# Más vale prevenir que lamentar.

## Consigue protección para todos los dispositivos en general con Lenovo.

Un portátil es robado cada minuto. De todos modos, esa no tendría que ser razón suficiente para impedir la movilidad de los trabajadores. Reduce los posibles riesgos con una **seguridad sólida de los dispositivos.**

## ¿Piensas que tu dispositivo es seguro? Piénsalo una vez más.

Cuando se trata de la seguridad de red, los dispositivos son más propensos a las amenazas.

Cada **53 segundos**, se roba un portátil.

**El 52 %** de los dispositivos se roban en la oficina.

**El 80 %** del coste de un portátil perdido corresponde a las filtraciones de datos.

## No hacer nada puede costarte caro

La pérdida de un dispositivo es dramática si se usa para acceder a datos confidenciales. No solo para el usuario, también para tu negocio.

- Noviembre de 2016: EMC y el Hospital Hartford pusieron una multa de 90 000 USD por el robo de un portátil que contenía datos de casi 9000 personas.
- Mediados de 2012: Cancer Care Group pagó 750 000 USD por el robo de un portátil que contenía información de identificación personal (PII) de 55 000 pacientes antiguos y actuales.
- 2006: Nationwide puso una multa de 980 000 £ por el robo de un portátil sin cifrar con datos personales de 11 millones de ahorradores.

# Enfoque de 360° de Lenovo en cuanto a la seguridad

## CONTROL DE ACCESO DE USUARIOS

Garantiza el acceso al PC solo al personal autorizado con las siguientes funciones:

### Autenticación multifactor

El reconocimiento de huellas dactilares biométrico de Lenovo garantiza la administración simplificada del acceso y también una seguridad sólida. Como líder de la autenticación multifactor, Lenovo también ofrece las siguientes características en sus dispositivos:

- **Tecnología de lector de huellas dactilares táctil Match-on-Chip (MoC FPR)**, que almacena las credenciales biométricas en un chip independiente, lo que imposibilita prácticamente cualquier ataque.
- Protege aún más la identidad y los datos con **Intel® Authenticate.**

### Acceso con tarjetas inteligentes

Almacenamiento seguro de información de inicio de sesión en tarjetas a prueba de alteraciones. Las contraseñas no son necesarias.

### Near Field Communication (NFC)

Una comunicación por radio como Bluetooth o Wi-Fi con una etiqueta, lo que imposibilita cualquier ataque al dispositivo.

### Cámara de infrarrojos con Windows Hello

Con Windows Hello, la cámara de infrarrojos opcional en dispositivos seleccionados simplifica y protege el proceso de inicio de sesión. La autenticación facial de Windows Hello usa una cámara configurada especialmente para que las imágenes casi de infrarrojos (IR) autentiquen y desbloqueen el dispositivo.

**Muestra tecnológica**
El lector de huellas dactilares Match-on-Chip (Moc FPR) de Lenovo es la tecnología de huellas dactilares más segura de los PC.

**Muestra tecnológica**
El obturador de cámara ThinkPad es una cubierta de cámara web física que los usuarios pueden abrir mientras atienden llamadas y cerrar si no se está utilizando.

## PROTECCIÓN FÍSICA Y DE PUERTO

Evita el robo de datos del puerto USB o de otros puertos de acceso en los PC de la empresa con estas características:

### Cámara con obturador

La cámara con obturador incorporado garantiza la privacidad.

### Candado de cable Kensington®

Estándar en todos los ordenadores Lenovo, el candado de cable Kensington® ayuda a reducir los robos permitiendo a los clientes gestionar el acceso de seguridad físico en las oficinas.

### Estación de acoplamiento ThinkPad Ultra Dock

Esta estación de acoplamiento ThinkPad Ultra Dock viene con un candado de seguridad que protege cómodamente el dispositivo y tu estación de acoplamiento al escritorio con una sola clave.

## PROTECCIÓN DE DATOS

Evita la pérdida y el robo de datos con las siguientes características:

### Mejor gestión y control

Experimenta la integración de Pro SSD con Intel® Remote Secure Erase de la tecnología Intel® (Intel® AMT) de gestión activa.

### Fast Identity Online (FIDO)

La autenticación FIDO atañe a los datos de acceso en línea cuando los usuarios inician sesión en sitios web internos y externos o realizan pagos en línea.

### Módulo de plataforma segura independiente (dTPM)

El chip dTPM 2.0 integrado en dispositivos ThinkPad habilita y almacena claves de cifrado RSA únicas específicas del sistema host para la autenticación de hardware.

### Administración de dispositivos móviles integrada

La asistencia de Administración de dispositivos móviles (MDM) de Windows 10 te permite usar servicios de gestión basados en la nube* para controlar los dispositivos empresariales y personales.

**Muestra tecnológica**
El chip dTPM 2.0 cifra los datos de usuario del PC.


*Se vende por separado

Fuente:
https://www.pcworld.com/article/3021316/security/why-stolen-laptops-still-cause-data-breaches-and-whats-being-done-to-stop-them.html
https://www.digicert.com/blog/45-percent-healthcare-breaches-occur-on-laptops/
https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

**Lenovo garantiza de forma permanente la seguridad de tus dispositivos y datos.**

Para más información, visita www.lenovo.com

Lenovo

Procesadores Intel® Core™