CÓMO MANTENER A SALVO LA INFORMACIÓN DE TU EMPRESA Y SUS SISTEMAS

VICTOR EDUARDO DEUTSCH

CIBER SEGURIDAD PARA DIRECTIVOS

RIESGOS, CONTROL Y EFICIENCIA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

LID

ÍNDICE

SEGUNDA PARTE:
CONTROL

AGRADECIMIENTOS

Gracias a mis padres, quienes me inculcaron el amor por la historia, la tecnología y las letras; este libro intenta ser el resultado de la convergencia de estas tres disciplinas. Gracias a mi esposa Verónica y a mis hijos, Felicitas y Beltrán, por su apoyo. Gracias también a los grandes profesores que conocí a lo largo de mi carrera, como Rodolfo Jáuregui, Eduardo Poggi, Carlos Portela, Fernando Cortiñas y Rubén Herskovits; a Mercedes Núñez, a su equipo del área de comunicación de Telefónica Empresas y a todos los colegas del blog de tendencias Think Big Empresas —reconocido en el Día de Internet con el premio al mejor medio de comunicación en la categoría de Transformación digital—, donde he anticipado algunas de las ideas que he desarrollado en este libro, y a Ricardo Baduell, por sus sabios consejos.

Por último, quiero expresar un agradecimiento colectivo a todos los profesionales de marketing y ventas de Telefónica Empresas en España, de los que he aprendido muchísimo, especialmente acompañando a sus gestores comerciales en el contacto directo con los clientes. Ellos son la mejor fuerza comercial del mundo.

INTRODUCCIÓN

En la actualidad cada vez son más las empresas víctimas de ciberataques que generan graves daños para el negocio y ponen en entredicho la reputación y la confianza en ellas, reduciendo considerablemente su valor. Ser vulnerable o tener una brecha de seguridad es algo que ninguna organización de cualquier tamaño se puede permitir pues en cuestión de minutos un incidente de este tipo puede bloquear su actividad, afectando incluso a clientes, proveedores o comunidades, provocando un impacto en ocasiones devastador para la organización o dificultando gravemente su recuperación. Por todo ello, la ciberseguridad o seguridad de la información ha pasado a ser una de las grandes preocupaciones de los directivos de empresas.

Para las compañías hay un mercado de miles de millones de personas y organizaciones conectadas a Internet que demandan nuevos servicios digitales. Los administradores públicos también perciben la exigencia de los ciudadanos de más modernos y mejores servicios digitales. Pero este proceso de transformación digital se asienta en la información, así como en la forma en la que esta fluye a través las redes de comunicaciones y se procesa por medio de aplicaciones. Por eso, esta preocupación por la seguridad de la información resulta bastante lógica. Entre otras cosas, los activos físicos se transforman en activos digitales y aparecen nuevos activos intangibles que hay que proteger (*software,* datos, etc.).

Según un estudio del Foro Económico Mundial[1], el 81 % de los directivos de empresa piensan que la transformación digital es el principal motivo para mejorar la *ciberresiliencia,* entendiendo esta como la capacidad de las organizaciones para soportar contingencias relacionadas con la ciberseguridad. Además, el 87 % de la misma muestra tiene la intención de establecer objetivos de mejora.

Esta preocupación es creciente. En la encuesta Global Risk Management Survey, llevada a cabo en 2017 por la aseguradora AON entre dos mil directivos de empresa de todo el mundo, la ciberseguridad aparecía en quinto lugar entre los riesgos que afrontan las compañías. Pero en 2021 el mismo estudio[2] revela que el riesgo de «ciberataques y fugas de información» sube hasta el primer puesto en la valoración de los ejecutivos, por encima incluso de la «interrupción del negocio» —un riesgo fuertemente influido por la pandemia— y del riesgo de sufrir una ralentización del crecimiento económico.

Desde la perspectiva de la gestión de una empresa, administrar la seguridad equivale a administrar los riesgos que amenazan sus recursos, sean estos personas, materiales o intangibles, como la propiedad intelectual, la reputación o la marca. Sin embargo, según mi propia experiencia, aunque la mayoría de los gerentes y directivos de empresas entienden, analizan y toman decisiones con bastante confianza en el ámbito de la gestión de riesgos tradicionales, se sienten bastante inseguros en el terreno de la ciberseguridad, hasta tal punto que muchas veces no solo delegan esta responsabilidad en especialistas internos o externos, sino que además llegan a depender de ellos.

Esto se debe a nuestra formación, ya que la mayor parte de nosotros crecimos en una cultura en la que los activos que se tenían que proteger de una empresa eran físicos: bienes de uso, materias primas e insumos o dinero en efectivo, para los que existen controles y medidas de seguridad desde hace cientos de años; tantos, que ya forman parte de nuestro sentido común.

Las universidades que forman a los directivos de las empresas (administradores, ingenieros y abogados) suelen capacitarlos muy bien para la gestión de aspectos legales y regulatorios, controles internos y procesos de auditoría, pero la formación en los aspectos diferenciales de seguridad de la información es apenas incipiente.

Nadie nos ha preparado para la protección de activos digitales como líneas de código de *software,* datos de usuarios, billeteras virtuales o criptomonedas. Ni para los miles de intentos de fraude que se producen en Internet todos los días. Quizás la nueva generación nativa digital que se está formando hoy en las escuelas incorpore ya ese acervo, aunque posiblemente tarde décadas en alcanzar el grado de conocimiento existente en la actualidad sobre los riesgos tradicionales.

Al directivo actual le queda el recurso de la autoformación. Hay mucha y muy buena bibliografía sobre ciberseguridad, si bien generalmente está dirigida a profesionales de tecnología de la información (IT) y a los especialistas que colaboran con organizaciones públicas y privadas, de modo que se exige como prerrequisito un conocimiento avanzado de informática, incluyendo sistemas operativos, redes y protocolos de datos y conceptos de desarrollo de *software*.

Este libro pretende ayudar al directivo, sin imponerle la necesidad de contar con una formación específica en IT, a conocer, valorar y tomar decisiones acerca de los riesgos de ciberseguridad a los que se enfrenta una compañía en la tercera década del siglo XXI y a establecer diferentes medidas de control.

El objetivo de *Ciberseguridad para directivos* no es dar respuesta a todos los problemas ni una receta para resolverlos, sino ofrecer herramientas para que los directivos puedan analizar y tomar decisiones de ciberseguridad a alto nivel desde su posición de gestores.

En estas páginas sugiero un modelo que permite abordar el problema de forma estructurada y sin dejar cabos sueltos. En la mayoría de los casos, para ilustrar las distintas alternativas, pongo ejemplos del mundo no virtual, así como de experiencias reales propias.

El libro se divide en tres partes: Riesgos, Control y Eficiencia. En la primera analizo la naturaleza de los riesgos y amenazas que debe considerar un directivo de empresa, incluyendo el nuevo factor que representan las redes sociales.

En esta parte, la mayoría de los cursos y textos introductorios sobre riesgos en ciberseguridad se estructuran de acuerdo con la tipología de los distintos ataques o amenazas posibles (virus, *ransomware* y DDoS —que definiré más adelante—) o según sus diferentes fuentes (correo electrónico, navegación por Internet y otros). Como este es un texto enfocado a directivos que no tienen

necesidad de conocer los detalles técnicos de estos ataques, lo he estructurado según las consecuencias o el impacto de las amenazas en la empresa.

Desde ese punto de vista, nuestro primer riesgo es el de caer víctimas del marketing del miedo, es decir, huir de los cambios que se producen en la economía digital por las terribles consecuencias que algunos sostienen que nos esperan; o caer víctimas de la impotencia y considerar que, como administradores, no podemos gestionar un área tan especializada.

Luego analizaré las amenazas más directas al patrimonio y a la cuenta de resultados de la empresa, detallando una serie de situaciones de riesgo previsibles cuando la compañía se interna en la economía digital.

Pero quizás lo más importante es el capítulo dedicado a exponer cómo la manera errónea de encarar las situaciones de crisis que resultan imprevisibles puede llegar a ser la peor amenaza para una organización al afectar a su reputación, a su credibilidad e incluso a la sociedad en su conjunto.

En la segunda parte se estudian los controles de seguridad informática en las empresas, advirtiendo que el nuevo perímetro de actuación excede las fronteras de las redes internas y se adentra en el ámbito de las aplicaciones en la nube y de todos los dispositivos conectados a Internet.

Pero para empezar a desgranar las diferentes medidas de control de riesgo, es necesario comenzar por hacer un poco de historia sobre la evolución de la IT y explicar el origen de algunas hasta llegar a la época actual.

A partir de allí, inevitablemente se clasifican los controles según la vieja teoría de sistemas: la forma en la que la información fluye dentro de una organización. Según este modelo, hay dos tipos de datos: en movimiento y estáticos. Simplificando, se puede decir que históricamente el mayor riesgo que corría la información se hallaba cuando estaba «en movimiento». Era más fácil proteger los recintos donde se protegían los registros (físicos o virtuales) con medidas de control de acceso permanentes. Pero cualquier dato que saliera de allí requería unas medidas especiales de protección que no siempre se podían garantizar en todo el trayecto. Por eso separo esta problemática en el capítulo «Seguridad en las redes de comunicación».

En el siguiente capítulo de esta parte abordo la seguridad de la información «estática», los almacenamientos de datos y sistemas, poniendo el foco en las pymes, dado que sus particularidades lo requieren. España es un país de pymes y su prosperidad es buena para la economía en general, además de que ejercen muchas actividades complementarias de las grandes organizaciones y se integran en su cadena productiva.

El último capítulo de esta segunda parte lo dedico a los controles en el ámbito de las tecnologías operacionales (especialmente en la industria), un área que tradicionalmente se desarrolló en paralelo con las tecnologías de la información y que actualmente, con el paradigma de industria 4.0, requiere unas medidas de control de ciberseguridad que hace años hubiesen sido innecesarias.

Finalmente, en la tercera parte incluyo algunas recomendaciones para diseñar procesos de negocios seguros y una organización de ciberseguridad adecuada a las estructuras y prácticas del paradigma de la transformación digital.

Si has llegado hasta aquí, se supone que tienes consciencia de los riesgos y que tomas decisiones empresariales para mantenerlos controlados. Con esto habrás hecho lo correcto, como dijo Peter Drucker, el analista más prestigioso en la gestión y dirección de empresas en el ámbito mundial, pero la empresa pide algo más: hacerlo en forma eficiente, maximizando los resultados y optimizando los costes.

Es decir, podemos mejorar la ciberseguridad en un orden de magnitud con grandes inversiones y un alto coste operacional, pero al precio de privar de recursos a la organización en áreas donde son necesarios para crecer y desarrollarse. Al fin y al cabo, la ciberseguridad, considerada dentro de la cadena de valor de Porter, en la mayoría de las compañías es un proceso de soporte, no forma parte del proceso central (aunque esto sería discutible en las compañías que venden confianza, como las del sector financiero).

A continuación proporciono herramientas que pueden ayudar al administrador a mejorar la eficiencia de sus procesos de ciberseguridad y analizo las principales funciones de seguridad en la empresa y las estructuras de recursos que normalmente se ocupan de ellas.

En los siguientes capítulos se expone el modelo de organización de IT que mejor se adapta a los tiempos actuales y que permitirá

alcanzar el mejor uso de los recursos y cómo encaja la organización con el modelo de gestión de ciberseguridad propuesto.

Para terminar, he incluido un apartado con las principales conclusiones y recomendaciones que deben tener en cuenta los administradores que decidan aventurarse en la ciberseguridad y un anexo documental en el que detallo algunos elementos que son importantes para el directivo: los estándares de seguridad, las autoridades y la normativa en España y las implicaciones del Reglamento General de Protección de Datos.

El libro está pensado para aquellos profesionales que no se dedican a la ciberseguridad pero sí son responsables de organizaciones y de su continuidad, por lo que está escrito con un lenguaje sencillo, alejado de tecnicismos, para que sea fácilmente asimilable y aplicable.

Espero que te sirva de utilidad para mantener a salvo y blindar la seguridad de tu empresa, sus sistemas y su información y la de tus clientes.

PRIMERA PARTE

RIESGOS

«La conciencia del peligro es ya la mitad de la seguridad y de la salvación».

Ramón J. Sénder (1902-1982), escritor español

1
EL MARKETING DEL MIEDO

1. «Algunos ya no estarán con nosotros»

En 2009, en plena pandemia global de la gripe A, una empresa farmacéutica líder nos convocó para presentarnos su propuesta de atención a la crisis. En síntesis, se trataba de que comprásemos miles de dosis de antivirales para proteger a los empleados que ocupaban posiciones críticas. Gracias a esto, según sugerían los representantes, aun en el punto máximo de infección, nuestra empresa podría seguir funcionando y brindando su servicio al público como infraestructura crítica. Eso sí, pasado ese punto, al ir retomando la actividad normal, nos advirtieron: «algunos ya no estarán con nosotros».

Los asistentes a la reunión, mandos medios de la organización, nos miramos nerviosos. Uno comentó que apenas saliera de la oficina pensaba pasar por la farmacia para comprar antivirales para toda su familia. Visto desde 2022, esto parece sacado de una novela de anticipación, pero no lo es tanto. Veníamos de años hablando del SARS, de la gripe porcina y, finalmente, de la gripe aviar. La técnica

de marketing que utilizaba el comercial de la compañía farmacéutica tampoco era tan novedosa.

El marketing del miedo *(fear-based marketing)* es bastante frecuente. No solo en el marketing político (quizás el caso más evidente), sino en muchos negocios. El caso mencionado anteriormente, relativo a la sanidad, es extremo e impactante, pero refleja un modo de hacer bastante habitual en algunos sectores. El de los seguros es uno de ellos, pero los mismos procedimientos se usan en el financiero, en la automoción, en la seguridad privada y en otros.

Nuestro cerebro está condicionado para reaccionar rápidamente ante una amenaza. El miedo es una de nuestras emociones básicas y, sin duda, nos lleva a tomar muchas decisiones. Es casi inevitable que se utilice como una herramienta de marketing, especialmente en los sectores que venden productos o servicios que afectan a nuestra seguridad en cualquiera de los sentidos, desde nuestra integridad física hasta nuestro deseo de tranquilidad *(peace of mind)*.

Actualmente muchos de los informes, noticias y reportajes referidos a los riesgos de ciberseguridad que leemos —y no solo publicidad— pueden darnos la sensación de estar ante este mismo tipo de campaña de marketing del miedo. He aquí algunos ejemplos de afirmaciones publicadas por la prensa:

«El 75 % de las organizaciones se encuentran en alto riesgo de sufrir un ciberataque, según un estudio».

La Razón, 29 de junio de 2016, basado en un estudio de RSA.

«Un gran número de empresas se encuentran en un estado de alto riesgo frente a cualquier tipo de ciberataque».

ABC, 25 de septiembre de 2017.

«Los ciberataques mueven ya más dinero que el narcotráfico».

Computing, 23 de junio de 2021.

«España, el país con más ciberataques recibidos: sufrió 51 000 millones el pasado año».

El Español, 17 de febrero de 2022.

Esto no quiere decir que los estudios que citan los medios de comunicación proporcionen datos falsos, pero habría que analizarlos, como se hace con las encuestas electorales, en el contexto en el que se extraen y contrastarlos con otras fuentes. La prensa es neutral: los estudios mencionados son noticias relevantes y ella se limita a reproducirlos y comentarlos; se trata solo de uno de los vehículos de este tipo de acciones.

El problema del marketing del miedo es que beneficia a los sectores que lo realizan a corto plazo, pero puede tener efectos colaterales a largo plazo. Por ejemplo, si una empresa de seguros hace una campaña muy agresiva sobre los accidentes de coche, ¿puede eso afectar el mercado de automoción? O, si se hace una campaña muy agresiva sobre los riesgos en el ciberespacio, ¿afectará a la adopción de nuevas tecnologías digitales?

Entonces, ¿cuál es la situación de la ciberseguridad en España? ¿Debemos preocuparnos hasta el punto de replantearnos la adopción de tecnologías digitales en particulares y empresas? ¿Estamos entrando en una jungla sin ley con resultados impredecibles? ¿O disponemos de ciertas garantías de seguridad para movernos al menos con la misma tranquilidad que en el mundo tangible?

Afortunadamente, disponemos de muchas fuentes, algunas muy objetivas, y podemos presentar un panorama general. Una de las mejores es el informe «Ciberamenazas y tendencias», que elabora anualmente el Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT)[1].

Los datos del CCN nos brindan una visión de los incidentes que afectan a la administración pública y a todas las empresas que reciben la consideración de «infraestructura crítica». Veamos lo que nos muestran: *a priori,* el número de incidentes ha crecido más del doble entre 2015 y 2019, antes de la pandemia, pasando de 18 232 a 42 997. Podríamos estar en una situación muy preocupante.

Los incidentes críticos han bajado, en números absolutos, de 66 (0.3 %) en 2015 a 43 en 2019. Si nos remontamos a 2014, fueron 132, la tercera parte. El peso de incidentes de nivel muy alto-alto cae del 73 al 64 %. ¿Dónde se da el mayor crecimiento en el número de incidentes? En los de impacto medio-bajo, que pasan de 5962 (32.7 %) a 15 435 (35.9 %). Podemos decir que hay más cantidad de incidentes detectados —lo que puede revelar una mejor capacidad de detección— menos graves.

De eso se trata la gestión de la ciberseguridad: de gestionar los riesgos, de conseguir detectar muchos incidentes y de que las medidas implementadas sirvan para mitigar sus efectos, reduciendo el impacto en las organizaciones. Esto no es consuelo para quien sufre un incidente grave, pero un gestor, en un contexto de incertidumbre, tiene que tomar decisiones en función de los datos.

Y los datos nos dicen que la inversión en ciberseguridad funciona. Mientras crece el número de incidentes menores, las administraciones públicas y las infraestructuras críticas son cada vez más seguras y capaces de enfrentarse a las amenazas más importantes, por lo cual están mejorando aceleradamente su posición para desarrollar una transformación digital en forma segura.

¿Pero qué pasa en el ámbito de las pymes y de los autónomos? Tengamos en cuenta que en este segmento hay una correlación directa con lo que ocurre en el espacio residencial, pues muchas veces los recursos que se utilizan son los mismos (el PC para el trabajo y para casa) y existe una misma conectividad (línea fija y móvil). Este es el terreno de la concienciación: en España tanto el Instituto Nacional de Ciberseguridad (INCIBE)[2], entidad oficial específicamente creada para ese fin, como las Fuerzas y Cuerpos de seguridad del Estado han dedicado muchos recursos a concienciar al público y generar prevención.

Para ver lo que está pasando disponemos del último informe del Observatorio Nacional de Tecnología y Sociedad (ONTSI), de abril de 2020[3], que incluye una evaluación, realizada con herramientas automáticas, de las medidas de protección instaladas en nuestros ordenadores, redes y terminales móviles. Estos son los datos más relevantes:

- El 96 % de los ordenadores conectados a Internet están protegidos por mecanismos de *hardware* o *software* que los protegen de accesos no autorizados.
- El 65 % están protegidos por antivirus.
- El 100 % tienen usuarios con privilegios restringidos.
- Con muchos menos años en el mercado, la mitad de los terminales móviles Android (51 %) ya tienen instalado al menos un antivirus.
- Al menos el 65 % de los terminales Android impiden la descarga de aplicaciones de fuentes desconocidas.

Tal vez lo más preocupante sea saber que el 62 % de los ordenadores personales (PC) y un 10 % de los teléfonos móviles tienen instalado algún *malware*[4] (*software* malicioso) de alto riesgo sin que el usuario lo sepa, aunque en este sentido predominan las amenazas que pueden ocasionar menor perjuicio económico: la publicidad *online* no deseada *(adware)*.

A pesar de ser un ámbito mucho menos crítico y con grandes posibilidades de mejora, la situación no parece catastrófica ni mucho menos, pero quizás lo más importante sea la confianza de los usuarios en el uso de Internet, clave para la transformación digital. Aquí la conclusión es inequívoca: el 85 % de la población tiene confianza (de suficiente a mucha) en Internet, el 15 % poca o ninguna y alrededor del 12 % cree que la seguridad en Internet ha empeorado en los últimos años.

En resumen, España reúne las condiciones para realizar una transformación digital sin caer en el descontrol: tiene organismos profesionales especializados, fuerzas de seguridad actualizadas y empresas y población concienciadas. Hay que continuar por este camino, mantener el ritmo de inversión en infraestructuras y en campañas de educación. La «confianza digital» es un tesoro que hay que conservar y hemos de evitar ser engañados por los miles de bulos que circulan acerca de la ciberseguridad.

2. El caso Wakefield y los bulos que matan

Hace algún tiempo Mercedes Núñez, la editora del blog corporativo de Telefónica, Think Big Empresas, me propuso escribir un artículo sobre las analogías entre los virus naturales y los informáticos. Inmediatamente me acordé de una pregunta que me hicieron en un curso de usuarios de PC a principios de la década de 1990. Un alumno preguntó muy seriamente en plena clase: «¿Pueden los virus informáticos transmitirse a los humanos?». En ese momento, contar esta anécdota producía una sonrisa benévola, cuando no un estallido de carcajadas. Ahora la reacción es sustancialmente diferente, sobre todo entre los más sesudos expertos en tecnología y seguridad de la información. Incluso se publican artículos como «¿Nos puede infectar un virus informático?[5]» en periódicos de tirada nacional.

Pero ¿estamos volviéndonos locos o es realmente posible? Vamos por partes.

En general, esto tiene que ver con la tendencia a la creciente incorporación de tecnología *wearable* para el control de enfermedades crónicas (como la diabetes), la prevención o el fomento de hábitos de vida saludable (p. ej., podómetros). La ciencia médica, además, hace años que está trabajando en el desarrollo de órganos artificiales u otros dispositivos que ayudan al funcionamiento de los órganos (como los marcapasos).

Incluso algunos futurólogos hablan de que la especie humana evolucionará hacia verdaderos cíborgs: seres mitad humanos, mitad máquinas. Está de más decir que todos estos elementos se basan en tecnologías digitales. La hiperconectividad actual permite también el control o la monitorización a distancia con una simple conexión inalámbrica a Internet. Es una tendencia irrefrenable por la eficiencia que aporta al sistema sanitario: reducción del número de desplazamientos, menor dedicación de muy costosos recursos especializados y disminución de infraestructuras hospitalarias.

Pero surge la idea de que estos dispositivos digitales (no las personas) pueden ser «infectados» por un virus informático, igual que un PC, porque disponen de un procesador, almacenamiento de datos y conjuntos de instrucciones o programas actualizables y es posible el acceso remoto a través de protocolos de Internet. Además, por reducir costes, muchas veces se basan en versiones de sistemas operativos comerciales muy difundidas en lugar de otras de propósito específico. ¿Estamos condenados entonces a que estos dispositivos sean «infectables»? ¿Corremos grave peligro de que fallen con consecuencias desastrosas frente a un virus informático o, aún peor, frente al ataque de un ciberdelincuente? ¿Tenemos que renunciar al uso de estos dispositivos por estos peligros?

En relación con estas preocupaciones circulan numerosos bulos y exageraciones. Está el caso de Barnaby Jack, el famoso *hacker* neozelandés, programador y experto en seguridad informática, que anunció que había logrado controlar un marcapasos a distancia, teniendo en sus manos la capacidad de alterar su funcionamiento y, por tanto, de causar la muerte de un paciente. Desafortunadamente, nunca pudimos enterarnos de cómo logró controlar el dispositivo médico porque murió pocas horas antes de pronunciarse en una

conferencia en la que iba a explicar su «original procedimiento» para advertir de estas y de otras vulnerabilidades como las que también decía haber encontrado en las bombas de insulina.

Uno puede estar tentado a no tomárselo en serio, pero estos bulos relacionados con la salud literalmente pueden matar. Aunque no por la supuesta «infección por virus informáticos», sino por el bulo en sí. Un buen ejemplo es el de los bulos antivacunas, como el de la vacuna triple vírica (VTV) en el Reino Unido en 1998.

Ese año la revista médica *The Lancet* publicó un trabajo de investigación firmado por Andrew Wakefield que afirmaba que la aplicación de la VTV (frente al sarampión, las paperas y la rubéola) tenía relación con la aparición de autismo y enfermedades gastrointestinales. Esta afirmación, a través de gacetillas y de una conferencia de prensa, llegó a periódicos tan serios como *The Guardian* y *The Independent*.

La alarma social se extendió rápidamente alimentada por Wakefield, quien presentó nuevos trabajos en 2001 y 2002, cuando se publicaron más de 1200 artículos sobre el tema. El temor creció cuando el primer ministro británico en aquel momento, Tony Blair, se negó a confirmar o desmentir si su hijo Leo había sido o no inmunizado con la vacuna, alegando que se trataba de un tema privado. A pesar de que las autoridades sanitarias presentaron otros estudios que demostraban la seguridad de la vacuna, gran parte del público no las creyó.

Como consecuencia, la tasa de vacunación de la VTV cayó del 92 al 61 % entre 1998 y 2003. El número de casos de sarampión se disparó de 56 a 449 en 2006, con una víctima fatal y dos niños que sufrieron graves secuelas, todos por falta de vacunación. Y los casos de paperas se incrementaron 37 veces hasta llegar a cinco mil en 2005. El fenómeno se extendió a países fronterizos como Irlanda, con más de mil quinientos casos y tres muertos en 2000. En 2008 el sarampión se declaró endémico en el Reino Unido.

El 22 de febrero de 2004 una investigación periodística de Brian Deer para *The Sunday Times* reveló que la investigación de Wakefield era un fraude. Algunos de los supuestos niños contagiados de autismo por la vacuna habían sido reclutados por un bufete de abogados para preparar una demanda contra los laboratorios fabricantes de la VTV (es decir, fueron elegidos porque tenían autismo antes de haber sido inoculados con la vacuna). Además, los abogados habían pagado a Wakefield 600 000 € por realizar el estudio y, peor aún, el

médico había presentado una solicitud de patente para una nueva vacuna del sarampión.

Wakefield fue expulsado de la profesión y se le prohibió el ejercicio de la medicina por graves faltas éticas e ignorar conflictos de intereses. Aunque demandó a Brian Deer y a los medios que denunciaron sus actividades, los jueces fallaron en su contra y debió afrontar los costes de las demandas. Ahora es un activista antivacunas y pseudocientífico, pero el bulo de la VTV todavía hoy tiene impacto: la tasa de vacunación en el Reino Unido y en otros países no se ha recuperado aún al nivel precedente; basta comparar las cifras de vacunación contra el coronavirus con las de otros países.

Por eso es muy conveniente la prudencia antes de tachar de inseguros los dispositivos sanitarios y publicar noticias sensacionalistas. Conviene recordar que actualmente cualquier *hardware* y *software* para este uso pasa por numerosos controles de calidad por parte de las autoridades sanitarias de EE. UU. y la UE, además de los propios de la industria (hasta las aplicaciones son fiscalizadas) y los colegios profesionales de las distintas especialidades médicas.

Por supuesto, siempre puede existir un fallo, pero los protocolos actuales y las normas de diseño ciertamente son más exigentes que nunca. Muchas veces, pese a que se puede acceder al dispositivo a través de la Red (para capturar datos o alguna actualización), algunos programas delicados se construyen como un sistema aislado del sistema de acceso remoto y solo se pueden modificar con cambios en el *hardware* o en el *firmware*[6] a través de una consola local.

En definitiva, uno puede estar razonablemente seguro de que si un profesional o un equipo médico indican el uso de estos dispositivos es probablemente la mejor opción a su alcance, y siempre puede contrastarlo con la opinión de otro profesional competente.

Pero, sobre todo, es importante no creer en bulos sin contrastar la información, se trate de «tratamientos milagrosos», denuncias contra la medicina convencional o historias de dispositivos *hackeables* no verificadas. Generalmente ocultan intereses económicos o políticos o incluso patologías mentales. Contribuir a difundirlos, incluso con la mejor intención, puede tener consecuencias imprevisibles y retrasar el desarrollo de una tecnología que puede mejorar la vida de muchas personas. Lo mejor que podemos hacer es desacreditarlos, confrontándolos con la realidad[7].