G Data

Estudio Internacional de Seguridad 2011

¿Cómo perciben los usuarios los peligros de Internet?

Go safe. Go safer. **G Data.**

Contenido

1 Resumen

1.1 Alcance y objetivos del estudio

No hay día en que los medios de comunicación no informen sobre nuevos ataques a internautas y empresas, robos de datos, software malicioso o las estructuras cada vez más organizadas del crimen informático. Los usuarios particulares son un creciente objeto de deseo para los piratas informáticos y cada vez son más las veces que caen víctimas de las mafias de ciberdelincuentes con un ámbito global de actuación. En la *era de Internet* que nos ha tocado vivir tiene una importancia vital proteger la propia identidad digital, en todos los estratos y manifestaciones sociales. Los usuarios pueden recurrir a una variada serie de soluciones informáticas de seguridad para proteger su ordenador personal. Pero ¿hasta qué punto estamos bien informados sobre los peligros reales que acechan en Internet y los métodos de los criminales? Los usuarios más jóvenes ¿están realmente mejor preparados en cuestión de seguridad informática que los más mayores? ¿Quiénes son mejores internautas, las mujeres o los hombres? En su Estudio de Seguridad 2011, una amplia aproximación al tema a nivel internacional, G Data responde a estas preguntas y a muchas más, somete a una mirada crítica diversos mitos de la seguridad informática y enseña a los usuarios a evaluar correctamente los peligros de Internet.

1.2 ¿Conocen bien los internautas los peligros de Internet?

En el '*Estudio de Seguridad 2011'* de G Data, los resultados de las encuestas, es decir, la percepción y valoración personal de los peligros, se han puesto en relación con la amenaza real existente. El análisis muestra que, en muchas áreas, los internautas tienen todavía conocimientos insuficientes y obsoletos.

Casi todos los que participaron en el sondeo tienen una idea general de los peligros de Internet e intentan en consecuencia proteger su ordenador frente a ellos. Pero este saber refleja en muy pocos casos el alcance real de los peligros. Así, nueve de cada diez usuarios de PC afirman que notarían una infección de su ordenador. Según estiman los encuestados, la contaminación se manifestaría mediante extrañas ventanas emergentes o porque el ordenador se haría más lento o dejaría de funcionar del todo. La mayoría de los que respondieron al cuestionario está convencida de que se produciría por lo menos uno de estos síntomas.

Pero los criminales de la Red se proponen ganar la mayor cantidad de dinero posible, por eso, les conviene precisamente que su víctima no note la infección durante el mayor tiempo posible. Por lo general, todos los datos, como la información sobre tarjetas de crédito, los datos bancarios, las claves de acceso a tiendas en línea, las cuentas de correo electrónico, etc. se sustraen al comienzo de la infección. Después se suele incorporar el ordenador a una red de bots que luego, sin conocimiento del usuario, se alquila en foros clandestinos para difundir spam o perpetrar ataques DDoS.

Los piratas de Internet llevan ya un tiempo recurriendo a las redes sociales para propagar su malware y publicando aquí enlaces a webs maliciosas. La difusión de spam y correos con adjuntos infectados no ha desaparecido, pero se ha quedado desfasada, en contra de la creencia de muchos encuestados. En las rutinas de propagación de software malicioso, el spam se usa para atraer a los destina-

tarios a páginas web dañinas y luego infectar el PC mediante el sistema de "*drive-by download*" (descarga silenciosa, véase también el capítulo 3.2.1: Los once mitos de la seguridad en Internet).

Los usuarios tienen una confianza ciega en las redes sociales: Un 35 por ciento confían en los enlaces publicados en su red y un 19 por ciento largo seleccionan enlaces sin importarles la procedencia, con lo que se convierten en un blanco fácil de los delincuentes informáticos y de sus oscuros negocios.

Pero ¿cómo se protegen los usuarios de los ataques? La buena noticia: Solo un once por ciento de los internautas se lanza sin protección a la Red y no usan ningún tipo de antivirus reconocido ni paquetes de seguridad en Internet. El 48 por ciento de los encuestados recurren a programas antivirus gratuitos, pero no los complementan ni con un cortafuegos, ni con un filtro web, programas antiespía o antispam. Y lo que puede parecer más grave: Más del 50 por cierto de estos últimos usuarios cree que tiene instalado un paquete completo de programas con todas estas tecnologías de protección (véase también el apartado 3.1: ¿Cómo se protegen los usuarios de los peligros de Internet?).

Primera conclusión: El Estudio de Seguridad 2011 de G Data pone de manifiesto que los usuarios no valoran correctamente los peligros reales de Internet y un gran porcentaje de los usuarios privados no protegen su ordenador como es debido. Es fácil imaginarse las consecuencias: Demasiada gente está expuesta al peligro de que su ordenador se infecte con malware sin querer. La falta de conocimientos se lo pone muy fácil a los ciberpiratas y autores de malware.

2 Metodología del estudio

El Estudio de Seguridad 2011 de G Data "*Cómo perciben los usuarios los peligros de Internet*" se basa en una encuesta internacional en línea en la que participaron 15.559 internautas de once países con edades comprendidas entre los 18 y los 65 años. Los encuestados respondieron a preguntas sobre los peligros de Internet, el comportamiento de navegación, el uso de soluciones de seguridad y su concienciación con respecto a la seguridad en Internet. Para cada país se creó una página de Internet propia con el mismo catálogo de preguntas en el idioma correspondiente. Los encuestados tenían todos su propio PC con acceso a Internet. La recogida de los datos tuvo lugar entre los meses de febrero y marzo del 2011. Survey Sampling International[1] se encargó de ello por encargo de G Data Software AG. La evaluación y el análisis de los datos se realizó en abril y mayo del 2011.

Tabla 1: Encuestados por edades y sexo

Edad	Hombres	Mujeres	Total
18-24	1273	1430	2703
25-34	1636	1796	3432
35-44	1603	1784	3387
45-54	1585	1647	3232
55-65	1381	1424	2805
Total	**7478**	**8081**	**15559**

[1] En el apéndice encontrará más información sobre Survey Sampling International.

Tabla 2: Encuestados por país

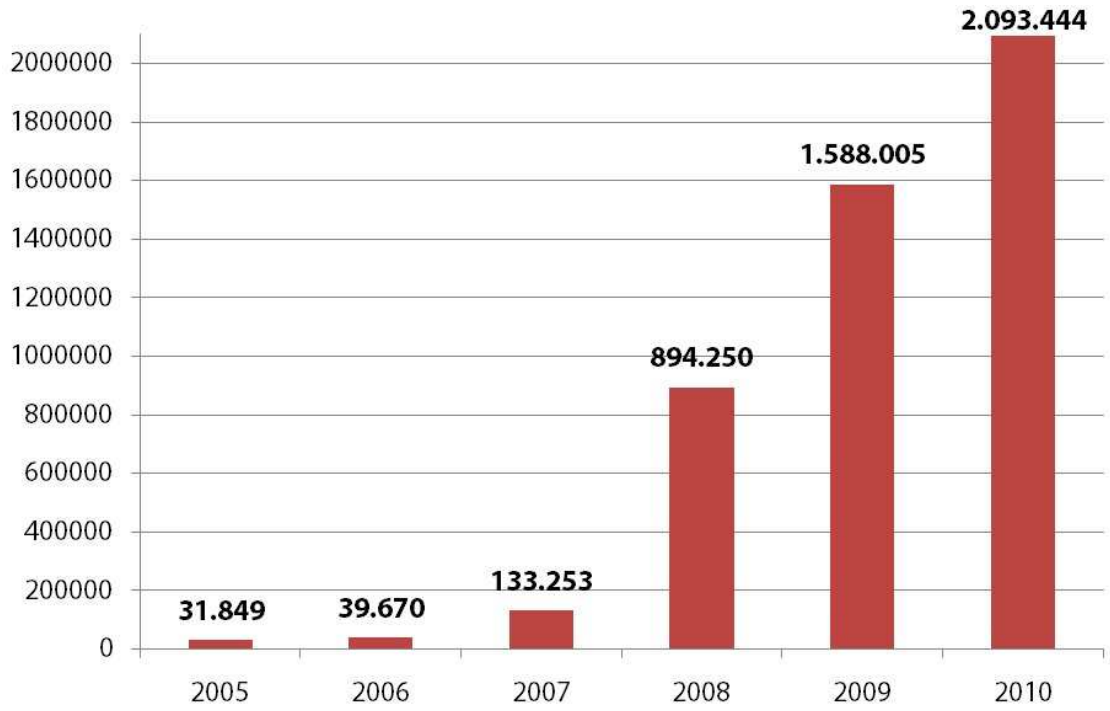
Países	Hombres	Mujeres	Total
Alemania	591	603	1.194
Austria	343	425	768
Bélgica	432	496	928
España	579	579	1158
Estados Unidos	2.646	2.958	5.604
Francia	582	622	1.204
Holanda	336	367	703
Italia	575	563	1.138
Reino Unido	545	561	1.106
Rusia	503	582	1.085
Suiza	346	333	679
Total	**7.478**	**8.081**	**15.559**

3 Resultados del Estudio de Seguridad 2011 de G Data

En los últimos años se ha registrado un notable aumento de los ataques informáticos a empresas y usuarios particulares. El crimen informático se ha convertido desde no hace tanto tiempo en un pingüe y muy rentable negocio y los delincuentes aplican los más variados métodos en sus ataques para infectar los ordenadores con programas intrusivos y robar a sus víctimas todos los datos imaginables, que luego se venden al mejor postor.

Solo durante el pasado año G Data registró más de dos millones de nuevos programas dañinos para los sistemas Windows[2].

Diagrama 1: Número de nuevos programas de malware al año desde 2005



Los criminales propagan su software malicioso por varios canales: Una posibilidad es colocar los programas dañinos en las páginas de Internet. Basta con visitar una de estas páginas contaminadas por el método de descarga silenciosa (*drive-by-download*) para infectar el ordenador con virus, troyanos, programas espía y otros programas lesivos. El usuario tropieza con estas páginas adulteradas al navegar por la Red o bien los delincuentes publican sus enlaces en las redes sociales o mediante mensajes en los programas de chat. Los piratas siguen usando correos basura para atraer con enlaces a los usuarios a las páginas engañosas o para hacer que abran adjuntos infectados. En los mensajes de correo, por ejemplo, se hace referencia a supuestas facturas, recordatorios de pago o fotos exclusivas sobre un tema de actualidad. Si los usuarios responden a estas invitaciones, aterrizan directamente en páginas maliciosas y acaban hospedando, sin por supuesto notarlo, un programa intrusivo en su ordenador.

[2] Véase también el Informe sobre malware 2/2010 de G Data, http://www.gdata.es/ueber-g-data/pressecenter/pressemeldungen/news-details/article/1888-cada-15-segundos-se-libera.html

Los usuarios solo pueden protegerse de estos peligros con la ayuda de una solución completa de seguridad y haciendo además un uso prudente de Internet.

3.1 ¿Cómo se protegen los usuarios de los peligros de Internet?

El resultado del '*Estudio de Seguridad 2011*' de G Data nos demuestra que más del 89 por ciento de los más de 15.500 usuarios encuestados usan software de seguridad en su sistema. De estos, el 48 por ciento se confía a programas gratuitos.

Diagrama 2: ¿Qué soluciones de seguridad han instalado los usuarios en sus sistemas?

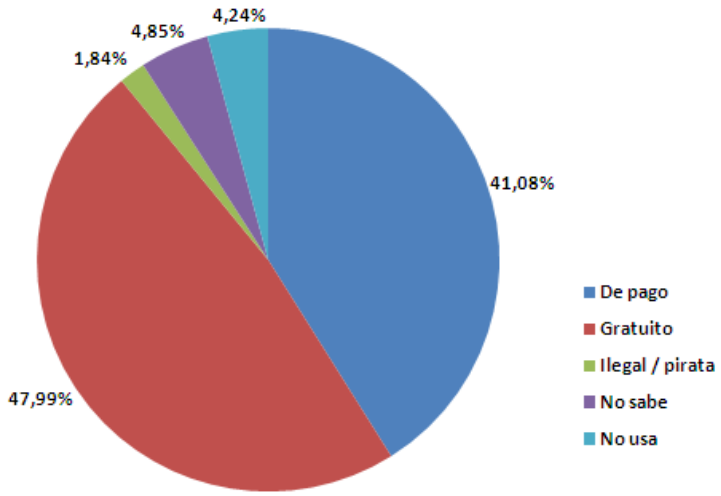


Tabla 3: Resultados de la pregunta por la solución de seguridad que tienen instalada los usuarios

¿Qué software de seguridad usas en tu PC?					
	De pago	**Gratuito**	**Ilegal / pirata**	**No sabe**	**No usa**
Hombres (18-24)	39,83%	43,99%	4,08%	4,87%	7,23%
Hombres (25-34)	42,60%	47,37%	2,14%	2,87%	5,01%
Hombres (35-44)	42,98%	47,16%	1,62%	3,93%	4,30%
Hombres (45-54)	42,15%	50,41%	1,32%	2,84%	3,28%
Hombres (55-64)	44,97%	48,08%	1,16%	2,68%	3,11%
Total Hombres	**42,55%**	**47,53%**	**2,01%**	**3,40%**	**4,52%**
Mujeres (18-24)	34,69%	51,47%	2,10%	6,08%	5,66%
Mujeres (25-34)	40,81%	47,05%	2,62%	5,57%	3,95%
Mujeres (35-44)	42,60%	46,92%	1,51%	5,44%	3,53%
Mujeres(45-54)	40,80%	48,33%	1,09%	6,86%	2,91%
Mujeres (55-64)	38,48%	49,02%	1,05%	7,30%	4,14%
Total Mujeres	**39,71%**	**48,41%**	**1,70%**	**6,20%**	**3,98%**
Total	**41,08%**	**47,99%**	**1,84%**	**4,85%**	**4,24%**

En comparación con el resto de países que participan en el '*Estudio de Seguridad 2011*', Gran Bretaña se desmarca positivamente: Más del 94 por ciento de los encuestados usan una solución de seguridad. El porcentaje más reducido corresponde a Rusia, con casi el 83 por ciento. Vemos por lo tanto que en todos los países cuatro quintas partes, por lo menos, de los encuestados usan un software de seguridad.

Diagrama 3: Soluciones de seguridad que han instalado los usuarios en sus sistemas, visto por países

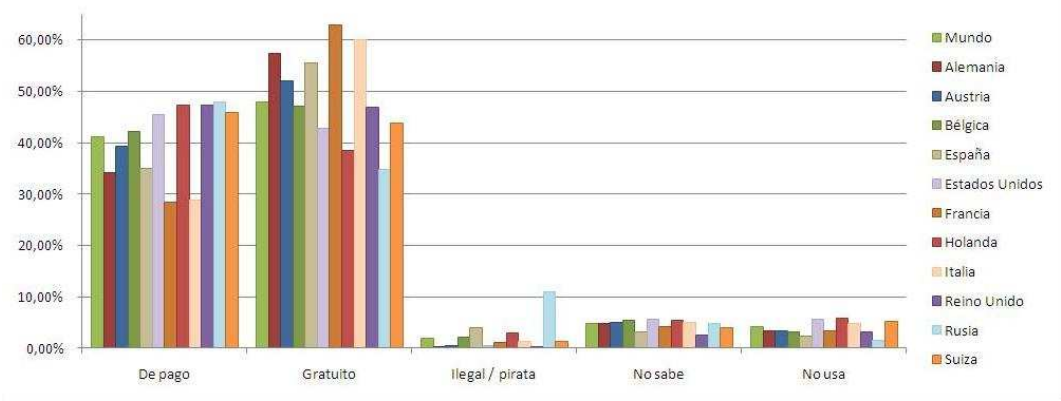


Tabla 4: Resultados en detalle de los países: ¿Qué solución de seguridad han instalado los usuarios?

¿Qué software de seguridad usas en tu PC?					
	De pago	Gratuito	Ilegal / pirata	No sabe	No usa
Hombres (18-24)	39,83%	43,99%	4,08%	4,87%	7,23%
Hombres (25-34)	42,60%	47,37%	2,14%	2,87%	5,01%
Hombres (35-44)	42,98%	47,16%	1,62%	3,93%	4,30%
Hombres (45-54)	42,15%	50,41%	1,32%	2,84%	3,28%
Hombres (55-64)	44,97%	48,08%	1,16%	2,68%	3,11%
Total Hombres	**42,55%**	**47,53%**	**2,01%**	**3,40%**	**4,52%**
Mujeres (18-24)	34,69%	51,47%	2,10%	6,08%	5,66%
Mujeres (25-34)	40,81%	47,05%	2,62%	5,57%	3,95%
Mujeres (35-44)	42,60%	46,92%	1,51%	5,44%	3,53%
Mujeres(45-54)	40,80%	48,33%	1,09%	6,86%	2,91%
Mujeres (55-64)	38,48%	49,02%	1,05%	7,30%	4,14%
Total Mujeres	**39,71%**	**48,41%**	**1,70%**	**6,20%**	**3,98%**
Total	**41,08%**	**47,99%**	**1,84%**	**4,85%**	**4,24%**

Los usuarios pueden combinar el software antivirus gratuito con otras herramientas también sin costo. Pero no obstante puede surgir el problema de que alguno de estos programas sea incompatible con la solución de seguridad utilizada.

Entre los componentes más importantes para proteger con efectividad el ordenador tenemos, además del antivirus, un cortafuegos personal, un filtro antispam y, también muy importante, un filtro de protección de Internet. G Data ofrece en esta área con G Data CloudSecurity un plugin gratuito para el navegador que es compatible con todas las soluciones de protección antivirus[3].

[3] Más información sobre el filtro gratuito de protección Web: http://www.free-cloudsecurity.com

3.1.1 ¿Qué opinión les merece a los internautas el rendimiento de las soluciones antivirus gratuitas?

Las vías de entrada de una infección en el PC son, como hemos visto ya, tan variadas como sofisticadas, pero las soluciones de seguridad más completas son capaces de proteger al usuario de todos estos peligros. Sin embargo, los programas antivirus gratuitos no tienen esta capacidad, si los analizamos bien. Porque no contienen las tecnologías de seguridad que son fundamentales para asegurar una protección exhaustiva. Podemos mencionar aquí los filtros antispam y de protección Web, el cortafuegos, el sistema de reconocimiento del código dañino en función del comportamiento o la seguridad en la nube.

A la vista de estos apuntes, se preguntó a los usuarios cómo valoraban el rendimiento y la calidad de los programas gratuitos de protección. Casi el 44 por ciento de los encuestados colocaban la calidad y funcionamiento del software de seguridad gratuito al nivel de las soluciones de pago.

Diagrama 4: Evaluación del rendimiento: El software de seguridad gratuito ¿es igual de bueno que las soluciones de seguridad de pago?

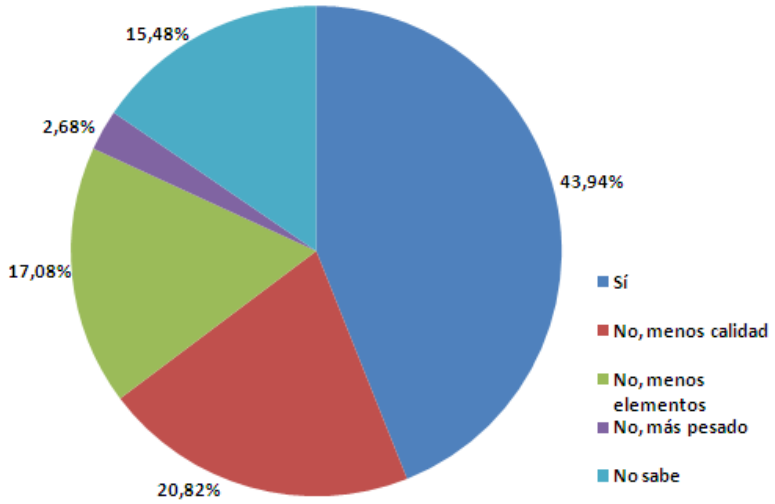


Tabla 5: Resultados en detalle de esta pregunta: ¿Valoran los usuarios igual las soluciones de seguridad gratuitas y de pago si atendemos a la calidad y al margen de funciones?

¿Es el software de seguridad gratuito tan eficaz como el de pago?					
	Sí	No, menos calidad	No, menos elementos	No, más pesado	No sabe
Hombres (18-24)	42,42%	25,69%	17,67%	2,83%	11,39%
Hombres (25-34)	46,03%	23,96%	17,30%	3,30%	9,41%
Hombres (35-44)	45,60%	22,46%	17,90%	2,87%	11,17%
Hombres (45-54)	42,84%	22,02%	19,05%	2,52%	13,56%
Hombres (55-64)	42,87%	20,71%	19,48%	2,32%	14,63%
Total Hombres	**44,06%**	**22,92%**	**18,27%**	**2,78%**	**11,97%**
Mujeres (18-24)	43,64%	22,10%	17,97%	2,45%	13,85%
Mujeres (25-34)	44,82%	21,27%	16,31%	3,29%	14,31%
Mujeres (35-44)	43,39%	20,74%	15,92%	2,30%	17,66%
Mujeres (45-54)	43,47%	16,03%	15,48%	2,19%	22,83%
Mujeres (55-64)	43,75%	13,55%	14,26%	2,67%	25,77%
Total Mujeres	**43,83%**	**18,87%**	**15,99%**	**2,59%**	**18,72%**
Total	**43,94%**	**20,82%**	**17,08%**	**2,68%**	**15,48%**

En la comparación de países, Francia encabeza la lista: El 53 por ciento de las personas encuestadas en este país no ve ninguna diferencia entre las soluciones de seguridad gratuitas y las de pago. Los holandeses participantes, en comparación, presentan la confianza más baja y apenas el 35 por ciento creen en la equivalencia de características entre el software de seguridad de pago y el gratuito.

Diagrama 5: Evaluación del rendimiento de las soluciones de seguridad gratuitas por países

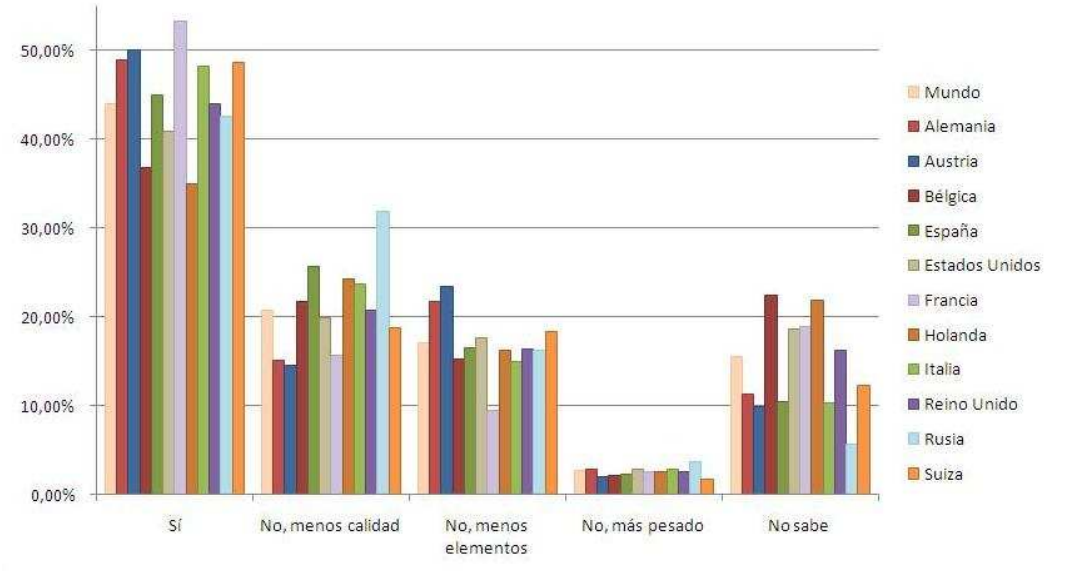


Tabla 6: Resultados por países: El software de seguridad gratuito ¿los encuestados lo consideran equivalente a las soluciones de seguridad de pago?

¿Es el software de seguridad gratuito tan eficaz como el de pago?					
	Sí	No, menos calidad	No, menos elementos	No, más pesado	No sabe
Mundo	43,94%	20,82%	17,08%	2,68%	15,48%
Alemania	48,91%	15,08%	21,78%	2,85%	11,39%
Austria	50,00%	14,58%	23,44%	2,08%	9,90%
Bélgica	36,85%	21,77%	15,30%	2,16%	22,41%
España	45,04%	25,74%	16,52%	2,26%	10,43%
Estados Unidos	40,94%	19,91%	17,68%	2,82%	18,65%
Francia	53,32%	15,70%	9,47%	2,66%	18,85%
Holanda	34,99%	24,32%	16,22%	2,56%	21,91%
Italia	48,15%	23,72%	14,94%	2,81%	10,37%
Reino Unido	44,03%	20,71%	16,46%	2,62%	16,18%
Rusia	42,58%	31,89%	16,22%	3,69%	5,62%
Suiza	48,60%	18,85%	18,41%	1,77%	12,37%

3.1.2 Número de ordenadores desprotegidos

Los usuarios parecen estar concienciados, en general, sobre la necesidad de proteger su ordenador personal. Entre todos los participantes en la encuesta encontramos una tasa relativamente baja de ordenadores desprotegidos. Solo un poco por encima del 4 por ciento (ver Diagrama 2), o, en cifras absolutas, 659 usuarios encuestados. Una buena noticia, por lo tanto. Pero casi otro 5 por ciento de los internautas no sabía dar cuenta de si tenía o no instalado en su sistema una solución de seguridad. Además, el 1,84 por ciento de las personas sondeadas admitió espontáneamente que usaban copias piratas. De estos datos se puede inferir que al menos un 6 por ciento, aproximadamente, de todos los participantes en la entrevista, se mueven en Internet sin protección. Además es presumible que también estén desprotegidos los encuestados que no saben si utilizan una solución de seguridad.

Los internautas rusos, poco concienciados con respecto a la seguridad

En comparación con otros países, en Rusia se encuentra el mayor porcentaje de ordenadores sin proteger. Los usuarios de aquí son los que más recurren a versiones ilegales de las soluciones de seguridad de pago, con una proporción cercana al 11 por ciento. En total, en Rusia un 17 por ciento de los PCs no está suficientemente protegido frente a los peligros de Internet. El Reino Unido ocupa la cabecera de la lista, en sentido positivo. Aquí apenas el seis por ciento de los participantes del sondeo dan respuestas que permiten inferir que no están protegidos.

3.1.3 ¿Suite de programas o solo antivirus?

Diagrama 6: ¿Qué solución de seguridad han instalado los usuarios?

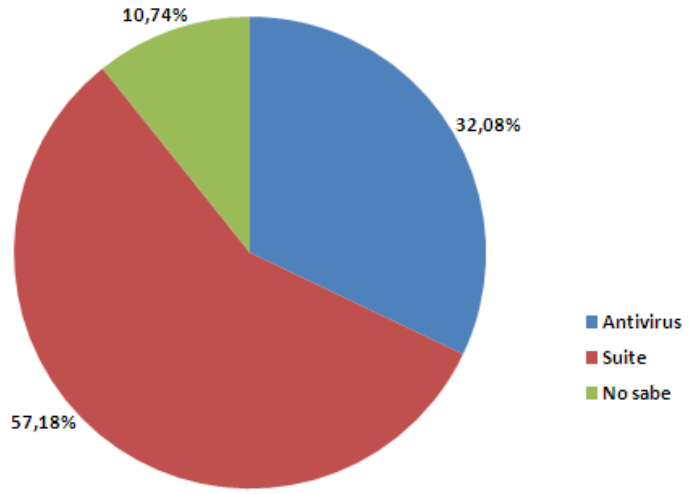


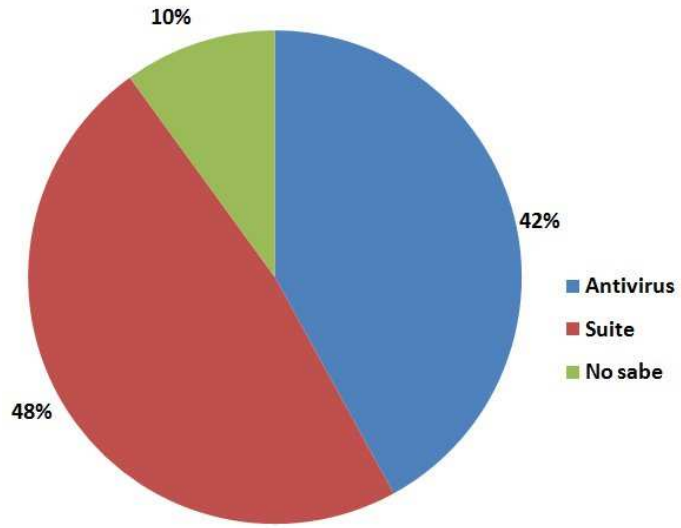
Tabla 7: Los resultados en detalle a la pregunta sobre la solución de seguridad instalada

¿Qué tipo de solución antivirus tienes instalada en tu PC?			
	Antivirus	**Suite**	**No sabe**
Hombres (18-24)	37,00%	55,29%	7,71%
Hombres (25-34)	35,52%	59,52%	4,95%
Hombres (35-44)	32,46%	60,69%	6,84%
Hombres (45-54)	29,55%	63,54%	6,91%
Hombres (55-64)	29,67%	62,93%	7,40%
Total Hombres	**32,73%**	**60,57%**	**6,69%**
Mujeres (18-24)	36,03%	52,34%	11,64%
Mujeres (25-34)	33,86%	53,39%	12,75%
Mujeres (35-44)	29,92%	56,13%	13,95%
Mujeres (45-54)	28,71%	56,29%	15,01%
Mujeres (55-64)	29,23%	51,36%	19,41%
Total Mujeres	**31,49%**	**54,05%**	**14,46%**
Total	**32,08%**	**57,18%**	**10,74%**

Los internautas saben bien que hay muchos peligros acechando en Internet y que hay que protegerse contra ellos; ¿o quizá no tan bien? Si tomamos los resultados de la pregunta formulada antes (véase el diagrama 2) con el enunciado "¿Qué software de seguridad tienes instalado en su ordenador?", sale a la luz una curiosa contradicción, a saber:

Las soluciones de seguridad gratuitas constituyen exclusivamente antivirus sin más, sin otras tecnologías de protección, como un cortafuegos, antispam o protección web. Actualmente no hay en el mercado ningún paquete de seguridad gratuito. No obstante, la mayoría de los encuestados que habían afirmado antes utilizar una solución antivirus gratuita (32%, véase diagrama 7), aseguran ahora tener en uso una suite de seguridad en Internet con cortafuegos personal, antispam y protección web (48%, diagrama 8).

Diagrama 7: Solución de seguridad instalada por los usuarios que afirmaban usar una solución de seguridad gratuita



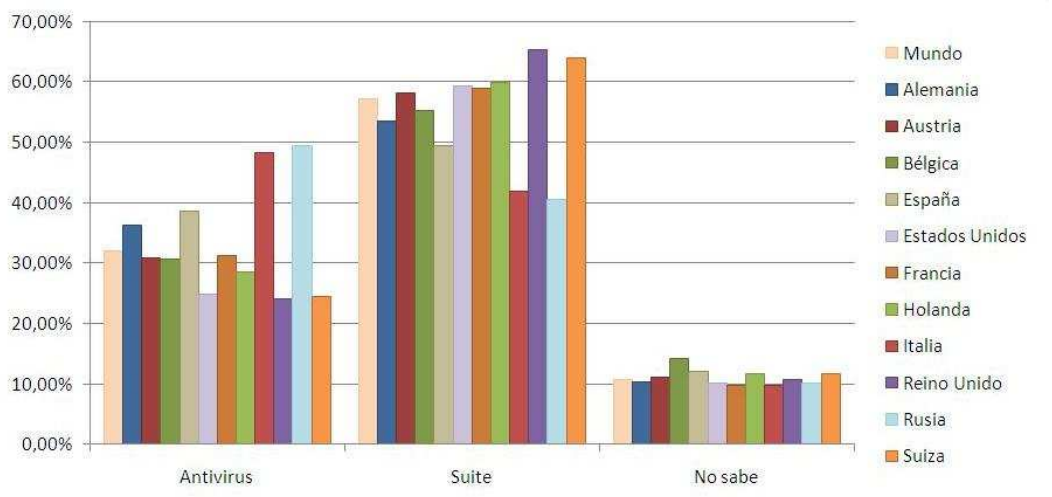
¿Qué nos dice esta aparente contradicción? La mayoría de los usuarios finales sondeados parecen tener una idea equivocada de la gama de funciones de los puros programas antivirus en comparación con las suites de seguridad en Internet y aparentemente no están bien informados sobre las tecnologías integradas de protección. Por eso la mayoría considera equivalentes los antivirus gratuito y los paquetes o suites de seguridad, sin apreciar las diferencias tecnológicas. Este error de estimación puede salirles caro a los internautas si observamos las distintas vías de difusión del código dañino.

Tabla 8: Soluciones de seguridad instaladas por países

¿Qué tipo de solución de seguridad tienes instalada en tu PC?			
	Antivirus	**Suite**	**No sabe**
Mundo	32,08%	57,18%	10,74%
Alemania	36,17%	53,51%	10,32%
Austria	30,86%	58,09%	11,05%
Bélgica	30,70%	55,17%	14,13%
España	38,52%	49,47%	12,01%
Estados Unidos	24,93%	59,35%	10,12%
Francia	31,30%	58,90%	9,80%
Holanda	28,55%	59,82%	11,63%
Italia	48,30%	41,92%	9,78%
Reino Unido	24,04%	65,33%	10,63%
Rusia	49,44%	40,45%	10,11%
Suiza	24,42%	63,92%	11,66%

Si analizamos el panorama por países, el porcentaje de usuarios de un paquete de seguridad también es mayor que el de usuarios de antivirus. Italia y Rusia son la excepción: Aquí las proporciones se invierten (véase tabla 8)

Diagrama 8: Soluciones de seguridad instaladas por países

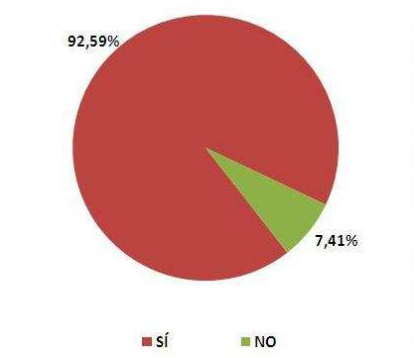


3.2 ¿Dónde esperan los internautas las mayores amenazas?

G Data, con el objetivo de hacerse una idea de dónde ponen los internautas sus temores en materia de cibercrimen, ha confrontado a los encuestados con once afirmaciones erróneas, entre otros enunciados. El resultado obtenido es que algunos de los encuestados creyeron correctas estas afirmaciones falsas. Por eso, las hemos denominado aquí "las once tesis de la seguridad en Internet".

3.2.1 Las once tesis de la seguridad en Internet

Tesis n.° 1: Cuando mi sistema está infectado con malware, lo voy a notar de alguna manera en el PC (93 por ciento).



Esta primera conjetura es la más difundida. Casi todos los internautas (el 93 por ciento, para ser exactos) de todo el globo están convencidos de que los programas intrusivos tienen un efecto perceptible en el ordenador. Así, el 45 por ciento de los participantes en el sondeo suponen que el ordenador falla inmediatamente al infectarse con malware. Casi el 57 por ciento presume que, por lo menos, algunas funciones iban a resultar afectadas o que algunos programas de software dejarían de funcionar. El 58 por ciento piensa que en el ordenador aparecerían ventanas emergentes y/o se oirían ruidos raros si estuviera infectado. Por fin, casi el 57 de los encuestados cuenta con que el ordenador se ralentizaría. Menos del 7,5 por ciento sostiene que en caso de contaminación no se percibiría nada extraño, que es justo lo que realmente pasa en la mayoría de los casos (véase la tabla 9).

Tabla 9: A juicio de los encuestados, ¿qué es lo que pasa cuando el ordenador está infectado? Se podían elegir varias respuestas

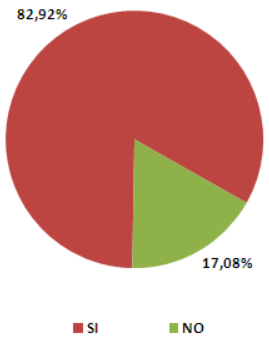
¿Qué sucede cuando se infecta tu PC?					
	Se bloquea / colapsa por completo	Algunos elementos dejan de funcionar	Aparece pop-ups y/o sonidos	Funciona más lento	Nada especial
Hombres (18-24)	43,52%	52,24%	56,64%	58,84%	10,45%
Hombres (25-34)	43,52%	57,46%	58,31%	59,96%	8,37%
Hombres (35-44)	46,35%	56,33%	58,58%	57,70%	7,99%
Hombres (45-54)	41,83%	54,57%	58,36%	57,03%	8,83%
Hombres (55-64)	37,44%	57,42%	54,89%	55,10%	7,10%
Total Hombres	**42,65%**	**55,71%**	**57,46%**	**57,77%**	**8,50%**
Mujeres (18-24)	48,46%	58,18%	64,06%	62,52%	6,43%
Mujeres (25-34)	50,17%	59,30%	64,37%	58,13%	5,57%
Mujeres (35-44)	47,48%	57,51%	57,12%	55,27%	7,29%
Mujeres (45-54)	46,81%	57,86%	56,22%	53,25%	5,65%
Mujeres (55-64)	46,00%	57,23%	50,56%	48,17%	7,16%
Total Mujeres	**47,85%**	**58,05%**	**58,62%**	**55,53%**	**6,40%**
Total	**45,35%**	**56,93%**	**58,06%**	**56,60%**	**7,41%**

En el pasado, los programas dañinos los escribían informáticos que querían poner a prueba sus habilidades técnicas. Si uno de estos programas conseguía contaminar un ordenador, la víctima lo notaba por las ventanas emergentes, fallos de funcionamiento o el fallo total y repentino del ordenador. Al parecer, mucha gente sigue acordándose bien de estas experiencias. Hoy en día, son criminales profesionales y con un alto nivel técnico los que programan código malicioso con la finalidad de apoderarse de la mayor cantidad de dinero posible.

Un elemento dañino bien programado permite ganar mucho dinero en el mercado negro de Internet. El código del programa se vende a otros delincuentes, quienes, a su vez, pueden utilizarlo por ejemplo para formar una red de bots que les proporcione una capacidad de computación lo más amplia posible con ordenadores infectados repartidos por todo el globo. Con estas redes de PCs zombis se pueden ejecutar, por ejemplo, ataques DDoS, enviar spam o difundir virus. Este tipo de economía sumergida está muy desarrollada. Los programadores y los administradores de las redes de zombis ofrecen sus conocimientos y sus servicios como prestaciones especiales en foros clandestinos a propósito. Otros criminales compran servicios o código malicioso en estas plataformas, por ejemplo para orquestar un ataque a la página web de una empresa o para iniciar una gran campaña de spam. Todo esto requiere un know how tecnológico específico.[4]

Los programadores y administradores de las redes de bots pretenden que su red sea lo más grande y estable posible. Esto significa que cada PC rescatado de su particular rebaño, por ejemplo al descubrirse y eliminarse la infección, supone una pérdida financiera para los hackers. Por eso, los creadores de malware construyen sus programas de tal manera que el usuario no note la infección. Vistas estas razones, hoy en día es muy improbable que una infección del PC se haga patente mediante caídas del sistema, restricciones de la velocidad del ordenador, ventanas emergentes sospechosas u otras características de este tipo. Esta evolución es muy peligrosa para los usuarios porque únicamente una infección detectada rápidamente puede también eliminarse con celeridad. Tampoco mejora la situación en absoluto que –a estas alturas– nueve de cada diez usuarios crean que el malware es fácil de detectar. Cuando su ordenador funciona sin incidencias, estos usuarios se figuran que no puede estar contaminado. Esta creencia es una baza que los ciberpiratas saben jugar a la perfección.

Tesis n.° 2: El software antivirus gratuito y los paquetes de software de pago ofrecen las mismas funciones de protección (83 por ciento)

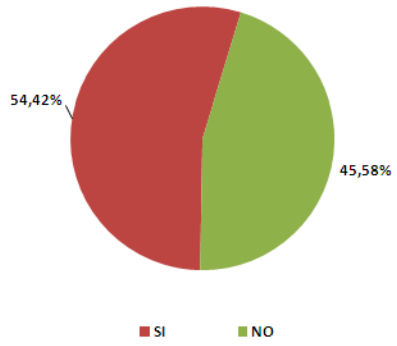


Esta afirmación errónea cuenta con el asentimiento de la mayoría de los consultados, un 83 por ciento. En la pregunta sobre las diferencias de calidad entre los productos de seguridad gratuitos (véase tabla 6), la mayoría de los participantes en la encuesta -el 56 por ciento- tiene sus dudas sobre si las dos clases de software son realmente equivalentes. No obstante muchos de ellos no son capaces de precisar las diferencias. El 15 por ciento de los entrevistados admitieron no conocer los resultados de las comparati-

[4] Encontrará más información sobre la economía sumergida virtual en el Libro Blanco sobre la cibereconomía sumergida de G Data: http://www.gdatasoftware.com/information/security-labs/information/whitepaper.html

vas de rendimiento entre los productos de seguridad gratuitos y las soluciones comerciales. Casi el 3 por ciento de los encuestados piensa que la diferencia radica en la carga exigida al sistema: Los productos gratuitos cargan el sistema en mayor medida que las soluciones de pago. Las ofertas gratuitas y de pago se diferencian sobre todo en las tecnologías de seguridad que incluyen. El software gratis ofrece un antivirus sin más. El software de seguridad de pago comprende más elementos de seguridad: Además del antivirus, estos productos suelen contar con un filtro http, un cortafuegos, un módulo antispam y un sistema de reconocimiento comportamental de código dañino. Pero solo un 17 por ciento de los entrevistados lo sabe en esta pregunta.

Tesis n.° 3: La mayor parte del malware se propaga por correo electrónico (un 54 por ciento).



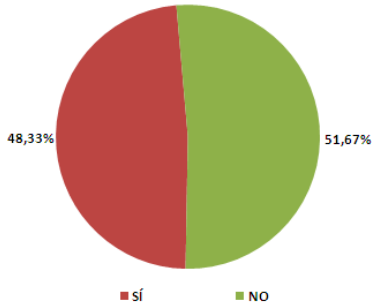
Esta suposición se ha quedado tan obsoleta como la primera tesis, pero a pesar de todo siguen creyéndosela el 54 por ciento de los entrevistados.

Es verdad que con "Melissa" y "I love you", a finales del pasado milenio, los e-mails fueron la vía más frecuente de difusión de malware. Las infecciones se producían por archivos adjuntos adulterados que mediante métodos de ingeniería social se presentaban especialmente tentadores para la víctima.

Muchos se acordarán todavía de los correos que prometían fotos de desnudos de Anna Kurnikova, la famosa tenista rusa. La realidad era muy diferente: al abrir este adjunto se instalaba un virus en el PC. Desde hace unos seis años, los archivos adjuntos a los correos se sustituyen cada vez más por enlaces maliciosos a páginas web (aunque desde hace unos meses hemos registrado un nuevo florecimiento de los adjuntos). Esta táctica permite a los hackers eludir los filtros de spam, por lo demás tan efectivos, para que llegasen a manos de usuarios desprevenidos.

Por otro lado, muchos usuarios se han hecho muy precavidos y cuando reciben correos de remitentes desconocidos, prefieren borrarlos inmediatamente sin abrirlos antes. Es archiconocido que los enlaces en los correos electrónicos suelen llevar a páginas web engañosas. Así las cosas, no es de extrañar que los delincuentes busquen otras formas de llegar a las víctimas: Por ejemplo, por las redes sociales (véase el apartado 3.3), optimizando las búsquedas, desarrollando "dominios con errores tipográficos", etc. Los programas dañinos se han mudado a las páginas web y estas páginas son, hoy por hoy, el factor infeccioso número uno.

Tesis n.° 4: Un PC no se puede infectar simplemente por cargar una página dañina (48 por ciento).

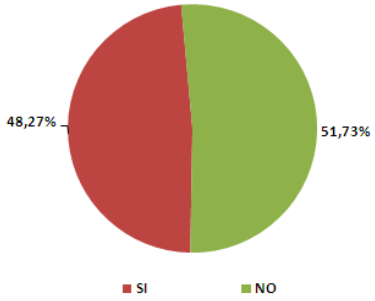


Deja helado que casi la mitad de los internautas esté de acuerdo con esta afirmación. Hace años ya que se puede infectar un ordenador a través de las que podríamos denominar como "*descargas silenciosas*" (drive-by download). Para la infección basta con entrar en una página de Internet convenientemente preparada. Así que queda patente lo erróneo que es pensar que no es suficiente con cargar la página, porque lo cierto es que este tipo de ataque se practica a gran escala.

Hay dos variantes de infecciones '*drive-by-download*': Por un lado, hay páginas web que han sido creadas con el objetivo de infectar ordenadores. Los criminales de la Red intentan atraer a sus víctimas al sitio infectado, publicando en las redes sociales un enlace con una descripción interesante, con publicidad de banners o mediante correos electrónicos con el link incorporado.

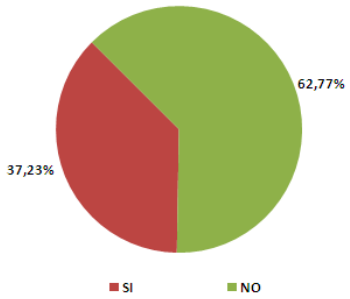
Otra variante es si cabe más sutil: En una página web popular, con un número de visitas aceptable y digna de confianza, se infiltra código dañino. Por ejemplo, se abre una ventana de, por ejemplo, 0x0 píxeles, invisible para el internauta. En ella se inicia una descarga que infecta el ordenador del usuario con programas maliciosos de forma subrepticia y automática. Este segundo método tiene la ventaja para los hacker de que no necesitan hacer publicidad de la página web. Pero para lograr su objetivo, los ciberdelincuentes deben hackear la página y manipularla. Si el sitio está protegido -lo que, por cierto, se puede decir solo de una pequeña parte de las páginas web- puede resultar muy difícil forzarlo.

Tesis n.° 5: La mayor parte de los virus y software dañino se propaga por archivos en las plataformas de intercambio como las redes P2P y los sitios de torrents (48 por ciento).



Es un hecho incontrovertible que por las plataformas de intercambio, como los sitios de torrents y redes P2P, circula gran cantidad de programas dañinos. Por eso no debe sorprender que el 48 por ciento de los participantes del sondeo tenga la impresión de que éste es el principal método de propagación de malware. Puede incluso que alguno de estos usuarios ya haya experimentado la infección de su sistema por participar activamente en este tipo de páginas. Pero tampoco esta tesis es verdad porque la mayor parte de los programas nocivos se propagan mediante páginas web adulteradas, como hemos expuesto antes.

Tesis n.° 6: En las páginas web de pornografía hay mayor peligro de toparse con malware que, por ejemplo, al entrar en sitios web sobre equitación o viajes (37 por ciento).

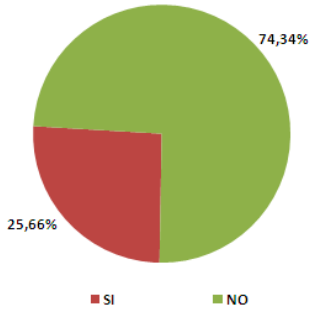


La pornografía tiene una reputación más que dudosa. Por eso no es raro que mucha gente (el 37 por ciento de las personas sondeadas) se figure aquí una relación con el cibercrimen. Pero no es un hecho incontrovertible que los sitios porno estén de verdad infectados con mayor frecuencia que las páginas web dedicadas, por ejemplo, a la hípica o a otras actividades de ocio.

En la industria del porno se gana mucho dinero. Para el propietario de un sitio de pornografía, la página web constituye su principal fuente de ingresos y, por eso mismo, suele encargar su programación, mantenimiento y seguridad a profesionales. Un cliente de pago que infecta con malware su PC por visitar la página, sería un cliente perdido para el empresario de la página y le supondría una pérdida financiera.

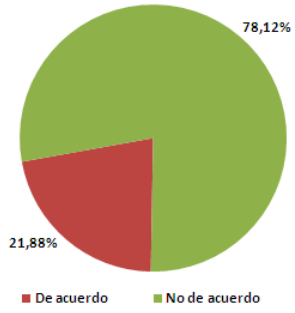
Un sitio de aficionados tendrá un administrador que quizá no sea un diseñador profesional de páginas web y por eso puede que no actualice con regularidad el software ni instale los parches necesarios para cerrar los agujeros de seguridad. Para los criminales es mucho más fácil penetrar en estas páginas web e infiltrar en ellas código dañino que en sitios profesionales y muy protegidos, como muchas veces son las páginas de contenido adulto. En general, las páginas pornográficas pueden suponer un mayor riesgo si proceden de proveedores poco recomendables. Los sitios serios dedicados al sexo no representan un potencial de riesgo tan alto.

Tesis n.° 7: Mi cortafuegos me protege de las infecciones por descarga silenciosa (drive-by download) (26 por ciento).



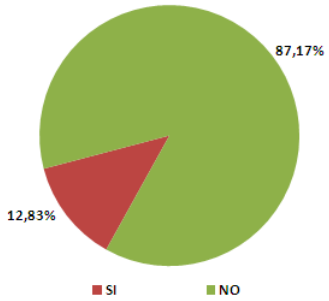
Esta afirmación se la creen aproximadamente el 26 por ciento de los encuestados. Pero está equivocada. Los cortafuegos son, ciertamente, un componente importante de un sistema de protección para el ordenador. Pero solo mediante un cortafuegos no es posible proteger un PC con eficacia frente a las infecciones *drive-by-download*. Para obtener una protección efectiva y suficiente, el internauta precisa además una solución de seguridad completa, con protección web integrada. Incluso cuando la infección se ha culminado, un cortafuegos no es siempre capaz de impedir que el programa intrusivo realice sus rutinas dañinas, como por ejemplo que los programas espía envíen datos sensibles a los criminales.

Tesis n.° 8: Si no se abre ningún archivo infectado, el PC tampoco puede llegar a infectarse (22 por ciento).



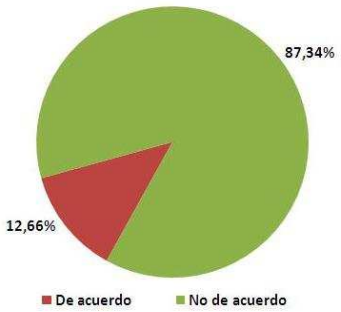
Esta aseveración se basa en hechos anticuados, que se han mantenido hasta ahora en forma de saber popular y que, en este caso, forma parte del acervo de creencias de casi el 22 por ciento de los entrevistados. Por supuesto, se siguen produciendo infecciones cuando los usuarios abren archivos peligrosos. Una ejecución automática de archivos dañinos solo es posible cuando los atacantes se pueden aprovechar de algún agujero de seguridad y en este caso el código dañino se activa automáticamente sin tener que abrir el archivo infectado. Por eso, siempre se debe partir de la base de que los archivos infectados representan un peligro para el usuario y que pueden llegar a ejecutarse independientemente de la actuación de éste.

Tesis n.° 9: La mayor parte del malware se propaga por memorias USB (un 12,83 por ciento)



Llegados a este punto ya hemos constatado que la mayor parte de los programas dañinos se difunden mediante páginas fraudulentas, lo que no quita que existan otras vías de infección. En la década de los ochenta y de los noventa, cuando Internet todavía no era omnipresente, los disquetes constituían con frecuencia un foco de infección. En los últimos años ha aumentado considerablemente la querencia de los hackers por las memorias USB y otros medios USB portátiles. Aquí usan en su provecho las funciones de autoinicio de los soportes de datos para que se ejecuten programas dañinos al conectar el medio al PC. El ejemplo más célebre es el gusano Conficker. Por esta razón es muy recomendable desactivar la función de reproducción automática del sistema operativo. Así se evita la instalación automática de un gusano al conectar la memoria USB con el ordenador.

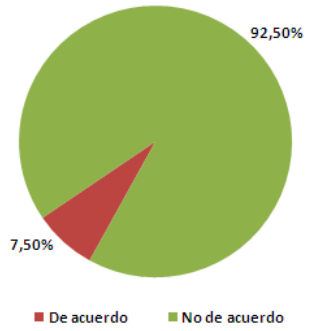
Tesis n.° 10: No visito sitios peligrosos… luego no estoy expuesto a infecciones por descarga silenciosa (‘*drive-by download*’, 13 por ciento)



Esta afirmación se puede refutar del mismo modo que la sexta tesis (las páginas porno entrañan un mayor peligro de dar con malware que, por ejemplo, visitar páginas sobre equitación o viajes). Los ciberpiratas no se fijan en el contenido de una página web. Solo les interesa poder infectar con código dañino el mayor número de visitantes aplicando el menor esfuerzo posible. Los delincuentes consiguen este objetivo, por ejemplo, manipulando los banner publicitarios y atacando continuamente los grandes dominios. Si tienen éxito y consiguen abrirse paso en el website elegido, pueden copiar en él código dañino con alguna herramienta ad hoc (las conocidas como ‘web exploit toolkit’) sin nece-

sidad de conocimientos técnicos. De este modo, páginas web con buena reputación pueden de pronto estar hackeadas y entrañar por tanto peligro de infección. Pero afortunadamente sólo se creen esta tesis casi el 13 de los encuestados.

Tesis n.° 11: Los cibercriminales no se interesan por los ordenadores de los usuarios particulares (8 por ciento).



Por suerte, a esta suposición es, de todas, a la que menos crédito se le concede, porque apenas un 8 por ciento la considera correcta. También en este caso se trata de una falsa hipótesis. Por supuesto, las redes corporativas son un objetivo muy interesante para los piratas de la red. Pero también, en general, son más difíciles de hackear. Los ordenadores privados tienen hoy en día unas altas prestaciones que les hacen muy tentadores como parte de las redes zombis. Además, con frecuencia atesoran muchos datos personales interesantes, como cuentas a tiendas online, perfiles en redes sociales y cuentas de correo eléctrico o incluso información de tarjetas de crédito, datos de los que los criminales pueden sacar mucho partido. Por todo ello, no debe subestimarse la importancia que los PC en manos de usuarios particulares tienen para los ciberdelincuentes.

3.2.2 ¿Quién está mejor informado: los internautas más jóvenes o los más mayores?

Los internautas más jóvenes, con edades comprendidas entre los 18 y los 25 años, han crecido en su inmensa mayoría con el ordenador e Internet y, además, son uno de los grupos más activos de Internet. Muy distinta es la situación que encontramos entre los encuestados más mayores, con edades entre los 55 y 64 años. Este estudio se realizó exclusivamente en línea, lo que significa que todos los encuestados se mueven en Internet. Pero para los participantes más mayores este medio es relativamente nuevo. Por eso, no sería descabellado pensar que la generación más joven conoce mucho mejor los peligros de Internet que la generación más madura. Otra posible hipótesis postula sin embargo que la generación de más edad ve peligros por todas partes y es más precavida, justo por su relativa falta de familiaridad con Internet y la informática.

Para averiguar el grado de información que posee la generación más joven y la de más edad, hemos investigado la credibilidad que estos dos grupos les dan a las tesis expuestas. La tabla siguiente proporciona una sinopsis de los resultados.

Tabla 10: ¿Quién se cree más las tesis expuestas antes: los usuarios más jóvenes o los más maduros?

Tesis / Mitos de la seguridad en Internet	Hombres	Mujeres	Total
1) Habrá evidencias si mi ordenador está infectado	91,50%	93,60%	92,59%
2) Los AV gratuitos ofrecen los mismos elementos de seguridad que los de pago	84,01%	81,73%	82,92%
3) La mayoría del malware se distribuye a través del correo electrónico	54,53%	54,31%	54,42%
4) Basta acceder a una web infectada para infectar tu PC	48,19%	48,46%	48,33%
5) La mayor parte del malware se distribuye a través de las descargas P2P y de torrents	49,13%	47,47%	48,27%
6) Es más probable encontrar malware en una web de contenido pornográfico que en otra relacionado con, por ejemplo, equitacion, deportes o viajes	43,88%	31,07%	37,23%
7) El firewall puede proteger el PC de los ataques drive-by-download (descarga silenciosa de malware)	26,02%	25,32%	25,66%
8) Si no abres el archivo malicioso, no puedes infectar el PC	22,65%	21,16%	21,88%
9) La mayoría del malware se distribuye a través de memorias USB	13,47%	12,24%	12,83%
10) No visito websites 'raras' o peligrosas, así que estoy a salvo de ataques drive-by-downloads	11,74%	13,51%	12,66%
11) Los cibercriminales no están interesados en los ordenadores de usuarios particulares	8,75%	6,35%	7,50%

Si en la tabla observamos la columna de los usuarios de menos edad, el resultado es, en principio, positivo. Los jóvenes se creen en menor medida las tres tesis principales, pero apenas se diferencian de la media de los encuestados. No así la cuarta tesis, que refleja un error muy peligroso, porque pone en duda la existencia y la eficiencia de las infecciones *drive-by download* (descarga silenciosa). Estas tesis se la creen los jóvenes con más asiduidad que los demás encuestados. Esto ocurre también en la quinta tesis, que versa sobre el malware en las plataformas de intercambio, como las páginas torrent y las redes P2P. La razón del fenómeno puede que sea que la generación más joven se descarga muchos archivos de estos sitios web y ya debe haberse topado con archivos infectados.

Los consultados más jóvenes sospechan también, en mayor medida que los mayores, que las páginas de pornografía son más peligrosas. Y la generación más joven está al parecer aún peor informada sobre las funciones de un cortafuegos. Todo esto no encaja con la hipótesis de que este tipo de usuarios conocen mejor las tecnologías con las que se han hecho mayores, más aun si tenemos en cuenta que los jóvenes tampoco se figuran que para una infección no es imprescindible abrir un archivo. Además, los participantes de menos edad creen más que la media que las memorias USB son la fuente principal de infecciones de malware. Los encuestados de menos años sobrevaloran sus conocimientos más que otros grupos de edad cuando se trata de impedir descargas silenciosas (*drive-by download*). Además, hay muchos más jóvenes que la media de encuestados que opinan que su ordenador particular no es interesante para los ciberdelincuentes.

Visto globalmente, los encuestados con menor edad no salen tan bien parados. Su nivel de conocimientos es aún más bajo que el del internauta medio y no es sostenible la hipótesis de que conocen mejor Internet que el grueso de la población porque han crecido con esta tecnología.

Si trasladamos nuestra atención a la columna de los encuestados de más edad, queda patente que esta horquilla concede más credibilidad a las tres tesis principales que el promedio de todos los encuestados. En la cuarta tesis, en que se tratan los ataques de descarga por *drive-by download*, el panorama cambia totalmente. Los consultados más mayores están obviamente mejor informados sobre estos peligros que los entrevistados de menos edad, pero sobre todo superan a los usuarios muy jóvenes. Pero esta ventaja comparativa no es motivo de alivio, porque también entre los más mayores, casi uno de cada dos cree que no hay descargas silenciosas *drive-by download*.

Muchos encuestados de la franja *senior*, más que el promedio, opinan que las páginas de compartir archivos son el foco principal de infecciones de malware. Pero esta diferencia con respecto al promedio es reducida. También las páginas de pornografía despiertan menos desconfianza en los más maduros que en la media de encuestados. Los mayores desconfían más de la capacidad de protección de los cortafuegos contra las descargas silenciosas que los entrevistados más jóvenes y que la media de todos los participantes. En contraposición, los consultados más mayores suelen creer que no es posible infectarse si no se abre un archivo. Las memorias USB constituyen, a ojos de los encuestados mayores, mucho menos el foco principal de la propagación del malware, una creencia acertada. También es cierto que las personas de más edad son aquí algo más prudentes que los más jóvenes. Merece mención positiva que los internautas mayores reconocen mejor que la media que sus ordenadores pueden estar en el punto de mira de los ciberdelincuentes.

Si evaluamos todos los datos, tampoco las personas mayores obtienen un buen resultado, aunque queda patente que se manejan con los peligros de Internet algo mejor que los encuestados más jóvenes. Este análisis nos permite sacar como conclusión que el grupo de edad entre 25 y 54 años es el que demuestra un mejor nivel de conocimientos sobre los peligros de Internet. Pero, en honor a la verdad, hay que mencionar que también en este grupo de edad circulan muchas falsas creencias sobre este tema y que estos encuestados no cuentan todavía con un saber suficiente.

3.2.3 ¿En qué país están los internautas mejor informados sobre los peligros de Internet?

Existen muchos prejuicios sobre en qué país están mejor (o peor) informados los usuarios. Así, mucha gente se pensará, por ejemplo, que los estadounidenses y los británicos están bien informados sobre los peligros que entraña Internet y que, por ejemplo, los rusos, saben menos del tema. Para determinar si realmente hay países en que los internautas están mucho mejor o peor informados sobre los peligros reales de la red, en la tabla 11 se han agrupado los resultados porcentuales de los encuestados que creen los mitos antes expuestos. El color verde muestra los países en que se concede menos credibilidad a la tesis. El rojo indica dónde la tesis tiene una mayor credibilidad.

Tabla 11: ¿En qué país se concede mayor (rojo) y menor (verde) credibilidad a estas tesis?

Mitos	Alemania	Austria	Bélgica	España	Estados Unidos	Francia	Holanda	Italia	Reino Unido	Rusia	Suiza	Mundo
1) Infección evidente	83,17%	86,46%	93,97%	95,30%	94,29%	92,28%	86,63%	94,38%	91,40%	97,88%	90,13%	92,59%
2) AV Gratuito	78,22%	76,56%	83,19%	83,48%	82,32%	90,53%	83,78%	85,06%	83,54%	83,78%	81,59%	82,92%
3) Malware vía e-mail	52,85%	55,47%	62,18%	58,61%	52,37%	57,64%	58,89%	58,88%	52,89%	38,80%	57,73%	54,42%
4) Website infectada	62,90%	60,68%	49,03%	57,83%	40,95%	49,25%	51,49%	63,44%	42,85%	48,48%	54,93%	48,33%
5) Torrent & P2P	35,26%	41,02%	46,76%	52,43%	52,73%	48,17%	43,53%	45,52%	48,73%	49,49%	44,48%	48,27%
6) Infección vía websites pornográficas	30,65%	34,11%	34,27%	32,43%	40,13%	31,89%	25,32%	32,25%	35,80%	60,18%	36,23%	37,23%
7) Firewall	29,31%	28,26%	28,34%	26,78%	24,32%	18,77%	31,44%	28,03%	24,95%	17,05%	29,16%	25,66%
8) Infección vía archivo malicioso	13,32%	14,06%	26,29%	30,78%	18,18%	23,59%	16,50%	30,67%	20,43%	38,53%	18,56%	21,88%
9) Infección mediante USB-stick	8,38%	8,72%	10,67%	20,09%	9,92%	17,28%	8,11%	15,38%	10,49%	30,05%	8,98%	12,83%
10) Websites peligrosas	11,81%	12,50%	13,69%	14,00%	10,79%	14,78%	18,07%	17,84%	9,67%	11,89%	14,14%	12,66%
11) PCs usuarios particulares	7,20%	9,90%	6,90%	8,87%	7,50%	5,98%	5,12%	8,35%	8,77%	6,54%	6,63%	7,50%

Esta tabla muestra que los entrevistados de Alemania son los que mejor informados están, por lo que parece, de los peligros que acechan en Internet. De todos los países, fueron los que menos credibilidad otorgaron a las tres tesis. Lo mismo se puede decir de los holandeses. Pero aquí hay que matizar que los holandeses en dos ocasiones son los que más se alejan de la verdad al estimar la verosimilitud de las afirmaciones. Curiosamente, uno pensaría quizá que los estadounidenses iban a ser los más eruditos en el tema, pero son los que más verosimilitud otorgan a la tesis que afirma que las plataformas de intercambio son "el lugar de Internet" donde más código dañino se propaga. En cualquier caso, no son los norteamericanos los peor informados sobre los peligros de Internet. El último de la fila es Rusia. De todas las nacionalidades, los rusos son los que más sostienen la veracidad de las falsas hipótesis. Por otro lado, son los que menos verosimilitud conceden a otros dos mitos, pero aún así no se salvan de este último lugar en el ranking.

3.2.4 ¿ Son los hombres mejores internautas?

Mucha gente tiene inconscientemente el convencimiento de que las mujeres tienen una menor destreza técnica que los hombres. Si esto fuera verdad, los hombres deberían también estar mejor informados que las mujeres sobre dónde acecha realmente peligro en Internet y qué temores se han quedado obsoletos o no se corresponden con la realidad. ¿Es cierta esta inferencia? El cuadro siguiente nos enseña cómo se sitúan realmente los hombres y las mujeres en el campo de las leyendas de Internet.

Tabla 12: ¿Quién se cree más las afirmaciones: los hombres o las mujeres?

Tesis / Mitos de la seguridad en Internet	Hombres	Mujeres	Total
1) Habrá evidencias si mi ordenador está infectado	91,50%	93,60%	92,59%
2) Los AV gratuitos ofrecen los mismos elementos de seguridad que los de pago	84,01%	81,73%	82,92%
3) La mayoría del malware se distribuye a través del correo electrónico	54,53%	54,31%	54,42%
4) Basta acceder a una web infectada para infectar tu PC	48,19%	48,46%	48,33%
5) La mayor parte del malware se distribuye a través de las descargas P2P y de torrents	49,13%	47,47%	48,27%
6) Es más probable encontrar malware en una web de contenido pornográfico que en otra relacionado con, por ejemplo, equitacion, deportes o viajes	43,88%	31,07%	37,23%
7) El firewall puede proteger el PC de los ataques drive-by-download (descarga silenciosa de malware)	26,02%	25,32%	25,66%
8) Si no abres el archivo malicioso, no puedes infectar el PC	22,65%	21,16%	21,88%
9) La mayoría del malware se distribuye a través de memorias USB	13,47%	12,24%	12,83%
10) No visito websites *'raras'* o peligrosas, así que estoy a salvo de ataques drive-by-downloads	11,74%	13,51%	12,66%
11) Los cibercriminales no están interesados en los ordenadores de usuarios particulares	8,75%	6,35%	7,50%

La tabla muestra que las mujeres se acercan a la verdad con notable mayor frecuencia que los hombres. Solo en tres de los falsos enunciados las mujeres se equivocan más a menudo que los hombres. Pero es dudoso que estos resultados por sí solos permitan inferir que las mujeres son mejores internautas. En la mayoría de los casos, hay menos de 2 puntos porcentuales de diferencia entre los sexos.

La diferencia más patente entre los hombres y las mujeres se muestra en la tesis "En las páginas web de pornografía hay mayor peligro de toparse con malware que, por ejemplo, al entrar en sitios web sobre equitación o viajes". El hecho de que haya muchos más encuestados del sexo masculino que corroboren esta afirmación errónea puede deberse a la misma razón que se aplicaba a las respuestas de los más jóvenes, que también se creían en mayor medida la tesis: "La mayor parte de los virus y software dañino se propaga por archivos en las plataformas de intercambio como las redes P2P y los sitios con torrent". Ciertamente, cuando un grupo tiene más experiencia y horas de navegación en determinados sitios web es, por estadística, más probablemente haya tenido con más frecuencia un mal encuentro con software dañino en estas páginas. Pero esto no constituye ninguna prueba de que la afirmación sea cierta. Porque, ¿acaso los hombres encuestados han visitado con la misma frecuencia páginas web sobre, por ejemplo, el deporte de la hípica? Y aunque este fuera el caso y no

hubieran sufrido ningún ataque de software dañino en estas páginas: ¿No podría ser una casualidad que en ninguna de ellas les haya ocurrido una infección de tipo *drive-by-download*?

Desde el punto de vista femenino, una página web porno posiblemente es tan peligrosa o inofensiva como cualquier otro sitio de la Red. Otra explicación más para la distinta valoración puede buscarse en una interpretación psicológica. La mayor parte de la gente tiene la pornografía por algo malo y reprobable, es decir, algo que hay que ver a escondidas. Cuando las personas se figuran estar haciendo algo prohibido, se esperan de alguna manera que les sobrevenga un castigo por su conducta. En esta caso, una infección con malware. Es un hecho estadístico comprobado que hay más hombres que mujeres que consumen porno y que por eso suponen más que van a encontrarse con código dañino en estos sitios pornográficos.

Hay otra afirmación, además de esta pregunta sobre las páginas pornográficas, en que las apreciaciones de los hombres y las mujeres se diferencian en grado considerable: Los hombres se figuran con más frecuencia que a los cibercriminales no les interesa su ordenador personal. Las mujeres se sienten en este punto menos seguras. Posiblemente se debe al hecho de que las mujeres, en general, usan su PC con más prudencia, quizá en el sentido de que tienen menos seguridad en sí mismas, y además porque los hombres son más amantes del riesgo.

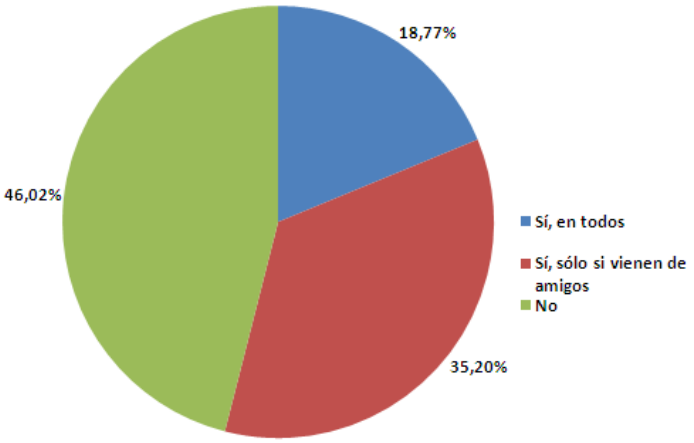
3.3 Conducta en las redes sociales

Las redes sociales son cada vez más populares y se han consolidado con una presencia estable del paisaje de Internet. En Facebook, Twitter y compañía, los usuarios se presentan y mantienen una red de amistades, con frecuencia muy amplia e internacional. La gran popularidad de las redes sociales las hace muy tentadores para los delincuentes, que abusan de los portales sociales para sus engaños y artimañas.

Los malhechores tienen aquí varias posibilidades de aprovecharse de los usuarios: En general, las cuentas con que los usuarios acceden a la Red se puede sustraer mediante métodos "clásicos" de phishing con páginas falsificadas que parecen auténticas, o asaltando la base de datos de acceso del proveedor. Un engaño muy usado por los ciberpiratas en las plataformas sociales es la difusión de direcciones a páginas maliciosas mediante una entrada en el muro o por un mensaje de chat o personal. El cebo puede ser, por ejemplo, un enlace a un vídeo.

Las páginas gancho suelen haber sido abreviadas mediante un acortador de URL de tal modo que el usuario no tiene ningún punto de referencia sobre el riesgo. Al pulsar estos enlaces se llega a una página web externa infectada de código dañino que roba datos mediante phishing, o bien mediante clickjacking, y que convierte a la víctima en un foco difusor de spam en las redes sociales. Este “secuestro de clics” hace que el usuario propague sin querer el enlace entre su círculo de amigos en la Red. Hay que tener cuidado no solo con los enlaces enviados por desconocidos. También las amistades pueden transmitir estas direcciones de Internet, como sucede cuando un hacker piratea y usa la cuenta pirateada en nombre de la víctima. En vista del alto potencial de peligro, el ‘*Estudio de Seguridad 2011*’ de G Data incluía una pregunta en torno a la atención prestada a los enlaces en las redes sociales.

Diagrama 9: La mecánica de los flujos de clics en enlaces situados en redes sociales

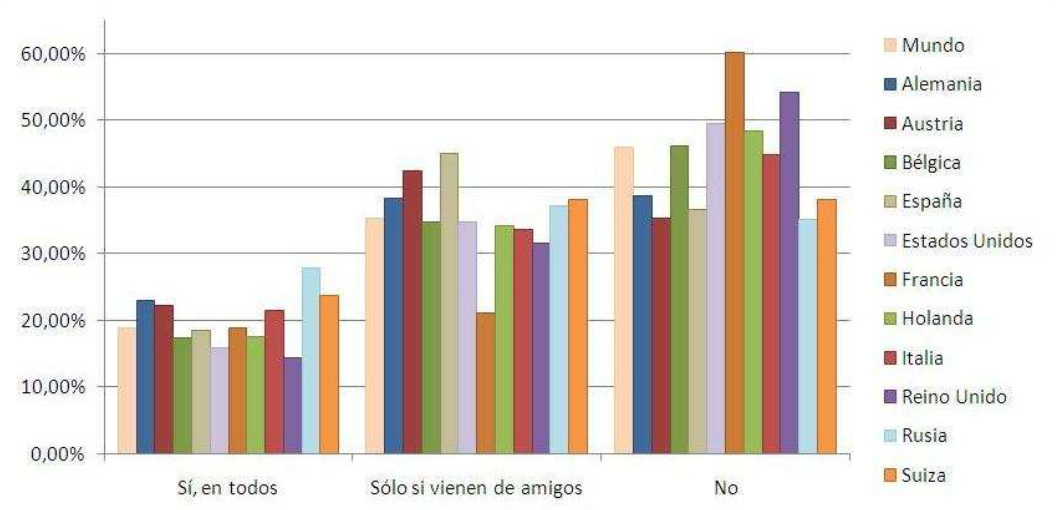


La mayoría de los participantes en el estudio usaba, en general, los enlaces que encontraba en las redes sociales. Un 46 por ciento de los encuestados no hacía clic en ninguna URL, independientemente de su origen (amigos o desconocidos). Más de un tercio confía en las direcciones de Internet publicadas por amigos de su propia red. Y un 19 por ciento largo pinchaba en los enlaces, viniesen de quien viniesen, convirtiéndose en un blanco fácil de los ciberdelincuentes y de sus oscuros tejemanejes.

En la comparativa de países destaca especialmente Francia:

El 60 por ciento de los franceses no hace clic en los enlaces de las redes sociales, el valor más elevado si lo comparamos con el resto de países, y el 18 por ciento participa de todos los enlaces posibles (coincide exactamente con la media de la comparativa de países). Además, solo el 21 por ciento de los encuestados pulsa los enlaces publicados por integrantes de su círculo de amistades en la plataforma social. Este porcentaje es el más bajo si lo ponemos en relación a los otros países y a la media general. Los franceses resultan ser los más concienciados sobre los peligros de los vínculos a las páginas web en las redes sociales.

Diagrama 10: Mecánica de los flujos de clics en los enlaces situados en las redes sociales, por países



Los participantes rusos en el sondeo son los que menos mentalizados están de los riegos de estos vínculos y más de una cuarta parte reconocen que pulsan las URL de todos los usuarios, conocidos y desconocidos, de la red social. Solo el 35 por ciento no hace clic en ninguna URL de Internet. El 37 por ciento de los rusos entrevistados seleccionan solo direcciones web de sus amistades.

Tabla 13: Mecánica de los flujos de clics en las redes sociales, desglose por países

¿Pinchas en los enlaces que te llegan en las redes sociales?			
	Sí, en todos	**Sólo si vienen de amigos**	**No**
Mundo	18,77%	35,20%	46,02%
Alemania	22,95%	38,36%	38,69%
Austria	22,27%	42,45%	35,29%
Bélgica	17,34%	34,80%	46,17%
España	18,43%	45,04%	36,52%
Estados Unidos	15,79%	34,80%	49,41%
Francia	18,77%	21,01%	60,22%
Holanda	17,50%	34,14%	48,36%
Italia	21,44%	33,66%	44,90%
Reino Unido	14,29%	31,46%	54,25%
Rusia	27,74%	37,14%	35,12%
Suiza	23,71%	38,14%	38,14%

3.3.1 ¿Quién hace un uso más seguro de las redes sociales: los hombres o las mujeres?

En el '*Estudio de Seguridad 2011'* de G Data se pone de manifiesto realmente una diferencia entre las mujeres y los hombres atendiendo al uso de los enlaces en las redes sociales. Pero, en contra de lo esperado, el resultado no nos dice que las mujeres procedan siempre con mayor prudencia en estas comunidades sociales.

La diferencia es más bien reducida: El 47 por ciento de las mujeres elude los hipervínculos en las plataformas sociales. Los hombres, con un 45 por ciento escaso, quedan algo por debajo. En contra-partida, hay más hombres que seleccionan links aunque no provengan necesariamente de su red de amistades. Las mujeres que dicen pulsar en los enlaces procedentes de su círculo de amistades (36,73%) constituyen más del doble que las que indican que lo hacen en todo tipo de enlaces (16,29%). Entre los hombres, un tercio de los consultados prefieren pulsar direcciones de los amigos antes que las de los demás usuarios.

Tabla 14: Resultados detallados de la pregunta incluyendo internautas de todos los países

¿Pinchas en los enlaces que te llegan en las redes sociales?			
	Sí, en todos	**Sí, sólo si vienen de amigos**	**No**
Hombres (18-24)	26,24%	38,02%	35,74%
Hombres (25-34)	25,92%	38,63%	35,45%
Hombres (35-44)	21,09%	33,56%	45,35%
Hombres (45-54)	18,23%	31,10%	50,66%
Hombres (55-64)	15,93%	26,21%	57,86%
Total Hombres	**21,46%**	**33,55%**	**44,99%**
Mujeres (18-24)	21,54%	45,38%	33,08%
Mujeres (25-34)	20,43%	40,92%	38,64%
Mujeres (35-44)	15,41%	35,59%	48,99%
Mujeres (45-54)	13,72%	31,27%	55,01%
Mujeres (55-64)	9,83%	30,48%	59,69%
Total Mujeres	**16,29%**	**36,73%**	**46,99%**
Total	**18,77%**	**35,20%**	**46,02%**

Los resultados desglosados por países arrojan un panorama similar, exceptuando Italia, Bélgica y Austria: Las mujeres presentan siempre, también en estos países, una aproximación más precavida a las redes sociales y evitan pulsar las URL en general o por lo menos cuando no conocen al remitente. En comparación con los hombres, actúan así con más frecuencia, aunque generalmente no hay una gran diferencia entre los sexos. Esta relación se invierte, como revela el Estudio de seguridad, en Italia, Bélgica y Austria: Aquí los hombres parecen ser ligeramente más sensibles a los peligros derivados de los enlaces en las plataformas sociales. Pero la diferencia también aquí es mínima.

Queda patente, por lo tanto, que entre los hombres y las mujeres sí que hay diferencias, pero casi insignificantes. Como conclusión no se puede constatar claramente cual de los dos sexos es más precavido en el uso de las redes sociales.

3.3.2 ¿Quién hace un uso más seguro de las redes sociales: los usuarios más jóvenes o los más maduros?

Ya se sabe que los internautas más jóvenes se mueven con mucha mayor frecuencia en las redes sociales y las usan con mayor intensidad que los más mayores. A pesar de esta experiencia, la generación de mayores es más prudente a la hora de usar las plataformas sociales, como muestra el resultado general del Estudio de Seguridad de G Data: Especialmente precavidos son lo mismo los hombres que las mujeres en las franjas de edades comprendidas entre 45 y 54 y entre 55 y 64 años (véase la tabla 14).

Más de la mitad de los entrevistados de estas edades se niega categóricamente a pulsar URL en las redes sociales. Las mujeres de esa generación, incluso, son todavía más críticas que sus coetáneos del sexo masculino. Los tres segmentos de edad por debajo de ellos (hasta 44 años) están predispuestos, como era de esperar, a hacer clic en páginas web publicadas por usuarios conocidos o desconocidos.

Conclusión: Los "abuelos internautas" se pone a la cabeza

La edad del encuestado (hombre o mujer) está en relación inversamente proporcional con la frecuencia con que selecciona en las redes sociales los vínculos a páginas externas. En esta correlación no juega ningún papel relevante si el origen de los enlaces está en personas conocidas o desconocidas. Entre los varones de 55 a 64 hay casi un 58 por ciento que se niega a pulsar cualquier tipo de enlace, pero este porcentaje desciende hasta el 36 por ciento si situamos la franja de edad entre los 18 y 24 años. Entre las mujeres esta diferencia se agranda: En la horquilla de más edad, el 60 por ciento dice no a pulsar estos links, porcentaje que contrasta con el tercio de las mujeres entre 18 y 24 años que sigue esta buena práctica. Siguiendo esta lógica, las entrevistadas, cuanto más jóvenes, más dispuestas están a seleccionar enlaces de conocidos y desconocidos. Lo mismo se aplica a los enlaces de conocidos del círculo de amistades de la red.

Esta prudencia que muestran los usuarios de más edad puede deberse a varios motivos. Es lógico pensar que la generación de mayores suele tener una mayor inseguridad al usar las redes sociales. Esta forma de Internet participativo y de comunicación no les resulta tan familiar y cercana como a la generación más joven. A algunas personas de más edad por eso puede que les falte simplemente la seguridad básica para usar los portales sociales.

Los más mayores (como ya hemos explicado antes) no usan las redes sociales con la intensidad con que lo hacen los jóvenes y tampoco se pasan tanto tiempo en ellas. Además también es posible que los contactos de las redes en este grupo de edad no publiquen ningún link externo o muy pocos y por eso los encuestados no les llega a afectar realmente esta temática. Otro aspecto a tener en cuenta es que los internautas más jóvenes consideran el propio Internet y también las redes sociales como una especie de herramienta: permiten mantener los contactos, crearlos nuevos, entretener el ocio y revelar aspectos personales.

4. Conclusiones

La investigación permite extraer una primera conclusión muy positiva: La mayor parte de los internautas, independientemente de su edad, sexo o nacionalidad, sabe que en Internet hay peligros. Pero desafortunadamente se trata de una vaga conciencia de peligro pues solo unos pocos son capaces luego de delimitar correctamente los riesgos actuales de la red de redes.

Muchos de los entrevistados saben también muy poco sobre cómo protegerse con eficacia de los programas dañinos. Otro aspecto digno de mención es que no son muchos los que conocen la forma de protegerse bien de los peligros ocultos.

Llama también la atención que en Internet circulan muchas suposiciones erróneas sobre los peligros de la propia Red. Casi todos se creen que saben todo lo que hay que saber sobre los virus y otros programas maliciosos, pero lo cierto es que tienen conocimientos totalmente obsoletos. Se tiene mucho miedo de peligros que, hoy por hoy, ocurren muy raramente, como por ejemplo del malware transmitido a través de correos en masa (el 54 por ciento cree que la mayor parte del software malicioso se propaga por esta vía), o la suposición de que el malware afecta de algún modo al funcionamiento del PC (el 92 por ciento lo cree así). Esto era cierto en los noventa y, a ocasiones, en la primera década del nuevo milenio, pero ya hace tiempo que ha dejado de ser así. La mayor parte de los programas dañinos están programados de tal madera que al usuario del PC le pasen desapercibidos. Una de las pocas excepciones son, por ejemplo, los falsos antivirus, o "rogueware".

El hecho de creer erróneamente que la mayor parte del malware se envía por correo electrónico no constituye en sí un gran problema y siempre es recomendable no dejar de lado la prudencia al gestionar los emails. Pinchar sobre los enlaces y abrir los adjuntos sigue siendo una conducta de riesgo, ahora como en el pasado y tampoco perjudica en absoluto estar siempre ojo avizor en este aspecto.

El otro ejemplo, el figurarse que los programas maliciosos dejan el ordenador fuera de combate, abre la puerta a problemas: Mientras que el usuario no nota nada extraño, alberga la infundada creencia de que todo va bien. Pero como ya ha sido expuesto aquí, el usuario no percibe las infecciones de hoy en día con código dañino. El malware puede así cumplir su objetivo sin estorbos y los hackers se salen con la suya.

Tampoco alegra especialmente constatar la ignorancia existente en torno a los peligros derivados de las páginas web. Casi la mitad de los encuestados no cree en la existencia de las descargas silenciosas por el método *drive by download*. El 48 por ciento de los entrevistados no se figuran que su ordenador pueda infectarse con solo visitar una web infectada. Esta vía de infección es actualmente el método más frecuente para los ciberpiratas de propagar su malware.

Los usuarios que han oído hablar o conocen las infecciones *drive-by download* tienen con frecuencia ideas preconcebidas sobre donde se localizan de forma más frecuente estas páginas contaminadas. Sobre todo los hombres (casi el 44 por ciento) suponen que las páginas pornográficas son más peligrosas que la media. Esto implica, sin embargo, que las páginas web infectadas no estarían salpicadas al azar por toda la red. Y esta presunción tampoco tiene en cuenta, además, que las páginas conocidas y de fiar podrían caer presas de hackers y ser infectadas con código dañino. Cada dos por tres los medios informan de que ha sido pirateada la página web de alguna conocida marcas de consumo.

Y esto son solo los casos que conocemos porque informan de ellos los medios de comunicación. Quién sabe cuántos ataques no salen a la luz. En pocas palabras: Las infecciones silenciosas '*drive-by-download*', como ya dice su nombre ("infecciones al pasar"), no son previsibles. Por eso, no es posible evitar mediante una actuación determinada que el PC pueda llegar a toparse con ellas.

El único modo efectivo de proteger los ordenadores de las descargas silenciosas es usar una solución de seguridad integral que incluya un filtro HTTP, que, antes de cargar las páginas web, las examine por si tienen malware. Las soluciones antivirus gratuitas no tienen esta tecnología de protección y por eso no protegen a sus dueños en grado suficiente. Estos usuarios, sin embargo, tienen con frecuencia la creencia de que la solución que usan les proporciona la protección amplia necesaria frente a los peligros de Internet, como pone de manifiesto el estudio. Este error podría resultar fatal, en el peor de los casos, y desembocar en una infección con algún peligroso programa dañino.

No menos del 62,58 por ciento de los usuarios de soluciones antivirus gratuitas mantienen la creencia de que estos productos protegen el PC de las descargas silenciosas. El 25,39 por ciento de los usuarios suponen (erróneamente) que el cortafuegos protege el PC contra ataques *drive-by-download*. Estos usuarios, por sus falsas creencias, no sentirán la necesidad de buscarse un filtro HTTP que les proteja de las páginas web contaminadas.

La protección frente a las páginas web infectadas también es una prioridad para los usuarios de las redes sociales. En estas plataformas se publican continuamente links a páginas web externas con contenidos graciosos o informativos, o con clips de vídeo. Las funciones como éstas confieren un atractivo adicional a las redes como Twitter y Facebook. Por eso, sería una pena dejar de lado siempre estos links por razones de seguridad, medida que, por cierto, adopta el 46 por ciento de los participantes en el sondeo. En este contexto hay que mencionar también que las URL acortadas suponen un aumento del riesgo, no solo en las plataformas sociales. Con servicios como el de http://longurl.org/ se puede averiguar la dirección original. Estos servicios, en combinación con un buen filtro HTTP, hacen un poco más seguro para el usuario seleccionar los links publicados en las redes sociales.

Es difícil extraer resultados concluyentes sobre quién está mejor informado sobre todos los peligros. Por lo que parece, los grupos de edad comprendidos entre 25 y 54 años son los que mejor mentalizados están sobre las amenazas de Internet, pero también muestran temor en situaciones que prácticamente no suponen peligro. Con todo, no está claro si se les puede considerar como los usuarios de Internet más prudentes.

La diferencia entre los hombres y las mujeres resulta muy reducida, aunque, si atendemos al resultado general del '*Estudio de Seguridad 2011'* de G Data, las mujeres parecen estar un poquito mejor informadas. Pero esta base no permite extraer como conclusión general que uno de los sexos tenga más conocimientos sobre los peligros potenciales en Internet.

Tampoco al considerar la nacionalidad de los encuestados se pueden identificar un ganador claro. En Alemania, Gran Bretaña e Irlanda del Norte los usuarios parecen algo mejor informados sobre las amenazas reales de Internet y las que no son tales, aunque también aquí son mínimas las diferencias con respecto a la media general. Un resultado desde luego es claro y patente: En Rusia existe la mayor falta de conocimiento sobre los peligros de la Red.

Por suerte, en Rusia, en comparación con todos los demás países, los internautas son los que más tienen suites de seguridad de pago. Pero hay que apuntar aquí, sin embargo, que en Rusia es también donde más se usan copias piratas de las suites de seguridad de pago, que, lógicamente, son menos estables y fiables que las versiones legales.

Como síntesis final del *Estudio de Seguridad 2011* de G Data se puede constatar que, a pesar del uso tan extendido de Internet, la mayor parte de los usuarios conocen mal los peligros y por eso no saben suficiente sobre las estrategias necesarias para impedir que el ordenador se infecte con código dañino.

Apéndice

G Data Software AG

G DATA Software AG, con sede en Bochum, Alemania, es una empresa de software innovadora y en proceso de rápida expansión enfocada a las soluciones de seguridad informática. Como especialista en seguridad en Internet y pionera en el sector de la protección antivirus, esta empresa fundada en 1985 en Bochum, desarrolló el primer programa antivirus hace ya más de 20 años.

G Data es, con este palmarés, una de las empresas de software de seguridad más antiguas del mundo. Desde hace más de cinco años G DATA ha ganado más distinciones y ha salido triunfadora de más certámenes y comparativas nacionales e internacionales que ningún otro fabricante europeo de software de seguridad.

La gama de productos comprende soluciones de seguridad para usuarios finales, pymes y grandes empresas. Las soluciones de seguridad G Data se comercializan en más de 90 países.

Encontrará más información sobre la empresa y sobre las soluciones de seguridad G Data en www.gdata.es

Hitos en la historia de G Data

1986
CeBIT comienza su andadura de éxito y G Data presenta en la primera edición de la feria el primer concepto de un antivirus para ordenadores ATARI.

1987
G Data desarrolla numerosos programas innovadores para ATARI ST, entre otros el primer programa antivirus del mundo: G Data AntiVirusKit.

1990
Los ordenadores personales se extienden como la pólvora. G Data comienza a desarrollar software para MS-Dos. El primer proyecto es adaptar el AntiVirusKit a los PC. Por aquel entonces lo nunca visto: la interfaz de usuario gráfica propia.

1991
G Data sigue creciendo y ofrece una amplia gama de diferentes programas de software para ATARI ST.

1992
Además de los antivirus, G Data desarrolla numerosas aplicaciones para MS-DOS y Windows. Especialmente innovador: El planificador de rutas GeoRoute, el primero con mapa interactivo para PC.

1995
Apertura de la primera filial extranjera en Polonia.

1998
PowerRoute, con un millón de unidades vendidas, se convierte en el planificador de rutas para PC de mayor éxito en Alemania.

2000
Transformación a una sociedad anónima: Los empleados de G Data obtienen participación en la empresa. Hasta hoy, la cuotas sociales mayoritarias están en manos de los empleados y de los fundadores de la compañía.

2001
Entrada en el sector de redes y corporativo con G Data AntiVirus Business y AntiVirus Enterprise.

2002
G Data desarrolla la tecnología DoubleScan y es el primer fabricante que consigue usar en su producto paralelamente dos motores antivirus.

2003
La empresa se internacionaliza y entra en el mercado japonés.

2004
G Data presenta en la CeBIT la primera generación de su paquete de seguridad integral G Data InternetSecurity.

2005
Un adelantado a su tiempo: G Data es una de las primeras empresas del mundo en integrar en su programa de protección tecnología de seguridad en la nube. OutbreakShield protege en tiempo real del spam y los programas dañinos desconocidos.
La organización de consumidores Stiftung Warentest elige a G Data InternetSecurity como el mejor paquete de seguridad.
La empresa se internacionaliza: Apertura de oficinas en Francia e Italia.

2006
Aumenta el número de programas dañinos y G Data pone la solución: Los clientes de G Data están protegidos rápidamente del nuevo malware con las actualizaciones de firma cada hora.

2007
Stiftung Warentest: Por segunda vez consecutiva, G Data InternetSecurity 2010 gana el primer puesto en el gran test comparativo de esta prestigiosa revista alemana de los consumidores.
Presentación en la CeBit 2007: G Data TotalCare.

Apertura de oficina en España

2008
Lanzamiento de una nueva solución especial de seguridad para los propietarios de ordenadores portátiles: G Data NotebookSecurity es una potente solución integral que reúne antivirus, backup y tecnología de codificación.

2009
Las soluciones de seguridad G Data están disponibles en más de 60 países. G Data prosigue su exitosa estrategia de expansión en Sudamérica, Rusia, Sudáfrica y China.

2010
G Data celebra su 25 aniversario
Presentación en la CeBIT: G Data EndpointProtection

2011

Presentación en la CeBIT de G Data CloudSecurity, un plugin gratuito para el navegador que hace más seguro el uso de Internet.

Protección inteligente para smartphones con Android y tabletas: G Data MobileSecurity.

Survey Sampling International

SSI fue el primero en el año 1977 en realizar sondeos comerciales en los EE.UU. Desde hace décadas establecemos el estándar de referencia en nuestra especialidad y en la calidad de los muestreos y del servicio al cliente en el área de la investigación de mercados.

SSI ofrece el acceso a más de 6 millones de participantes en sondeos en 54 países. Entre nuestras fuentes tenemos comunidades de grupos de consulta en 27 países, un número creciente de filiales bajo nuestra dirección y una amplia red mundial de empresas asociadas. SSI trabaja con una plantilla interna de 400 empleados en 50 países, que hablan 36 idiomas, para más de 1800 clientes de la investigación de mercados que suponen tres cuartas partes de las principales empresas de este sector.

La empresa tiene 17 sedes repartidas por el globo: en Pekín, Frankfurt, Londres, Los Ángeles, Madrid, México D.F., París, Rotterdam, Seúl, Shanghai, Shelton (CT), Singapur, Estocolmo, Sydney, Timisoara (Rumanía) Tokio y Toronto. Además cuentan con representantes de SSI en Hong Kong.

Encontrará más información sobre Survey Sampling International en www.surveysampling.com

Glosario

Bot: Los bots son pequeños programas que se ejecutan en segundo plano en el ordenador de la víctima, casi siempre sin que ésta note nada. Allí realizan diversas tareas, en función del rango de funciones que tenga el bot: desde ataques DDoS o enviar correos basura, hasta registrar las entradas de teclado del usuario, entre otras muchas posibilidades. La gama de funciones depende sobre todo de la cantidad de dinero que se desee invertir en el ordenador capturado. Los bots con un amplio margen de funcionalidades son, como es de suponer, más caros que los bots más sencillos que pueden hacer pocas cosas. Se venden, entre otros lugares, en los foros clandestinos.

Botnets: Una red de bots es un conjunto de "ordenadores zombis". Para administrar la red de bots se utilizan los servidores de "Command and Control" (servidores C&C). Las redes de bots se utilizan, entre otras cosas, para ejecutar ataques selectivos de sobrecarga contra servidores web (ataques DoS y DDoS) y para enviar spam.

Clickjacking: O “secuestro de clics”. Técnica mediante la que se consigue que el internauta haga clic en determinados enlaces sin ser consciente de ellos (mediante por ejemplo botones ocultos en una web infectada y aparentemente inofensiva) y que permite revelar información confidencial o tomar el control de sus ordenadores.

DoS (Denial of Service): En el caso de los "Denial of Service Attacks" (ataques de denegación de servicio), uno o varios ordenadores (suele tratarse de servidores web) sufren un "bombardeo" de muchas consultas o muy específicas que desbordan el sistema. De este modo se impide la ejecución de los servicios del servidor y el sistema se colapsa.

DDoS (Distributed Denial of Service): Un ataque distribuido de denegación de servicio se basa en el mismo principio que un ataque DoS normal. La única diferencia radica en que en el que nos ocupa se trata de un ataque repartido. Con frecuencia, estos ataques los llevan a cabo miles y miles de ordenadores zombi.

Infección drive-by-download (descarga silenciosa): Estas amenazas consiguen que baste visitar una página web adulterada para que se descargue y ejecute código dañino en el PC sin que lo note el usuario. Para estos ataques, los delincuentes aprovechan los agujeros de seguridad en el navegador y sus plugins. Los atacantes se fijan especialmente en las vulnerabilidades de las funciones para ejecutar contenidos activos (como por ej. JavaScript, Flash o Java).

Exploit: Se trata de un programa que aprovecha un fallo de seguridad existente en el ordenador objetivo para ejecutar un determinado código de programa.

Phishing: Se entiende por "phishing" el intento de obtener datos personales, como los nombres de registro, contraseñas, números de tarjeta de crédito, datos de accesos a cuentas bancarias, etc., mediante páginas web falsificadas o mediante e-mails indeseados. La mayoría de intentos de phishing se dirigen a clientes de bancos ofreciendo ofertas de banca online (CityBank, Postbank), servicios de pago (Paypal), proveedores de servicios de Internet (AOL) o tiendas online (eBay, Amazon). Con este fin la víctima es conducida por correo electrónico o mensajería instantánea a las páginas web falsificadas que imitan con gran exactitud a las páginas auténticas que les sirven de modelo.

Ingeniería social: Ingeniería social es el nombre que se da a las tácticas de convicción con las que un hacker induce a un usuario a revelar una información que luego podrá utilizar para dañar al propio usuario o a su organización. A menudo se simula ser una autoridad para conseguir los datos de acceso o contraseñas.

Spam: A mediados de los años 90 se llamaba spam a la difusión desmesurada de mensajes iguales en foros Usenet. El término surgió de un sketch de Monty Python. En la actualidad, la palabra spam tiene varios significados. De forma genérica, se consideran spam todos los correos electrónicos recibidos sin haberlos solicitado. En un sentido más estricto, este concepto se reserva a los correos publicitarios, es decir, los gusanos, hoaxes, correos de phishing y de autorespuesta no se consideran spam.

PC zombi: Zombi es un ordenador controlado a distancia desde un programa "backdoor" o puerta trasera. Como ocurre en las películas del género, los ordenadores zombis solo obedecen y ejecutan las órdenes, con frecuencia criminales, de un cabecilla oculto. Muchos zombis se agrupan en las llamadas redes de bots o "botnets".