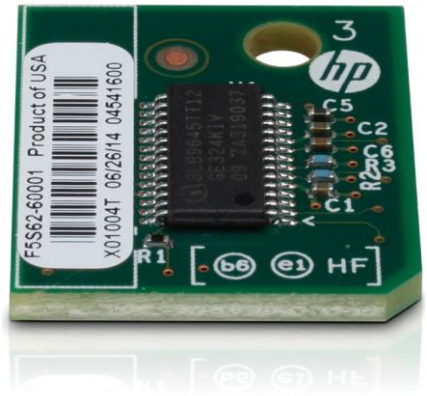
**Hoja de datos**

# HP Trusted Platform Module

## Conecte y proteja

Añada un nivel adicional de seguridad para proteger la información confidencial. El HP Trusted Platform Module (TPM) refuerza la protección de las credenciales y los datos cifrados que están almacenados en su impresora o equipo multifunción[1].




## Identifique y gestione los riesgos

No debe subestimar el valor de los datos de su organización. Cuantos más datos adquiere y comparte, más riesgos y requisitos de seguridad debe afrontar. Su entorno de impresión y procesamiento de imágenes no es inmune a las costosas brechas de seguridad[2]. Las lagunas de seguridad pueden dejar peligrosamente expuestos los datos confidenciales. El HP Trusted Platform Module (TPM) le ayuda a protegerse de esos riesgos.

Con el TPM, puede:

- **Proteger los datos confidenciales de los usuarios:** el TPM es un chip de seguridad de fácil instalación que permite el almacenamiento seguro de información como contraseñas y claves de seguridad. Al sellar automáticamente las claves de cifrado de los dispositivos, el TPM refuerza la protección de las credenciales y los datos codificados que almacenan sus impresoras o equipos multifunción[3]. El TPM "envuelve" las claves de cifrado con su propia clave raíz de almacenamiento, que se guarda dentro del TPM.
- **Proporcionar identidades de dispositivos seguras:** el TPM genera claves privadas para los certificados y las protege. Así tendrá la garantía de que incluso la información, los datos y los documentos más confidenciales de sus clientes están a salvo. La impresora o equipo multifunción usa los certificados creados para verificar la identidad del dispositivo. Como las claves privadas de los certificados nunca salen del TPM, los certificados de identidad no se pueden falsificar o copiar. Esto asegura que la información recibida del dispositivo es legítima y que los datos que se mandan al equipo llegan al destino deseado.
- **Conseguir tranquilidad:** el TPM está diseñado de acuerdo con los estándares internacionales del sector, concretamente el estándar TPM 1.2 del Trusted Computing Group (TCG)[4]. Cuando llegue el momento de retirar su impresora o equipo multifunción, podrá hacer que el equipo deje de usar el TPM. Entonces, el TPM borrará permanentemente la clave raíz de almacenamiento y nadie que acceda posteriormente al dispositivo podrá recuperar los datos que estaban protegidos con esa clave.

## Instalación rápida y fácil

Empiece a proteger sus datos confidenciales de usuario inmediatamente: la instalación apenas requiere conocimientos técnicos. Solo tiene que conectar el accesorio TPM al formateador del dispositivo y encender el equipo. Tras la instalación, el TPM se empareja automáticamente con su impresora o equipo multifunción. A partir de entonces, el TPM protege automáticamente las claves, contraseñas y certificados de seguridad.

### Instalación

**1** Conecte el TPM

**2** Encienda el dispositivo

**3** Las claves, contraseñas y certificados están protegidos

# Especificaciones del producto

| | |
|---|---|
| **Número de pieza** | F5S62A |
| **Impresoras y equipos multifunción compatibles** | Equipos compatibles con la última actualización del firmware que usan HP FutureSmart 3.0:<br>**HP LaserJet:** M602, M603, M604, M605, M606, M712, M806<br>**HP LaserJet MFP:** M630, M830<br>**HP Color LaserJet:** M552, M553, M651, M855<br>**HP Color LaserJet MFP:** M680, M880<br>**HP OfficeJet:** X555<br>**HP OfficeJet MFP:** X585 |
| **Dimensiones** | 21,62 x 18,03 x 6,2 mm (0,85 x 0,71 x 0,24 pulg.) |
| **Peso** | 1,71 g (0,06 oz) |
| **Contenido del paquete** | HP Trusted Platform Module, guía de instalación |
| **Garantía** | Un año de garantía limitada en sus instalaciones |
| **Condiciones ambientales** | Temperatura recomendada: en funcionamiento: de 13 a 30 °C (de 56 a 86 °F); en almacenamiento: de 0 a 40 °C (de 32 a 104 °F)<br>Humedad: en funcionamiento: de 10 a 80% de humedad relativa; en almacenamiento: de 10 a 90% de humedad relativa |
| **Estándares y certificaciones** | Diseñado de acuerdo con el estándar TPM 1.2 del Trusted Computing Group[4] |

## Más información en
**hp.com/go/jetadvantage**

### Notas
[1] El uso del accesorio HP Trusted Platform Module puede requerir una actualización del firmware.
[2] El coste medio de una brecha en la seguridad de los datos es de 136 dólares por registro puesto en peligro y 5,4 millones de dólares en total. Fuente: Estudio sobre el coste de las brechas en la seguridad de los datos en 2013: un análisis global, Ponemon, mayo de 2013.
[3] HP no se responsabiliza del mantenimiento de las claves de recuperación. Se recomienda encarecidamente a los clientes que lleven a cabo los procedimientos aconsejados para hacer copias de seguridad de sus claves y datos.
[4] El Trusted Computing Group (TCG) es un grupo de estándares internacionales del sector que desarrolla especificaciones para sus miembros. El TCG publica las especificaciones para su implementación y uso en el sector.

## Regístrese y reciba las actualizaciones
**hp.com/go/getupdated**



4AA5-4782ESE , Abril de 2015