

Definiendo el significado de los programas espía

Prólogo

Por favor, consulte la [introducción](#) a nuestra sección Glosarios, para una mejor comprensión de los criterios, terminología y convenciones utilizadas.

 **Importante:** Se sugiere la consulta al [Glosario sobre terminología básica](#) antes de la lectura de este documento.

 Podrá hacer búsquedas simples en cada página, utilizando el atajo de teclado **Control + F**

Definiciones de la Coalición contra programas espía (Anti-Spyware Coalition)

Primeros conceptos

En la actualidad, los programas espía no representan sólo una molestia, sino que se han convertido en una de las amenazas más graves que enfrenta Internet. Muchos usuarios se encuentran atrapados en una batalla cíclica contra los programas que se instalan sin avisar, abren peligrosos agujeros de seguridad y se reinstalan después de haber sido eliminados.

Los peores tipos de estos programas habilitan a los delincuentes informáticos para secuestrar la información personal y/o confidencial del usuario, cada vez que lo deseen. Incluso las variantes más benignas pueden perjudicar el rendimiento del ordenador, al emplear sus recursos de procesamiento en servicios no solicitados.

Para empeorar el problema, los desarrolladores de códigos espía utilizan sofisticadas estratagemas, de modo de lograr la instalación de estos programas en los ordenadores de usuarios desprevenidos. A menudo, para difundir estas aplicaciones indeseadas, los distribuidores de programas espía se sirven de las vulnerabilidades de seguridad, de estafas inteligentes, de algunas distribuciones poco claras de programas agrupados y de otras prácticas.

A medida que la amenaza crece, aumenta la necesidad de montar una defensa coordinada contra estos programas no solicitados y sus efectos adversos.

La **Coalición contra programas espía (Anti-Spyware Coalition)** fue convocada para reafirmar esa defensa, progresando a partir de los grandes avances que la industria de la tecnología ya ha realizado para combatir este problema.

Durante los últimos años, los fabricantes de ordenadores y los desarrolladores de programas han tomado serias medidas para proteger sus productos, y para educar a los consumidores en la prevención contra los programas espía.

Al mismo tiempo, la sólida industria contra programas espía, en constante crecimiento, ha creado una serie de herramientas para ayudar a los consumidores a identificar y eliminar de sus ordenadores la tecnología no solicitada. La coalición contra programas espía está compuesta de grupos públicos de interés, asociaciones de comercio y las más importantes empresas desarrolladoras y distribuidoras de productos contra programas espía.

Combinando los conocimientos técnicos de todos sus miembros, la coalición está trabajando para establecer definiciones, herramientas y prácticas para mejorar la efectividad de la tecnología contra programas espía, y para ayudar a los consumidores a comprender aún mejor cómo funcionan estas herramientas.

Los miembros de la coalición consideraron vital establecer definiciones comunes de programas espía y otras tecnologías potencialmente no solicitadas, de modo que los proveedores, los desarrolladores de programas y los consumidores puedan comunicarse mejor acerca de los tipos de tecnologías que presentan problemas, y de cómo las aplicaciones de seguridad identifican los programas no solicitados.

Los siguientes documentos representan la finalización de la primera fase de ese proceso.

- Una definición simple y formal de programas espía y otras tecnologías potencialmente indeseables, con que la coalición define el conjunto de técnicas informáticas que pueden afectar negativamente el uso, la privacidad o la seguridad de los usuarios.

- Un **Glosario** exhaustivo, que ofrece definiciones claras para los términos comúnmente utilizados en discusiones acerca de programas espía y otras tecnologías potencialmente perjudiciales.

📖 El [Glosario sobre las amenazas de Internet](#), presentado en esta sección, incluye también las definiciones aportadas por la Coalición contra programas espía.

- Un grupo de pautas comunes de la industria, para el proceso de resolución de conflictos con el proveedor. Este documento describe los pasos que los productores y distribuidores de soluciones contra programas espía deberían seguir, en casos en que los desarrolladores aleguen que es inadecuada la clasificación de sus aplicaciones como programas espía.
- Finalmente, los consejos de seguridad contra programas espía, ofrecen una guía básica para que los consumidores puedan proteger sus datos privados y sus ordenadores.

Estos documentos son borradores de trabajo, que serán el fundamento de los esfuerzos constantes de la coalición contra programas espía.

Establecen la base para el trabajo permanente y futuro de la coalición.

Los documentos evolucionarán a medida que se identifiquen nuevos problemas y se profundicen nuestros conocimientos.

Continuamente necesitamos información, de parte de los usuarios de todos nuestros documentos públicos, a medida que avanzamos.

Acerca de la coalición contra programas espía

La coalición contra programas espía es un grupo dedicado a crear consenso acerca de definiciones y mejoras prácticas en el debate acerca de códigos espía y otras tecnologías potencialmente nocivas.

Compuesta de empresas de aplicaciones contra programas espía, académicos y grupos de consumidores, esta coalición busca reunir un grupo diverso de perspectivas acerca del problema de controlar estas amenazas y las de otras tecnologías potencialmente no deseadas.

El [Centro para la Democracia y la Tecnología](#) (CDT, *Center for Democracy and Technology*) es el coordinador de la coalición contra programas espía.

Las empresas de aplicaciones contra programas espía o los grupos públicos de interés que deseen unirse a la coalición, deben contactarse con Ari Schwartz, director adjunto del C.D.T., escribiendo a asc@cdt.org.

Los programas espía y otras tecnologías potencialmente no deseadas

Tecnologías implantadas sin el consentimiento adecuado por parte del consumidor y/o implementadas de forma que dificultan el control del usuario sobre:

- Los cambios materiales que afectan su uso y su privacidad, o la seguridad del sistema.
- El uso de los recursos del sistema, incluyendo la instalación de programas en sus ordenadores.
- La recolección, uso y distribución de información personal u otros datos confidenciales.

Ejemplos de programas espía y tecnologías potencialmente indeseables

La siguiente tabla enumera algunas tecnologías que han sido utilizadas para dañar o incomodar a los usuarios de ordenadores.

Es importante tener en cuenta que con un aviso adecuado, consentimiento y control, algunas de estas tecnologías pueden brindar importantes beneficios.

El seguimiento puede utilizarse para la personalización de la navegación en Internet, la publicidad puede subsidiar el costo de un producto o servicio, las herramientas de monitorización pueden prevenir el acceso a sitios indeseados y las características de control remoto pueden permitir que los servicios de soporte técnico diagnostiquen problemas de forma remota.

Por ejemplo, la tecnología subyacente que utiliza un capturador de pulsaciones del teclado (*keylogger*) es un programa de seguimiento.

El programa de seguimiento puede tanto dañar como ayudar al usuario.

Un *keylogger* puede utilizarse para fines legítimos y con pleno consentimiento, por ejemplo, para permitir al personal de soporte técnico que asista a un usuario en el diagnóstico de un problema, desde un equipo remoto.

En cambio, cuando un *keylogger* se instala y ejecuta de manera encubierta, se trata de un programa espía.

La tecnología subyacente, por lo general, se convierte en indeseable cuando se implementa de una forma que no brinda beneficios, o directamente provoca daños, a los usuarios autorizados.

• **Grupo 1**

Programas involucrados

- Programas espía (limitado)*
- Programas para seguimiento (*Snoopware*)
- Capturadores de pulsaciones de teclado (*Keylogger*) no autorizados
- Capturadores de pantalla (*Screen scraper*) no autorizados

Tecnología subyacente

Programa de seguimiento

Utilizado para monitorear el comportamiento o reunir información acerca del usuario, que algunas veces incluye datos de identificación personal u otra información confidencial.

¿Por qué la tecnología subyacente puede ser indeseable?

- Realiza un seguimiento encubierto, lo que equivale a espiar.
- Compila información personal que puede compartirse ampliamente o ser robada, lo que resulta en fraude o robo de identidad.
- Puede utilizarse para cometer otros delitos, por ejemplo, violencia doméstica y acoso sexual.
- Puede disminuir el rendimiento del equipo.
- Puede asociarse con riesgos en la seguridad y/o pérdida de datos.

¿Por qué la tecnología subyacente puede ser requerida?

- Puede utilizarse para un control legítimo: por parte de los padres o las empresas, entre otros ejemplos.
- Puede ser un componente necesario de programas de publicidad (*adware*), vinculado a programas solicitados.
- Puede permitir la personalización del sistema

• **Grupo 2**

Programas involucrados

- *Adware* molesto o dañino

Tecnología subyacente

Programa de publicidad

Cualquier programa que muestra contenido publicitario.

¿Por qué la tecnología subyacente puede ser indeseable?

- Puede ser una molestia y reducir la productividad.
- Puede mostrar contenido censurable.
- Puede disminuir el rendimiento del equipo, causar denegaciones de servicio o pérdidas de datos.
- Puede no brindar a los usuarios las herramientas de eliminación adecuadas.
- Puede estar asociado con riesgos de seguridad.

¿Por qué la tecnología subyacente puede ser requerida?

- Puede estar vinculada a otro programa o contenido solicitado, subsidiando su costo.
- Puede brindar publicidad requerida por el usuario.

• Grupo 3

Programas involucrados

- Puertas traseras
- Redes de ordenadores infectadas (*Botnets*)
- Programas para el control remoto de ordenadores (*Droneware*)

Tecnología subyacente

Programas de control remoto

Utilizados para permitir el acceso o control remoto de sistemas de informática

¿Por qué la tecnología subyacente puede ser indeseable?

- Puede capturar el equipo de un usuario para transformarlo en un remitente de correo masivo, para enviar ataques de denegación de servicio o para utilizarlo como servidor de contenido malicioso o inapropiado.
- Si se realiza en forma encubierta, equivale a robar ciclos del procesador y otros recursos.
- Puede disminuir el rendimiento de los equipos.
- Puede estar asociado a la pérdida de datos.
- Puede compartir demasiado ampliamente la información personal, o permitir su robo.

¿Por qué la tecnología subyacente puede ser requerida?

- Puede permitir el soporte técnico o la resolución de problemas de forma remota.
- Puede brindar, a los usuarios, acceso remoto a sus propios datos o recursos.

• Grupo 4

Programas involucrados

- Programas de marcado no autorizados

Tecnología subyacente

Programas de marcado

Se utilizan para realizar llamadas o acceder a servicios por medio de un módem o conexión a Internet.

¿Por qué la tecnología subyacente puede ser indeseable?

- Puede generar el marcado de llamadas interurbanas o internacionales indeseadas, con costos a cargo del usuario.

¿Por qué la tecnología subyacente puede ser requerida?

- Puede permitir el acceso a servicios solicitados.

• Grupo 5

Programas involucrados

- Secuestradores
- Troyanos que impiden la detección de claves del registro (*Rootkits*)

Tecnología subyacente

Programas modificadores del sistema

Utilizados para modificar las configuraciones en el sistema: por ejemplo, las páginas de inicio y las páginas de búsqueda en Internet, el reproductor de medios predeterminado, u otras funciones del sistema en niveles inferiores

¿Por qué la tecnología subyacente puede ser indeseada?

- Sin un consentimiento adecuado, la modificación del sistema se considera secuestro.
- Puede comprometer la integridad y la seguridad del sistema.
- Puede enviar al usuario a sitios de Internet falsificados para robar su identidad.

¿Por qué la tecnología subyacente puede ser requerida?

- Puede utilizarse para la personalización del sistema a pedido del usuario

Grupo 6

Programas involucrados

- Herramientas de delincuentes informáticos (incluyendo a los verificadores de puertos)

Tecnología subyacente

Programas de análisis de seguridad

Utilizados por el usuario de un ordenador para analizar o sortear protecciones de seguridad.

¿Por qué la tecnología subyacente puede ser indeseable?

- Con frecuencia se utilizan con objetivos maliciosos.
- La presencia puede violar las políticas corporativas o las reglas aplicadas por una familia.

¿Por qué la tecnología subyacente puede ser requerida?

- Puede utilizarse para investigación de seguridad y otros propósitos legítimos.

• Grupo 7

Programas involucrados

- Programa de descarga automática

También recibe la denominación de *Trickler*.

Tecnología subyacente

Programas de descarga automática

Utilizados para descargar e instalar programas sin interacción con el usuario.

¿Por qué la tecnología subyacente puede ser indeseable?

- Puede ser utilizado para instalar aplicaciones no autorizadas, incluyendo las mencionadas anteriormente.

¿Por qué la tecnología subyacente puede ser requerida?

- Puede utilizarse para las actualizaciones automáticas u otras operaciones de mantenimiento automático del sistema.

• Grupo 8

Códigos involucrados

- *Cookies* de seguimiento no autorizadas

Tecnología subyacente

Tecnología de seguimiento pasivo

Utilizada para reunir información limitada acerca de las actividades del usuario, sin instalar ningún programa en los ordenadores de los usuarios.

¿Por qué la tecnología subyacente puede ser indeseable?

- Puede permitir la recolección indeseada de información (por ejemplo, los sitios de Internet que el usuario haya visitado)

¿Por qué la tecnología subyacente puede ser requerida?

- Puede utilizarse para personalización o modificaciones solicitadas. Por ejemplo, búsqueda de elementos similares que podrían interesar al usuario.
- Puede evitar que los publicistas muestren, con demasiada frecuencia, los mismos anuncios a la misma persona.