Universidad de Buenos Aires
Facultad de Ciencias Económicas

Troyanos, Virus y Spyware

Material de Estudio

TROJAN vs VIRUS vs SPYWARE

They're NOT the same — here's the difference

TROJAN

Disguised danger

What it is:
Malware that pretends to be a safe app or file

How it gets in:
You install it yourself (fake app, cracked software, "update")

What it dos:
- Steals data
- Opens backdoors
- Installs more malware
- Takes control quietly

Key idea:
You invite a Trojan in

VIRUS

Self-spreading infection

What it is:
Malware that copies itself and spreads to other files

How it gets in:
Infected files, USB drives, shared documents

What it does:
- Corrupts files
- Slows systems
- Spreads without permission

Key idea:
A virus safe on its own

SPYWARE

Silent observer

What it is:
Malware designed to watch and collect information

How it gets in:
Bundled apps, shady downloads, malicious websites

What it does:
- Tracks activity
- Reads messages
- Logs keystrokes
- Steals personal data

Key idea:
Spyware watches you quietly

CyberSecurity for Computer & AI HuB

Share Like Follow

CYBERSECURITY
For Computer & AI HuB

 Traducción y Comentarios

TROYANO vs VIRUS vs SPYWARE

No son lo mismo — esta es la diferencia

---

1. TROYANO (Trojan)

Peligro disfrazado

Qué es

Malware (*Malicious Software / Software malicioso*) que **simula ser un archivo o programa legítimo**.

Cómo ingresa

- El propio usuario lo instala
- Aplicaciones falsas
- Software pirateado
- Falsas "actualizaciones"

Qué hace

- Roba información
- Abre **backdoors** (*Puertas traseras*)
- Instala más malware
- Toma control del sistema de forma silenciosa

Idea clave

👉 **El troyano entra porque el usuario lo invita.**

En sistemas de información:

Explota fallas humanas, malas prácticas y ausencia de controles de seguridad.

---

2. VIRUS (Virus)

Infección que se auto-propaga

Qué es

Malware que **se copia a sí mismo** y se propaga infectando otros archivos o sistemas.

Cómo ingresa

- Archivos infectados
- Dispositivos USB
- Documentos compartidos

Qué hace

- Corrompe archivos
- Ralentiza sistemas
- Se propaga sin autorización del usuario

Idea clave

👉 **Un virus se propaga por sí solo.**

Impacto organizacional:

Afecta la **disponibilidad** y la **integridad** de los sistemas de información.

---

3. SPYWARE (Software espía)

Observador silencioso

Qué es

Malware diseñado para **vigilar al usuario y recolectar información** sin ser detectado.

Cómo ingresa

- Aplicaciones empaquetadas

- Descargas poco confiables
- Sitios web maliciosos

Qué hace

- Rastrea la actividad del usuario
- Lee mensajes
- Registra pulsaciones del teclado (*Keystrokes*)
- Roba datos personales y credenciales

Idea clave

👉 **El spyware observa y recopila información en silencio.**

Riesgo para la gestión:

Compromete la **confidencialidad** de datos personales, financieros y estratégicos.

Comparación conceptual resumida

Tipo	Forma de ingreso	Comportamiento	Riesgo para la organización
Troyano	Engaño al usuario	Control oculto del sistema	Robo de datos y accesos
Virus	Archivos infectados	Auto-propagación	Caídas y corrupción de sistemas
Spyware	Instalación silenciosa	Espionaje continuo	Fuga de información

---

Enfoque para estudiantes de administración

Diferenciar estos tipos de malware permite:

- diseñar mejores **controles internos**,
- reducir **riesgos operativos**,
- proteger **activos de información críticos**.

La ciberseguridad no es solo un tema técnico: es **gestión del riesgo en los sistemas de información**.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.