

# Protege tu impresora desde el arranque hasta el apagado



## Funciones de seguridad de la impresión integradas de HP Pro

La última generación de los dispositivos de impresión HP Pro ofrece tres tecnologías clave diseñadas para frustrar los ataques. Estas funciones de seguridad integradas se incluyen en los modelos HP OfficeJet Pro 8000/9000<sup>1</sup>, PageWide Pro de las series 400/500 y LaserJet Pro de las series M200 y M400/M500.

### Arranque seguro

El código de arranque de HP es un conjunto de instrucciones de arranque utilizadas para cargar los componentes principales de hardware e iniciar el firmware. Cuando se enciende la impresora, el arranque seguro trabaja en segundo plano para protegerla de los ataques. El arranque seguro valida la integridad del código de arranque en cada ciclo de arranque al garantizar que el código lo firma HP y es auténtico. Si el código se ha visto expuesto, el dispositivo se coloca en modo de recuperación con funcionalidad limitada hasta que se pueda reinstalar el código original de HP.

### Validación de la integridad del firmware

Al igual que el sistema operativo de un ordenador, el firmware coordina las funciones de hardware, ejecuta el panel de control, determina qué funciones se encuentran disponibles al imprimir, escanear o enviar un archivo por correo electrónico, y ofrece seguridad en la red. Un firmware afectado podría poner en peligro el dispositivo y la red frente a un ataque. Todas las actualizaciones de firmware se validan, de modo que solo se instale código auténtico y conocido en el dispositivo con la firma digital de HP. Durante el proceso de encendido del dispositivo, si no se puede validar la firma del código, el dispositivo se reinicia a un estado de recuperación seguro y queda a la espera de una actualización válida de firmware. La notificación de código de firmware no válido se muestra a través de un mensaje en el panel de control.

### Integridad del código en tiempo real

Esta función protege los dispositivos cuando están operativos y conectados a la red, momento en el que suelen producirse la mayoría de los ataques. La integridad del código en tiempo real evita que los intrusos introduzcan código malicioso mientras se ejecuta la impresora. Toda la memoria de código de tiempo de ejecución está protegida contra escritura y toda la memoria de datos se considera no ejecutable.

### Gestión de los ajustes de seguridad de la impresora

Los administradores de TI pueden utilizar HP JetAdvantage Security Manager para evaluar y, si es necesario, corregir los ajustes de seguridad de los dispositivos en toda la flota, con el fin de cumplir las políticas de seguridad corporativa establecidas previamente<sup>1</sup>.

Más información en: [hp.com/go/printersthatprotect](http://hp.com/go/printersthatprotect).

<sup>1</sup> HP JetAdvantage Security Manager debe adquirirse por separado. Para HP OfficeJet Pro, HP JetAdvantage Security Manager solo es compatible con las series 8730 y 8740 de HP OfficeJet Pro. Para obtener más información, visita [hp.com/go/securitymanager](http://hp.com/go/securitymanager).

## ¿Cómo funciona?

Las funciones de seguridad integradas abarcan tres pasos básicos en el ciclo de un dispositivo HP Pro.

HP JetAdvantage Security Manager completa el ciclo de comprobación.

### Verificación del código de arranque

#### Arranque seguro

Garantiza que, durante el encendido del dispositivo, solo se cargue un código de arranque original con la firma de HP. Si el código ha estado expuesto, el dispositivo entra en modo de recuperación.

### Comprobación de firmware

#### Validación de la integridad del firmware

Verifica que el firmware contiene código original de HP durante el encendido del dispositivo. Si se detecta una anomalía, el dispositivo se reinicia a un estado seguro conocido.

### Gestión de los ajustes de seguridad

#### HP JetAdvantage Security Manager

Verifica y corrige todos los ajustes de seguridad afectados de los dispositivos en toda la flota.

### Protección de la memoria

#### Integridad del código en tiempo real

Evita que los intrusos introduzcan código malicioso en la memoria durante el funcionamiento del dispositivo.

Suscríbete para recibir novedades  
[hp.com/go/getupdated](http://hp.com/go/getupdated)



Compartir con compañeros

© Copyright 2016–2017, 2019 HP Development Company, L.P. La información que contiene este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de HP quedan establecidas en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. Nada de lo aquí indicado debe interpretarse como una garantía adicional. HP no se responsabiliza de errores u omisiones técnicos o editoriales que puedan existir en este documento.

4AA6-4973ESE, octubre de 2019, rev. 4