¿Qué son «WPA-PSK», «WPA2-PSK», «TKIP» y «AES»?

«WPA» es la sigla en inglés para Wi-Fi Protected Access, una especificación de codificación de datos diseñada para mejorar la seguridad de las redes LAN inalámbricas. Se basa en el Protocolo de Autenticación Extensible (EAP) para asegurar el acceso a la red y utiliza un método de codificación para proteger las transmisiones de datos.

Esta tecnología se implementa típicamente con un servidor de autenticación 802.1X que asigna claves individuales a cada usuario. Sin embargo, también puede ser utilizada en un modo menos seguro llamado «Clave Pre-Compartida» (PSK), diseñado para entornos como hogares u oficinas pequeñas, donde todos los usuarios comparten una misma frase de contraseña. Esta variante se conoce como «WPA-Personal». Tanto en el caso de «WPA-PSK» como de «WPA2-PSK», la máquina inalámbrica de Brother puede asociarse con puntos de acceso utilizando los métodos de codificación TKIP o AES.

TKIP (Temporal Key Integrity Protocol) es un método de codificación que proporciona una clave única para cada paquete de datos, garantizando la integridad del mensaje con un mecanismo de re-escritura.

Por otro lado, AES (Advanced Encryption Standard) es el estándar de codificación seguro autorizado por Wi-Fi.

Tanto «WPA-PSK» como «WPA2-PSK» pueden utilizar TKIP o AES, y requieren una Clave Pre-Compartida (PSK) de al menos 8 caracteres de longitud, con un máximo de 63 caracteres.