

# Música y películas: el entretenimiento frente al riesgo en Internet

Evitar los riesgos asociados con la música,  
los vídeos y las películas en Internet





## Introducción

Los consumidores de hoy en día, ávidos de entretenimiento, optan cada vez más por los medios online tales como películas, música, TV, radio y vídeos digitales. De hecho, más de 178 millones de internautas de EEUU visualizaron vídeos online en julio de 2010 frente a los 158 millones de hace un año.<sup>1</sup> Mientras que los adultos ven vídeos en streaming para estar al día de las noticias mundiales, los adolescentes buscan los pósters de su película favorita o el tono de llamada del último éxito de Lady Gaga. Los contenidos audiovisuales online nos lo ofrecen todo de manera rápida y fácil, pero a un precio. El acceso al entretenimiento online sin tomar las precauciones necesarias puede exponer potencialmente a los consumidores y a sus equipos e identidades a numerosas amenazas.

Aunque es cierto que existen riesgos online, todavía puede disfrutar de Internet, entretenerse y obtener información. Protéjase sabiendo qué buscar y cómo protegerse a si mismo y a su equipo.

Los contenidos audiovisuales sociales han cambiado la manera en la que accedemos al entretenimiento y a la información. Los ciberdelincuentes se aprovechan de nuestra fascinación y nuestra necesidad inmediata por las noticias de última hora y los temas de actualidad para conseguir que hagamos clic en correos electrónicos no deseados o que nos descargemos vídeos "que no nos podemos perder" para distribuir su software malicioso, malware y otras amenazas. Los sitios web con contenidos audiovisuales sociales como YouTube, que tuvo 143,2 millones de espectadores en julio de 2010<sup>2</sup> son muy atractivos para los ciberdelincuentes que desean atacar a audiencias en masa que no se lo esperan.

A continuación ofrecemos un resumen de algunos hallazgos importantes aportados por nuestro equipo de investigación de los laboratorios McAfee Labs™ sobre el entretenimiento en Internet:

- **Los "Fans" atraen páginas peligrosas:** McAfee ha descubierto miles de URLs maliciosas y sospechosas asociadas con clubes de fans o comentarios realizados en páginas de fans, incluso cuando los comentarios se han realizado vía redes sociales como Facebook, MySpace, YouTube y Twitter.
  - **Los anuncios maliciosos aumentan de manera exponencial:** La publicidad maliciosa (publicidad online que se utiliza para distribuir software malicioso o redirigir el navegador del usuario sin su conocimiento) es un medio común de infección, incluso en sitios bien establecidos. Por ejemplo, el 1 de junio de 2010, McAfee identificó "publicidad maliciosa" en perezhilton.com que redirigía usuarios a un dominio que distribuía cargas maliciosas.
  - **Los sitios de contenido ilegal a menudo engañan a los consumidores:** Los sitios creados para distribuir contenido ilegal son difíciles de detectar por parte de los consumidores y a menudo distribuyen software malicioso y exponen a los usuarios a otros riesgos. Estos sitios web son tan sofisticados que mediante el rastreo de la propiedad de los dominios de los sitios web y las relaciones y herramientas utilizadas para desarrollarlos, se suele averiguar que éstos pertenecen a asociaciones delictivas. Esto no es algo que la mayoría de consumidores puedan o vayan a hacer.
- **Lo "gratis" puede salir caro:** Añadir la palabra "gratis" a una búsqueda de tonos de llamada conlleva un riesgo tres veces mayor en los sitios web encontrados por los buscadores más importantes en inglés. El uso de la palabra "gratis" en otros idiomas conlleva resultados similares en otros buscadores.
  - **Los "MP3s" aumentan el riesgo:** Buscar "MP3" aumenta el riesgo de las búsquedas de música, mientras que buscar "MP3 gratis" hace que la búsqueda se torne todavía más peligrosa. Incluso cuando un consumidor indica en su búsqueda que desea pagar por el MP3, los resultados le enviarán a contenido pirata.

<sup>1</sup> ComScore, Inc. Julio 2010 U.S. Online Video Rankings - [http://www.comscore.com/Press\\_Events/Press\\_Releases/2010/8/comScore\\_Releases\\_July\\_2010\\_U.S.\\_Online\\_Video\\_Rankings](http://www.comscore.com/Press_Events/Press_Releases/2010/8/comScore_Releases_July_2010_U.S._Online_Video_Rankings)

<sup>2</sup> Ibid

## Riesgos de las películas digitales

Al centrarnos en películas, nuestra investigación reveló que estos tipos de amenazas giraban alrededor del tráfico de la web y las tendencias del momento. Tanto si se trata de salvapantallas o de la película más demandada, los ciberdelincuentes están presentes en los sitios web que despiertan más interés por parte de los consumidores.

### Distribución de contenidos audiovisuales sin interrupción o streaming: radio, TV e imágenes de video en tiempo real

Los consumidores visitan videos porque son un método rápido y cómodo de visualizar contenido actualizado. Los sucesos mundiales, como el terremoto en Haití, o acontecimientos deportivos como el Mundial de la FIFA o temas de actualidad, tienden a generar mucho tráfico en los sitios web de videos.

El inconveniente es que la creciente demanda de contenido audiovisual sin interrupción o streaming es muy tentadora para los ciberdelincuentes que buscan una gran audiencia a la que engañar. Por ejemplo, en abril de 2010, McAfee identificó sitios web alojados en Rusia y Brasil que anunciaban imágenes y videos para el Mundial de la FIFA de 2010. Sin embargo, en lugar de dirigirse a contenido del Mundial, en realidad publicitaban programas antivirus no autorizados, suplantaban la información personal y financiera de los consumidores (phishing), o intentaban instalar software malicioso en el equipo del usuario.

### Películas "gratis", salvapantallas y pósteres

¿Cómo es de seguro realizar búsquedas en Internet de información relacionada con películas, como por ejemplo índices de clasificación, reseñas y cines? ¡Sorprendentemente seguro! Sin embargo, los consumidores se exponen al riesgo de forma significativa cuando buscan películas "gratis" o "salvapantallas gratis" relacionados con películas. Además, los pósteres e imágenes de películas suelen esconder sorpresas no deseadas, como por ejemplo software malicioso.

McAfee fue consciente por primera vez de las amenazas relacionadas con las películas en 2009, cuando se estrenó el tráiler de *Luna Nueva* en los premios MTV Music Awards. El mismo día, los investigadores de McAfee observaron la aparición repentina de

diversos pósteres de *Luna Nueva* en .JPG y archivos .GIF infectados con software malicioso en distintos lugares en Internet, como por ejemplo foros de fans y páginas wiki. Desde ese momento, esta tendencia se ha observado en películas notorias y muy esperadas.

En general, cuando se busca contenido informativo y de entretenimiento sin conocer su procedencia o sin estar seguros de la legitimidad del sitio en el que se encuentran, y no se cuenta con el software de seguridad necesario y las configuraciones en el equipo, uno se expone a un riesgo mayor.

### Sitios de fans de películas

McAfee Labs encontró más riesgos en varios sitios web de fans de películas. Un fan de una película, que puede que tenga pocos conocimientos de seguridad, visita un sitio para recabar información sobre su estrella favorita. Sin que el fan tenga la menor idea, el sitio podría estar infectado y comprometido por estafadores que están deseando aprovecharse de los fans.

Sin embargo, muchas veces los ataques no son ni siquiera tan sofisticados. Cualquiera puede publicar un vínculo a un sitio web malicioso o distribuir una imagen que incorpora software malicioso. Desde siempre, estos sitios secundarios (de poco tráfico) son los más sencillos y los que más éxito tienen para infectar a los usuarios. De hecho, es bastante común encontrar múltiples sitios de fans creados por ciberdelincuentes con la finalidad expresa de conseguir tráfico para vender anuncios o infectar usuarios.

Es más probable que estos sitios secundarios creados por fans de películas con buenas intenciones no noten la vulneración de la seguridad en su sitio y por lo tanto no puedan actuar de inmediato y de manera necesaria para limpiar su página. McAfee ha descubierto una serie de sitios web de este tipo que todavía contienen vestigios de ataques que ocurrieron con varios meses de anterioridad.

De hecho, es bastante común encontrar múltiples sitios de fans creados por ciberdelincuentes con la finalidad expresa de conseguir tráfico para vender anuncios o infectar usuarios.



## Películas

Se sabe que las películas que todavía no cuentan con una amplia distribución son un objetivo de búsqueda muy popular entre los ciberdelincuentes, que anticipan que una gran cantidad de personas buscará dichas películas online.

Los consumidores se introducen en terreno peligroso cuando buscan películas que sólo se encuentran en cines locales y no cuentan con una distribución global, o cuando buscan películas que todavía no están disponibles, como por ejemplo la última película de Harry Potter.

Los ciberdelincuentes ponen trampas al anunciar estas películas tan solicitadas. Una vez que el consumidor hace clic en su sitio web, éstos proporcionan a los consumidores programas antivirus de seguridad fraudulentos, herramientas peligrosas (que en principio están diseñadas para ayudar a los usuarios a descargarse películas o programas), o ataques y descargas ocultos. (Un ataque "oculto" se produce en el PC del usuario sin que se requiera la autorización expresa ni la acción del mismo, de manera que éste ni siquiera es consciente de que se ha producido dicho ataque).

Los gobiernos y varias asociaciones industriales han divulgado el hecho de que piratear contenido quebranta la ley, sin embargo la gente continúa haciéndolo. Más allá de consideraciones legales, los consumidores necesitan comprender los riesgos a los que se exponen ellos mismos y a sus equipos al acceder a estos sitios web. Particularmente, aunque un sitio parezca legítimo, puede que no lo sea.

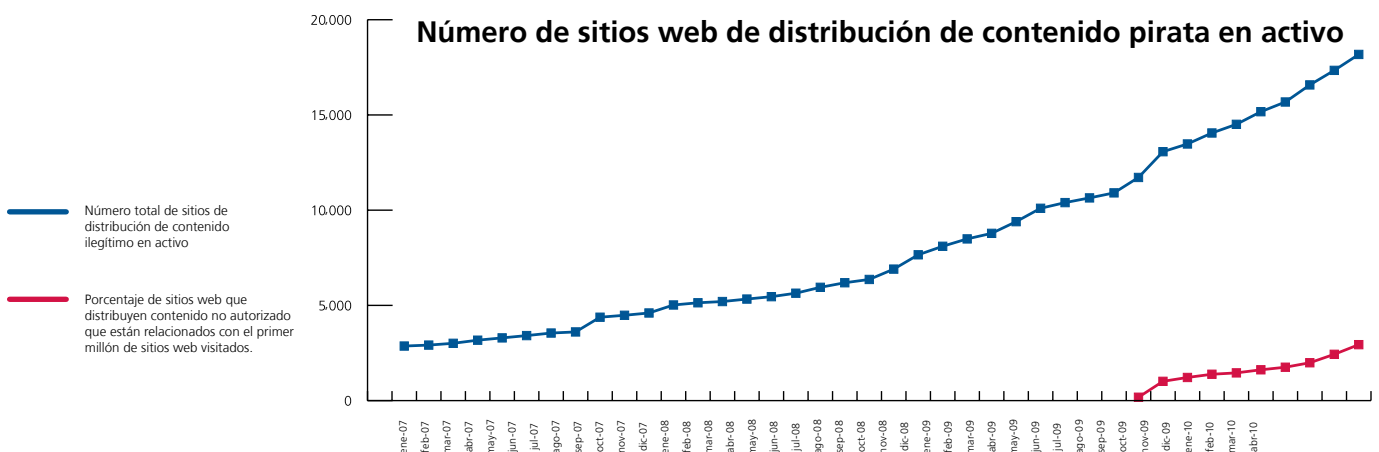
Los consumidores deberían actuar con cuidado y asegurarse de que cuentan con un software de seguridad actualizado que pueda bloquear y eliminar virus, spyware y adware de su ordenador.

## Televisión

Tras su debut en los Estados Unidos, el final de la serie de televisión *Lost* se vio en todo el mundo con restricciones en algunos países como Alemania. Este hecho no impidió que algunos de los fans de *Lost* vieran el final. Encontraron una manera de evitar estas restricciones a través de unos servicios de anonimización. Los servicios de anonimización permiten a los usuarios mantenerse en el anonimato, enmascarar o falsear el lugar desde el que estaban viendo el programa.

Mientras que los servicios de anonimación son prácticos, los consumidores deberían tener presente que cuesta dinero mantenerlos. Los sitios que distribuyen contenido ilegal necesitan vender publicidad para pagar la banda ancha y el almacenamiento necesarios y éstos no son necesariamente exigentes en cuanto a la procedencia del dinero. Ante esta situación, los usuarios deberían ser recelosos al proporcionar información a estos sitios o al descargar cualquier tipo de herramienta que les puedan ofrecer. Por ejemplo, los estudios de McAfee han determinado que un usuario puede recibir una cantidad significativa de "publicidad no deseada" una vez que se registra en uno de estos sitios web.

Mientras tanto, presenciamos cómo crece el número de sitios web diseñados únicamente para atraer usuarios y dirigirlos a sitios ilegítimos. El gráfico que aparece más abajo representa el número de servidores que alojan sitios web que envían usuarios hacia contenido ilegítimo. La línea azul detalla el número total de sitios activos que distribuyen dicho contenido. La línea roja indica qué porcentaje de estos sitios que distribuyen contenido desautorizado está asociado con los 1.000.000 de sitios web más visitados (según los datos de Alexa).



La popularidad de los sitios web de contenido pirata está aumentando.

Los sitios que distribuyen contenido no autorizado no son sólo numerosos, también pueden resultar altamente engañosos. Puede resultar muy difícil para el consumidor medio determinar si éstos son servicios legales. Esto es porque en estos sitios, los usuarios pueden clasificar las descargas de películas, configurar alimentadores RSS y encontrar vínculos a sitios web legítimos, como por ejemplo IMDb.com (La Base de Datos de Películas de Internet). Todas estas características los hacen más convincentes frente a los usuarios. Por eso, contar con un software de seguridad y con herramientas de búsquedas seguras y actualizadas es esencial para el consumidor medio que no puede detectar estos sitios altamente engañosos.

### Publicidad maliciosa

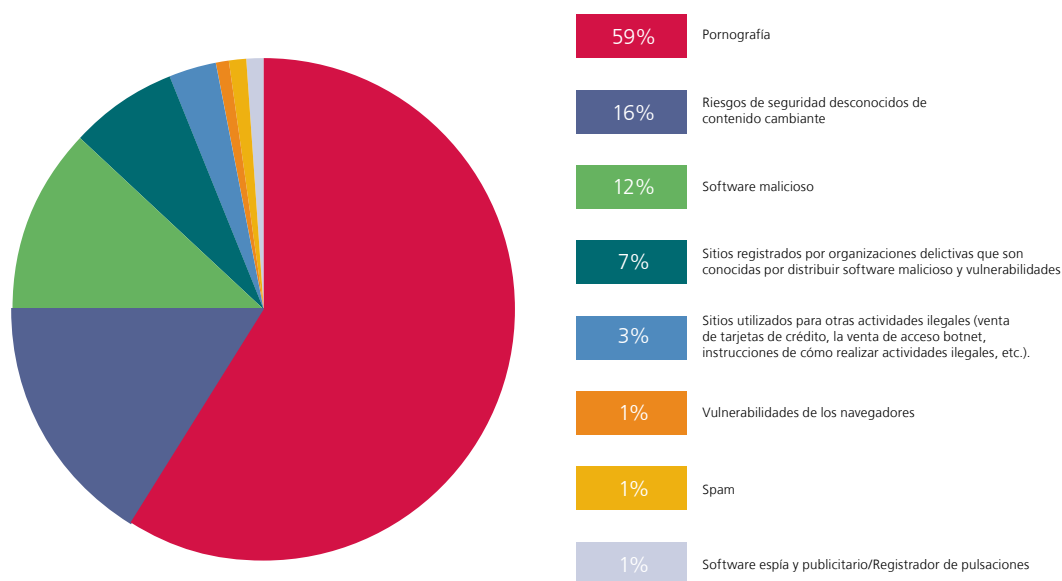
La publicidad online en los sitios web de contenidos audiovisuales se ha convertido en una manera efectiva para conseguir que los consumidores hagan clic en vínculos peligrosos. Estos vínculos pueden conducir a virus, a un sitio web de antivirus fraudulentos o a un ataque a la vulnerabilidad del navegador que redireccionará o alterará la configuración de su equipo, redireccionará URLs o distribuirá contenido sin su conocimiento. Todo esto sucede porque los ciberdelincuentes pueden adaptar sus anuncios a la audiencia del sitio web, haciendo que parezcan legítimas e interesantes.

El gráfico que hay a continuación ilustra los riesgos a los que los consumidores se enfrentan cuando deciden utilizar sitios que publicitan contenido no autorizado. Los visitantes pueden exponerse a pornografía, robo de identidad, robo de información, distribución de software malicioso y otros riesgos.

Tenga en cuenta que el 7 % de los sitios web que distribuyen contenido no autorizado tienen asociaciones con organizaciones de ciberdelincuentes. Los sitios suelen tener un aspecto muy profesional y pretenden seducir al usuario con la idea de un "periodo de prueba" o incluso una cuota mínima muy inferior a lo que se cobra en última instancia. Una vez que el usuario envía su información, los ciberdelincuentes tienen acceso a la misma y la pueden usar con fines maliciosos.

De nuevo, los consumidores deberían recordar que "gratis" suele ser el gancho que usan los ciberdelincuentes y que el consumidor medio no puede identificar la ilegitimidad de una reclamación o sitio web. Con los potentes avances de la ciberdelincuencia, el contenido ilegal se ha convertido en una plataforma más diseñada para atraer y atacar a los consumidores con tecnología sofisticada con el fin de que el usuario no sea consciente de los riesgos a los que se han expuesto.

## Riesgos de los sitios web que anuncian contenido no autorizado



Este gráfico proporciona los detalles sobre los riesgos asociados con el acceso a sitios web que distribuyen contenido no autorizado.



La publicidad online en los sitios web de contenidos audiovisuales se ha convertido en una manera efectiva para conseguir que los consumidores hagan clic en vínculos peligrosos.

## Peligros de la música digital

Hay muchos aspectos de la música digital, desde los sitios web de letras musicales y páginas de fans a la distribución de contenidos de radio sin interrupción y sitios web de descarga de MP3, que ofrecen a los ciberdelincuentes una multitud de formas de engañar a los consumidores menos precavidos. Mientras que algunas plataformas como la iTunes store de Apple Inc. han contribuido a que los usuarios compren contenido acreditado y legítimo, nos volvemos a encontrar con que una fuerte demanda por el contenido, interacción y entretenimiento gratuitos ha desarrollado numerosos riesgos.

### MP3 descargas

Por ejemplo, entre 2009 y 2010, McAfee observó un aumento del 40% en el número de sitios web que distribuyen MP3 infectados o que parecen haber sido contruidos con el único propósito de perpetrar algún tipo de ciberdelito (por ejemplo, robo de la identidad, fraude financiero, transmisión de software malicioso) a través personas que buscan archivos MP3 online.

### Vínculos y Tweets

Los ciberdelincuentes suelen publicar vínculos maliciosos en blogs y en foros y desvían el tráfico mediante el envío de tweets a los fans que contengan estas URLs. Los usuarios hacen clic en el vínculo tranquilamente, y sólo tras haberlo hecho pueden visualizar el contenido. De esta manera ofrecen a los ciberdelincuentes la oportunidad de propagar software malicioso sin su conocimiento.

Por ejemplo, McAfee realizó una búsqueda de "Lady Gaga" en mayo de 2010. Los resultados de dicha búsqueda obtuvieron un vínculo a un sitio web de Lady Gaga y un foro de fans. Sin embargo, al hacer clic en el vínculo, observamos publicidad que nos dirigía a contenido para adultos así como a un "servicio videotelefónico". El servicio de video dirigía a los consumidores a una dirección web a través de la cual podrían conocer "solteras calientes y atractivas". ¡Imagínese a qué podrían estar expuestos los jóvenes y los adolescentes vulnerables si realizaran esta búsqueda y continuaran haciendo clic!

### YouTube y descargas musicales

YouTube es un sitio web que ha tenido un fuerte impacto en la industria de la música. Cualquier grupo puede grabar una actuación y subirla a YouTube para darse a conocer, conseguir fans o simplemente compartir vídeos de forma mutua. Los creadores de software malicioso también son conscientes de la popularidad de YouTube y se han aprovechado muy bien de ella.

En junio de este año, los investigadores también descubrieron más de 700.000 páginas web diseñadas para tener un aspecto idéntico a YouTube, con la excepción de que éstas se habían creado para distribuir software malicioso. Engañaban a los consumidores con la promesa de un vídeo "que no se podían perder" relacionado con la mancha de crudo de British Petroleum, las eliminatorias de la Asociación Nacional de Baloncesto (NBA), películas de Harry Potter y otros temas de actualidad. Las páginas falsas contenían incluso el logo de YouTube. Pero cuando los usuarios intentaban reproducir el vídeo, se les incitaba a descargar e instalar un programa. Al hacer clic en "OK", sus navegadores se redirigían a otros sitios hasta que finalmente acababan en un sitio web de distribución de software malicioso.

Los medios audiovisuales sociales hacen más rápido y fácil que podamos compartir información con amigos y, a medida que crecen en cuanto a uso y popularidad, es cada vez más fácil distribuir estas amenazas.

### Búsquedas relacionadas con la música

No es quien eres lo que te hace peligroso, es tu posición en el ranking. Esta es la conclusión a la que llegó McAfee tras investigar qué artistas musicales estaban asociados a un mayor riesgo al realizar una búsqueda de los mismos por Internet. Los artistas que ocupan los primeros puestos de la lista de éxitos de cada país (tanto si se trata de los 40 principales de *Billboard* en los EEUU o los 50 primeros puestos de la lista de éxitos ARIA de Australia) suponían un mayor riesgo para los fans que realizaban búsquedas acerca de ellos.

A continuación se presentan los principales resultados de búsquedas relacionadas con la música en las que "riesgo" hace referencia a la exposición de los usuarios a cualquiera de los siguientes elementos: software espía y publicitario, antivirus fraudulentos, software malicioso y pornografía.

- **Los números 1 aumentan el riesgo:** La búsqueda de un artista popular junto con sus éxitos más actuales aumenta el riesgo de la misma, frente a si sólo se realiza la búsqueda a través del artista.
- **Letras versus tonos de llamada:** Las búsquedas de "letras de canciones" de un artista en concreto son el doble de peligrosas (por término medio) que las búsquedas de "tonos de llamada" de los mismos artistas en las cinco primeras páginas. Sin embargo, si un usuario continúa más allá de las cinco primeras páginas, "los tonos de llamada" suelen ser, por lo general, un término de riesgo.
- **De nuevo, lo gratuito puede salir caro:** Añadir la palabra "gratis" a tonos de llamada conlleva un riesgo tres veces mayor en los sitios encontrados por los mayores buscadores.
- **Pague para estar seguro:** Añada la palabra "comprar" a "tonos de llamada" y los resultados de búsqueda serán inmediatamente más seguros.
- **Los salvapantallas no lo van a salvar a usted:** La búsqueda del artista más el "salvapantallas" produjo un aumento del riesgo adicional del 50% sobre el riesgo asociado con los "tonos de llamada".
- **Peligros de los "MP3":** Buscar "MP3" conlleva incluso más riesgos que eliminar el término "MP3" de la ecuación de búsqueda.





## Resumen

La ciberdelincuencia es un gran negocio y los medios audiovisuales online son una de las minas de oro más grandes de los ciberdelincuentes. La demanda de los medios audiovisuales, tanto si se trata de música, vídeos, televisión u otro contenido en streaming, ha alcanzado proporciones alarmantes, y los ciberdelincuentes pretenden explotar su popularidad de todas las maneras posibles.

A medida que los medios audiovisuales online y los dispositivos cambian, creemos que las amenazas se adaptarán y se harán más imperceptibles, aunque no esperamos que desaparezcan. La simple búsqueda de medios audiovisuales online puede parecer segura, sin embargo, la verdad es que los ciberdelincuentes se sirven de muchas maneras diferentes de distribuir amenazas. Las amenazas se han desarrollado más allá de las búsquedas de alto nivel y están más presentes que nunca.

La única manera de que los usuarios estén protegidos es tomar conciencia de los riesgos asociados con los medios audiovisuales digitales, permanecer atentos ante nuevos peligros potenciales y utilizar un software de seguridad integral.

A continuación detallamos algunos consejos importantes para garantizar nuestra seguridad mientras que disfrutamos de los medios audiovisuales digitales.

- Evite buscar contenido "gratis". En su lugar, diríjase a sitios web legítimos y de pago para adquirir música y películas.

- No haga clic en vínculos de banners sobre sitios web de música, películas y descargas que no estén bien establecidos.
- Para estar a salvo de las últimas amenazas, instale un software de seguridad integral como McAfee® Total Protection que esté continuamente actualizado y que prevenga, bloquee y elimine amenazas potenciales.
- Use el sentido común: no haga clic en vínculos publicados en foros o páginas de fans y utilice sitios web de medios audiovisuales bien establecidos.
- Utilice un complemento seguro de búsqueda como el software McAfee SiteAdvisor® para que éste le avise de sitios potencialmente peligrosos durante sus búsquedas.
- Tenga en cuenta que cuanto más solicitado y popular sea un tema, una película o un artista, mayor es el riesgo al que se enfrenta cuando los busca en Internet.

## Acerca de McAfee, Inc.

McAfee, Inc., con sede en Santa Clara, California, es la empresa dedicada a la tecnología de seguridad más importante del mundo. La empresa proporciona servicios y soluciones proactivas y comprobadas que ayudan a hacer más seguros los sistemas, redes y dispositivos móviles en todo el mundo, y permiten a los usuarios conectarse, navegar y comprar en Internet con mayor seguridad. Respaldada por el inigualable McAfee Global Threat Intelligence, McAfee crea productos innovadores que ayudan a los usuarios, las empresas, el sector público y los proveedores de servicios, permitiéndoles cumplir con las normativas, proteger datos, prevenir interrupciones, identificar vulnerabilidades, así como controlar y mejorar continuamente la seguridad. McAfee asegura su mundo digital.

<http://www.mcafee.com>



McAfee, Inc.  
2821 Mission College Boulevard  
Santa Clara, CA 95054  
1.866.622.3911  
[www.mcafee.com](http://www.mcafee.com)

La información incluida en este documento se proporciona sólo con fines educativos y para la conveniencia de los clientes de McAfee. La información aquí contenida está sujeta a cambios sin previo aviso y se proporciona "TAL COMO ESTÁ", sin garantía ni aval en cuanto a la precisión o la aplicabilidad de la información relacionada con cualquier situación o circunstancia específica.

McAfee, el logotipo de McAfee, McAfee Labs, McAfee Total Protection y SiteAdvisor son marcas registradas o marcas comerciales de McAfee, Inc. o sus subsidiarias en los Estados Unidos y en otros países. Otras marcas pueden reclamarse como propiedad de otros. Los planes, especificaciones y descripciones de los productos aquí mencionados se ofrecen sólo con fines informativos, están sujetos a cambio sin previo aviso y se proporcionan sin garantía de ningún tipo, ya sea expresa o implícita. Copyright © 2010 McAfee, Inc.  
13201rpt\_dig-music-movies\_0810