

Descargas seguras



Claves que debes conocer para protegerte eficazmente

Las descargas de archivos son una parte importante del día a día en Internet, ya que nos ayudan a compartir contenido entre plataformas e internautas. Por desgracia, hay ciberdelincuentes que utilizan las descargas para colarse en nuestros dispositivos y llevar a cabo acciones perjudiciales para nuestros intereses.

Afortunadamente, vigilar los archivos que descargamos para garantizar la seguridad en la red es una tarea sencilla que puedes poner en práctica hoy mismo. De hecho, **la mejor herramienta a tu alcance es la precaución**. Por ejemplo, si no entiendes qué te ofrece la página web para descargar, no aceptes el contenido.

Esta es la clave para conseguir una protección eficaz. Procura leer a fondo qué es lo que vas a almacenar en tu dispositivo, busca información al respecto y actúa en consecuencia. En caso de que certifiques que estás frente a una amenaza, abandona el sitio web.

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Ofic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

A continuación te facilitamos algunas pautas adicionales para que gestiones tus archivos descargados de forma segura y responsable.

1. **Cómo actuar frente a las descargas:**

Existen todo tipo de sitios web de descargas en los que acceder a una amplia variedad de archivos. Películas, videojuegos, libros o canciones son algunos de los ejemplos más habituales. Si bien no tendrás problemas para encontrar una página que cumpla la ley, existen sitios en los que es posible realizar una descarga ilegal de contenidos. Es en estos espacios donde hay que extremar las precauciones.

Para empezar, procura no visitarlos ni descargar ninguno de los archivos que ofrecen. No solo estarías cometiendo un delito al descargar una película pirata, por ejemplo, sino que también se podría generar una brecha en la seguridad de tu ordenador. Los propietarios del sitio web podrían insertar programas maliciosos o un virus informático, como es el caso de un troyano, en los archivos.



Además, mientras permanezcas en estas páginas, irán abriéndose ventanas automáticamente. Estos pop-ups o ventanas emergentes suponen un riesgo real, ya que algunas descargan información en tu ordenador sin pedir permiso

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Ofic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

 @CERTpy

 /CERT-py

ni avisar. Por tanto, evitar este tipo de sitios web es una medida muy efectiva de ciberseguridad.

Además de esto, también puedes configurar tu navegador para que bloquee cualquier ventana emergente que aparezca. Esto no solo mejora el rendimiento del ordenador y reduce las molestias que provocan, sino que impide las descargas no deseadas.

El funcionamiento de estas herramientas es muy eficiente, ya que frenan su aparición por completo. Es una forma simple y sencilla de aumentar tu seguridad.

2. Errores frecuentes que debes evitar

Existen diferentes errores frecuentes que debes conocer para poder evitarlos en la medida de lo posible.

- **Clicar en enlaces poco fiables**

Es frecuente clicar enlaces en páginas de terceros o un anuncio de dudosa procedencia. Estos **pueden llegar a tu pantalla a través de un correo electrónico o aparecer en una web**. Por regla general, están pensados para iniciar la descarga de un archivo o para conducirte a un lugar donde efectuarla. Es preciso que no sigas los *links* de este tipo, ya que podrían llevarte a una estafa o a la instalación de programas maliciosos en tus equipos.

Recuerda mantener el sentido común y no descargar un archivo que no entiendas o del que desconozcas su origen. También podrías recibir mensajes con enlaces de este tipo a través de redes sociales. En este caso, no dudes en bloquear a la cuenta que te ha contactado. De esta manera, no podrá seguir enviándote contenido que no te interesa y que potencialmente puede causar daños.

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Ofic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

 @CERTpy

 /CERT-py

- **Utilizar aplicaciones gratuitas de origen dudoso**

Puedes encontrar una amplia variedad de aplicaciones de uso gratuito. La mayoría son pruebas de algunas funcionalidades de un programa concreto. Un buen ejemplo son los antivirus, los cuales suelen ofrecer una protección básica sin coste, que puedes mejorar según tus necesidades. Si bien su funcionamiento es lícito y eficaz, podrías encontrarte con programas maliciosos.

Presta especial atención a aquellos programas que se encarguen de tareas sensibles, ya que pueden suponer una amenaza, por ejemplo en el caso de usar una VPN privada. Se trata de un programa que te permite acceder a una red privada, algo útil para navegar con seguridad y de forma anónima.

Al poder afectar a tu privacidad y bienestar en Internet, procura no emplear productos gratuitos y de procedencia dudosa para este tipo de funciones. Podrían resultar en un acceso indebido a tu ordenador.

- **No disponer de programas de seguridad**

Los antivirus son una defensa excepcional para evitar descargas potencialmente dañinas. Estos se encargan de analizar el fichero en busca de irregularidades y lo ponen en cuarentena si detectan algún problema. De hecho, llegan a impedir el acceso a las páginas de origen si estas no son suficientemente seguras. Además, te impiden abrir el archivo por despiste.

Su funcionamiento suele ser muy bueno, pero en ocasiones se dan falsos positivos. Suceden cuando adquieres un programa en una

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Ofic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

 @CERTpy

 /CERT-py

página legal y no sospechosa. El antivirus detecta algún problema y evita que accedas al archivo en cuestión. Es por esto que lo mejor es tener muy en cuenta la página o plataforma en la que realizas la descarga, ya que es un indicador fiable de que no habrá problemas.

- **Mantener los programas, aplicaciones y navegadores desactualizados**

Cualquier programa o aplicación desactualizada se puede convertir en una fuente de problemas. **Los desarrolladores las actualizan para reforzar su seguridad frente a nuevas amenazas**, así como para mejorar su funcionamiento. Por tanto, si no las mantienes al día, no detectarán posibles amenazas al efectuar una descarga. Al no estar preparados, no podrán reconocer los peligros que encierra el archivo.

Esto **también se extiende a los navegadores, cuyo funcionamiento no será el óptimo**. No te impedirán entrar en páginas inseguras, ya que no reconocerán las faltas de seguridad. Por suerte, evitar este error es tan simple como mantener actualizados los programas y aplicaciones que utilices. No te llevará mucho tiempo, pero te ahorrará más de un disgusto a largo plazo.

¿Cómo llevar a cabo una descarga segura?

- Lo primero que debes tener en cuenta es dónde vas a realizar la descarga. **Recurre siempre a los sitios del fabricante o páginas de terceros que sean seguras**. Por ejemplo, en el caso de un videojuego, puedes adquirirlo del propio desarrollador o a través de una tienda en línea. Esta es la manera más sencilla de evitar tu exposición a una amenaza. Si optas

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Ofic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

 @CERTpy

 /CERT-py

por piratearlo, tu exposición será mayor y puedes acabar enfrentándote a un problema de seguridad digital.

- En caso de que desconfíes del archivo, no dudes en emplear un antivirus para analizarlo. Esta acción es especialmente recomendable en archivos comprimidos. El problema en estos últimos reside en que pueden contener programas maliciosos en su interior junto a otros que son inocuos. Al descomprimirlos, la amenaza tiene la posibilidad de instalarse en tu ordenador.
- Por último, evita abrir ficheros sospechosos o descargar archivos adjuntos desconocidos. En situaciones como esta, es recomendable eliminarlos. Para asegurarte utiliza antes el antivirus, pero si la duda persiste, envíalos a la papelera de reciclaje. Así, evitarás poner en riesgo el contenido de tu dispositivo.

¿Qué medidas preventivas puedes usar?

- Tienes a tu alcance una amplia variedad de medidas preventivas para garantizar tu seguridad. Para empezar, **recurre a las versiones de prueba de los programas**. Si tienes alguna duda de su comportamiento o de si este puede resultar peligroso, esta versión te permitirá evaluarlo con una exposición mínima. Luego podrás decidir si te convence o no de acuerdo con tu experiencia.
- **Estudia a fondo la información que te ofrecen en la página web acerca del archivo**. Esto te permitirá saber si te están engañando o no. Los comentarios de otras personas te resultarán de ayuda, ya que no dudarán en contar una mala experiencia. Son una advertencia de los

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Ofic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

 @CERTpy

 /CERT-py

posibles riesgos a la hora de llevar a cabo la descarga. Aunque si dudas de la legalidad del sitio, sal inmediatamente.

- **Protege tus dispositivos móviles**, un detalle al que muchas personas no prestan atención. También puedes descargar archivos en ellos, los

cuales están expuestos a los mismos riesgos que un ordenador. Sin embargo, es común ver teléfonos o tabletas sin antivirus ni protección de ningún tipo, lo que permite a los programas maliciosos infectarlos y luego extenderse a otros aparatos conectados.

- **No dejes de controlar activamente lo que descargas y ten especial cuidado con los menores de la casa.** Asegúrate de explicar los riesgos que pueden existir, ya que su falta de conocimiento podría hacer que acaben cayendo en alguna amenaza.

Por ejemplo, podrían acudir a una web fraudulenta pensando que les regalan un videojuego y acabar descargando un virus al ordenador. Por tanto, vigila que no se metan en problemas en un entorno tan amplio como es Internet.

En definitiva, controlar las **descargas** que llevas a cabo es importante para mantener una buena ciberseguridad. Pese a que la mayoría de plataformas son seguras, no olvides actuar de forma precavida. Desconfía si no demuestran qué medidas de seguridad utilizan, recurre al antivirus y elimina los ficheros sospechosos.

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Ofic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

 @CERTpy

 /CERT-py