 puntos)	
	Solo mis contactos (1 punto)	
VERIFICACIÓN EN DOS PASOS	Activa (1 punto)	
	No activa (0 puntos)	
BLOQUEO DE PANTALLA	Sí (1 punto)	
	No (0 puntos)	

PUNTUACIÓN TOTAL	

CONCURSANTE 2

DISPOSITIVOS VINCULADOS	Conoces todas las sesiones iniciadas y lugares (1 punto)	
	No reconoces todas las sesiones iniciadas y lugares (0 puntos)	
FOTOGRAFÍA DEL PERFIL	Todo el mundo puede ver la fotografía del perfil (0 puntos)	
	Sólo los contactos (1 punto)	
	Nadie puede verla (2 puntos)	
DOBLE CHECK AZUL	Activado (1 punto)	
	Sin activar (0 puntos)	
ÚLTIMA SESIÓN	Todos pueden verla (0 puntos)	
	Solo los contactos (1 punto)	
	Nadie (2 puntos)	
BIOGRAFÍA	Todos pueden verla (0 puntos)	
	Solo tus contactos (1 punto)	
	Nadie (2 puntos)	
GRUPO DE WHATSAPP	Todos te pueden añadir (0 puntos)	
	Solo mis contactos (1 punto)	
VERIFICACIÓN EN DOS PASOS	Activa (1 punto)	
	No activa (0 puntos)	
BLOQUEO DE PANTALLA	Sí (1 punto)	
	No (0 puntos)	

PUNTUACIÓN TOTAL	

CONCURSANTE 3

DISPOSITIVOS VINCULADOS	Conoces todas las sesiones iniciadas y lugares (1 punto)	
	No reconoces todas las sesiones iniciadas y lugares (0 puntos)	
FOTOGRAFÍA DEL PERFIL	Todo el mundo puede ver la fotografía del perfil (0 puntos)	
	Sólo los contactos (1 punto)	
	Nadie puede verla (2 puntos)	
DOBLE CHECK AZUL	Activado (1 punto)	
	Sin activar (0 puntos)	
ÚLTIMA SESIÓN	Todos pueden verla (0 puntos)	
	Sólo los contactos (1 punto)	
	Nadie (2 puntos)	
BIOGRAFÍA	Todos pueden verla (0 puntos)	
	Solo tus contactos (1 punto)	
	Nadie (2 puntos)	
GRUPO DE WHATSAPP	Todos te pueden añadir (0 puntos)	
	Solo mis contactos (1 punto)	
VERIFICACIÓN EN DOS PASOS	Activa (1 punto)	
	No activa (0 puntos)	
BLOQUEO DE PANTALLA	Sí (1 punto)	
	No (0 puntos)	

PUNTUACIÓN TOTAL	

CONCURSANTE 4

DISPOSITIVOS VINCULADOS	Conoces todas las sesiones iniciadas y lugares (1 punto)	
	No reconoces todas las sesiones iniciadas y lugares (0 puntos)	
FOTOGRAFÍA DEL PERFIL	Todo el mundo puede ver la fotografía del perfil (0 puntos)	
	Sólo los contactos (1 punto)	
	Nadie puede verla (2 puntos)	
DOBLE CHECK AZUL	Activado (1 punto)	
	Sin activar (0 puntos)	
ÚLTIMA SESIÓN	Todos pueden verla (0 puntos)	
	Sólo los contactos (1 punto)	
	Nadie (2 puntos)	
BIOGRAFÍA	Todos pueden verla (0 puntos)	
	Solo tus contactos (1 punto)	
	Nadie (2 puntos)	
GRUPO DE WHATSAPP	Todos te pueden añadir (0 puntos)	
	Solo mis contactos (1 punto)	
VERIFICACIÓN EN DOS PASOS	Activa (1 punto)	
	No activa (0 puntos)	
BLOQUEO DE PANTALLA	SI (1 punto)	
	No (0 puntos)	

PUNTUACIÓN TOTAL	

8.2.- CONFIGURAR TELEGRAM PARA QUE SEA SEGURO

Telegram es una de las aplicaciones de mensajería que más ha crecido en los últimos años, bajo la bandera de ser más segura que Whatsapp y más respetuosa con la privacidad de sus usuarios. Es algo intermedio entre una aplicación de mensajería y una red social, se tiene un nombre de usuario y te pueden buscar por el (algo que no ocurre en Whatsapp).

Tiene muchas ventajas si configuramos bien las diferentes opciones que nos da, sino puede ser incluso peor que Whatsapp. Vamos a hacerlo (y a terminar el capítulo y el libro me da pena).

- **TELEGRAM PC**

Comencemos por lo que ya habíamos visto en Whatsapp, recuerda lo que acabas de leer sobre cómo hackear Whatsapp vinculándolo con otro dispositivo. Aquí todavía es más importante, porque se puede acceder a Telegram por el ordenador. Vaya novedad Iván, pues como Whatsapp. Cierto, pero aquí se puede aunque tu móvil esté apagado.

Revisa las sesiones que tienes abiertas tú y tu hijo.

La ruta es: **<Ajustes>** - **<Dispositivos>** - **<Otras sesiones>**. Pulsa en las diferentes sesiones y cierra las que no identifiques. Revisa también la opción que aparece en la parte inferior (a mí me encanta), dice algo así como: **Cerrar Sesiones Automáticamente**, si están inactivas por 1 semana, 1 mes, 3 meses o 6 meses. De esta forma se cerrarán automáticamente, marca una semana o un mes. No más.

- **GRUPOS Y CANALES**

Es aplicable todo lo que hemos hablado en Whatsapp, no permitas

que cualquier persona pueda añadirte a un grupo.

Esta es la ruta: **<Ajustes>** - **<Privacidad y Seguridad>** - **<Grupos y Canales>**. Puedes además editar quién puede y quién no añadirte a grupos.

- **NÚMERO DE TELÉFONO**

Quizás una de las diferencias más importantes respecto a Whatsapp. Configura quién puede ver tu móvil.

La ruta es: **<Ajustes>** - **<Privacidad y Seguridad>** - **<Quién puede ver mi número>**.

- Configura también **el resto de opciones**, ya sabes cómo:

  a. Última vez y en línea

  b. Foto de perfil

  c. Llamadas, si desactivas la opción peer to peer todas las llamadas pasarán por los servidores de Telegram para evitar dar a conocer tu dirección IP, pero eso hará disminuir la calidad del audio y vídeo.

  d. Mensajes reenviados, esta opción es importante para que no se puedan añadir enlaces a tu cuenta al reenviar mensajes.

- Y también me encanta la opción de **eliminar mi cuenta automáticamente**, si no estás en línea al menos una vez durante ese período. Puedes establecer 1 mes, 3 meses, 6 meses y 12 meses.

Con esto tu Telegram y el de tu hijo quedan también protegidos.

- Ah, no olvides activar dentro de **<Ajustes>** - **<Privacidad y Seguridad>**, tanto el **Código y Touch ID**. Y la **verificación en dos pasos**, que es una contraseña adicional que te solicitará al iniciar sesión en un nuevo dispositivo, además del código que se recibe por SMS.

JUERETO 10.- TELEGRAM SEGURO

"ME LO CONTARON Y LO OLVIDÉ; LO VI Y LO ENTENDÍ; LO HICE Y LO APRENDÍ"

Nuestro último "Juereto", aunque prometo que volverán en el siguiente libro. Espero que los hayáis disfrutado tanto como yo creándolos.

La idea es la misma que el anterior pero con Telegram. Nos sentaremos de nuevo todos los integrantes de la familia, y completamos el check list de seguridad de Telegram.

Cada uno lo hará sobre su propio Telegram pero esta vez lo haremos por parejas. Porque es muy posible que todavía no tengáis Telegram todos los miembros de la familia, pero lo acabaréis teniendo.

Cada opción posible tiene indicados los puntos que otorga.

¿Quién gana? Fácil el que más puntos tenga.

La decisión sobre qué premio daréis la tomáis entre todos, pero es importante que haya premio. Ánimo.

Recordad que tenéis material adicional que podéis encontrar en el mismo lugar donde habéis adquirido este libro. Y que una reseña tuya ayudará primero a mejorar el libro (las leo todas) y en segundo lugar a que más personas lo conozcan.

PAREJA 1

TELEGRAM PC	Conoces todas las sesiones iniciadas y lugares (1 punto)	
	No reconoces todas las sesiones iniciadas y lugares (0 puntos)	
CERRAR AUTOMÁTICA-MENTE LAS SESIONES	1 semana (3 puntos)	
	1 mes (2 puntos)	
	3 meses (1 punto)	
	6 meses (1 punto)	
	No configurado (0 puntos)	
GRUPOS Y CANALES	Todos pueden añadirte (0 puntos)	
	Sólo tus contactos pueden añadirte (1 punto)	
NÚMERO DE TELÉFONO (quién puede ver mi número de teléfono)	Todos (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
ÚLTIMA VEZ Y EN LÍNEA	Todos (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
FOTO DE PERFIL	Todos pueden verla (0 puntos)	
	Tus contactos (1 punto)	
LLAMADAS	Todos pueden hacerte llamadas (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
MENSAJES REENVIADOS (quién puede añadir un enlace a mi cuenta al reenviar mis mensajes)	Todos (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
ELIMINAR MI CUENTA AUTOMÁTICAMENTE (si no estás en línea al menos una vez en el periodo que designes)	1 mes (3 puntos)	
	3 meses (3 puntos)	
	6 meses (2 puntos)	
	12 meses (1 punto)	
CÓDIGO Y TOUCH ID	Si configurado (1 punto)	
	No configurado (0 puntos)	
VERIFICACIÓN EN DOS PASOS	Si activada (1 punto)	
	No activada (0 puntos)	

PUNTUACIÓN TOTAL	

PAREJA 2

TELEGRAM PC	Conoces todas las sesiones iniciadas y lugares (1 punto)	
	No reconoces todas las sesiones iniciadas y lugares (0 puntos)	
CERRAR AUTOMÁTICA-MENTE LAS SESIONES	1 semana (3 puntos)	
	1 mes (2 puntos)	
	3 meses (1 punto)	
	6 meses (1 punto)	
	No configurado (0 puntos)	
GRUPOS Y CANALES	Todos pueden añadirte (0 puntos)	
	Sólo tus contactos pueden añadirte (1 punto)	
NÚMERO DE TELÉFONO (quién puede ver mi número de teléfono)	Todos (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
ÚLTIMA VEZ Y EN LÍNEA	Todos (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
FOTO DE PERFIL	Todos pueden verla (0 puntos)	
	Tus contactos (1 punto)	
LLAMADAS	Todos pueden hacerte llamadas (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
MENSAJES REENVIADOS (quién puede añadir un enlace a mi cuenta al reenviar mis mensajes)	Todos (0 puntos)	
	Tus contactos (1 punto)	
	Nadie (2 puntos)	
ELIMINAR MI CUENTA AUTOMÁTICAMENTE (si no estás en línea al menos una vez en el periodo que designes)	1 mes (3 puntos)	
	3 meses (3 puntos)	
	6 meses (2 puntos)	
	12 meses (1 punto)	
CÓDIGO Y TOUCH ID	Si configurado (1 punto)	
	No configurado (0 puntos)	
VERIFICACIÓN EN DOS PASOS	Si activado (1 punto)	
	No activada (0 puntos)	
PUNTUACIÓN TOTAL		

AHORA TE TOCA A TI

Decía Unamuno: "*Vale más tener un lápiz corto que una memoria larga*".

Creé el Método Canguro Digital para que tuvieras un paso a paso, con un único objetivo: ayudarte a proteger y educar a tus hijos en este mundo digital.

Este libro nació con la idea de ser un libro basado en mi experiencia (tienes decenas de ejemplos reales, por supuesto he cambiado los nombres y he utilizado nombres de mis familiares y amigos, espero que les haga ilusión ver sus nombres en el libro). Un libro fácil de poner en práctica, me encanta mantener las cosas fáciles pero no simples.

He intentado dejarte ejercicios en forma de retos ("Jueretos") a lo largo del libro, además de formularios denominados "Hojas de ruta" para que esto no sea una relación entre autor y lector de forma pasiva, sino una conversación entre nosotros, los ejercicios son esa conversación. Pero no solo entre tú y yo, sino también con tu familia. Si he logrado que habléis de alguno de los temas que he tratado en el libro en familia, ya me doy por feliz.

Escuchemos a nuestros hijos, recuerdo que un día mi hija Sofía me preguntó si la estaba escuchando. Yo le dije que sí, pero mirando la pantalla del móvil. Me cogió con sus manos y me dijo: "Papi, escúchame con los ojos también".

El poco tiempo no puede ser una excusa. Recuerdo que esta era una frase que yo solía decirle a mi hijo Jesús: "Papi está poco tiempo, pero el tiempo que estoy es para vosotros".

Ahora comprendo que ellos no miden la calidad, miden la cantidad. Son egoístas en el buen sentido. Unos hijos quieren y necesitan el máximo tiempo con sus padres. Leí una frase hace no mucho que se

me ha grabado en el alma: “Hasta la mejor gota de agua del mundo, hará que una planta se seque”.

Este libro espero que te haya cambiado al leerlo como me cambio a mí al escribirlo. Tenemos una responsabilidad y necesito tu ayuda. Debemos lograr que este conocimiento alcance a la mayor parte de personas posibles. Ese es mi sueño. Recuerda el cuento de la estrella de mar al inicio del libro. Juntos podemos.

Por mi parte, seguiré. Es mi compromiso. A este libro seguirán otros. Además, este libro como sabes viene acompañado de materiales adicionales, para poder realizar los ejercicios en colegios, ampas, asociaciones, clubes, etc… Además de un libro de sopa de letras, esto no es nada habitual, pero es una forma de seguir aprendiendo con nuestros hijos mientras jugamos. Esa es la clave. Aprovecha también el libro de contraseñas para padres e hijos, ya sabes lo importante que es esto.

Yo no me iré muy lejos, prometido, estaré siempre que me necesites:hola@metodocangurodigital.com

GRACIAS, GRACIAS Y GRACIAS.

¿TE PUEDO PEDIR UN FAVOR?

Gracias por el tiempo que hemos pasado juntos. Si este libro te ha parecido que puede ayudar a otras personas, te estaré eternamente agradecido si puedes dejar un comentario en Amazon. Esto es muy importante para que este libro pueda seguir su camino, y es muy importante para mí. Amazon tiene muy en cuenta los comentarios, sin opiniones este libro morirá. Además me ayuda a mejorarlo, leo todas, y todas son todas, las opiniones que me dejáis, con ellas intento mejorar.

Puedes dejar tu opinión en la página de este libro en Amazon, encuentras esta opción un poco más abajo en el apartado:

Amazon.es: **<Opiniones de Clientes>** - **<Escribir mi opinión>**

Amazon.com: **<Customer Reviews>** - **<Write a Customer Review>**

Recuerda: *"A veces sentimos que somos una gota en el mar, pero el mar sería menos sin esa gota".* Santa Teresa de Calcuta.

CÓDIGOS QR DE LAS WEBS Y APLICACIONES MENCIONADAS EN EL LIBRO

CAPÍTULO 1

www.web.archive.org

www.google.es/alerts

CAPÍTULO 2

https://www.elevenpaths.com

CAPÍTULO 3

https://edpb.europa.eu/

www.aepd.es

CAPÍTULO 4

https://haveibeenpwned.com/

https://www.passwordmonster.com/

https://nordpass.com/es/most-common-passwords-list/

https://www.torproject.org/es/download/

CAPÍTULO 5

https://adssettings.google.com/authenticated

www.myactivity.google.com.

CAPÍTULO 6

https://help.instagram.com/contact/1474899482730688?helpref=faq

MyiB9nxkxdUnCafnjVDI0nxbmkfpmwiA9Ngn4rygIPTOHnxI

https://www.aepd.es/es/guias-y-herramientas/videos

CAPÍTULO 7

www.myactivity.google.com

CAPÍTULO 8

Sin enlaces.

REGALO PARA LOS LECTORES

Tengo dos regalos para ti. Ya me vas conociendo, me encanta ayudar, nací para eso.

1.- REGALO PLUS. - SUSCRIPCIÓN GRATUITA DURANTE UN AÑO A NUESTRO SERVICIO DE ALERTAS DE SEGURIDAD

VALORADO EN 120 EUROS MÁS IVA.

Podrás estar informado de todos los riesgos que suceden en este mundo de internet, y que afectan a nuestros peques.

Ya te he contado lo que significan las reseñas para que este libro siga su camino, además me ayudarán a seguir creando más libros en el futuro.

Me encantaría darte las gracias en persona por cada reseña que recibo (así son de importante para mí), pero como no puedo déjame que te lo agradezca con este regalo. En otras ediciones es posible que este regalo desaparezca.

Para obtenerlo, tan solo tendrás que remitirme un correo electrónico con una copia de la reseña: hola@metodocangurodigital.com.

2º.- EBOOK GRATUITO CON 20 SOPAS DE LETRAS SOBRE EL CONTENIDO DEL LIBRO

Este regalo es para todos los lectores del libro.

Ah, como no sé si tendré la web terminada (www.metodocangurodigital.com) para cuando estés leyendo esto, podrás pedírmelo también por correo electrónico: hola@metodocangurodigital.com.

Estoy seguro de que te divertirás mucho, como yo me he divertido creándolas. Disfrutemos del camino.

AGRADECIMIENTOS

Gracias a mi mujer (Raquel), sin ella nada sería posible. Ella hace mejor a las personas que la conocen, el cielo existe porque ella es un ángel. Gracias Dios por ponerla en mi camino cuando éramos dos niños. Te amo.

Gracias a mis hijos, Jesús y Sofía. Espero que algún día estéis tan orgullosos de mí como yo lo estoy de vosotros, sois mi inspiración. Os quiero.

Gracias a mis padres (Salvador y Manola) y mi hermano (Yosis), ellos me han enseñado que el amor es para siempre, y que los valores son el verdadero tesoro de esta vida. Sois los mejores padres que un hijo podría soñar.

Gracias a mis ángeles en el cielo, os quiero abuelos/as. Os siento cerca siempre.

Gracias a mi familia del trabajo: Mel, Sole, Gracia, Noelia, Belén, Álvaro, Adriana, Susana y Pedro.

Gracias a todos los que en algún momento se han cruzado en mi vida, de todos aprendí.

Gracias a mi familia literaria, mi adorado Grupo 5 de Triunfa con tu Libro, a ti Ana Nieto y al resto de compañeros. Gracias por ayudarme a cumplir este sueño.

Para mis hijos, vosotros habéis inspirado este libro.

En las páginas de mi vida vosotros sois el mejor capítulo.

Os amo.