CLASIFICACIÓN DEL *MALWARE* SEGÚN SU FORMA DE PROPAGACIÓN

NOMBRE	PROPAGACIÓN	EFECTOS
Virus 	Una vez instalado en la memoria del dispositivo, no se ejecuta automáticamente, sino que espera oculto a que el usuario (sin percatarse del potencial daño) lo ejecute. Inmediatamente empieza a infectar los archivos y a reproducirse, propagándose incluso por todo el sistema informático al que dicho equipo esté enlazado, pero sin propagarse de manera automática a otros sistemas.	De leves a graves, sus efectos van desde simplemente manifestar su presencia con mensajes inoportunos, entorpecer el trabajo del usuario y afectar el desempeño del dispositivo, hasta destruir datos guardados en su disco duro o formatearlo, con la consecuente pérdida de información.
Gusano 	Se reproduce y propaga automáticamente, pasando de un sistema a otro, sin la intervención del usuario, enviando copias de sí mismo, a través del correo electrónico o la mensajería instantánea. Basta con que el dispositivo esté encendido y conectado a la NUBE y que el sistema del cual forma parte tenga vulnerabilidades en su seguridad, para que el gusano se reproduzca y propague a otros sistemas.	Su efecto no consiste tanto en alterar archivos, para afectar el funcionamiento del dispositivo invadido en particular, sino en modificar los parámetros del sistema en general, para, por ejemplo, controlarlo de manera remota o saturarlo para provocar su caída.
Troyano 	Se trata de un ***software*** que, descargado de la NUBE o como adjunto de un correo electrónico, evade la seguridad del dispositivo, aparentando tener una legítima utilidad para el usuario, cuando en realidad tiene una función oculta y potencialmente dañina.	Al ser ejecutado por el usuario del dispositivo, puede ceder el control remoto del mismo al ciberdelincuente, a fin de que, por ejemplo, pueda robar información personal o corporativa, con fines fraudulentos.