# TPM (Secure Boot): Algunas ventajas, desventajas y ¿Por qué es tan problemático?

Morales Zilli Luis Fernando & Magno García Omar

## Introducción

La seguridad es una de las principales preocupaciones en el mundo de la tecnología. Con el aumento de los ataques cibernéticos y las brechas de seguridad, es cada vez más importante asegurar la información y los datos almacenados en nuestros dispositivos electrónicos. Los TPMs (Trusted Platform Modules) se han convertido en una herramienta esencial para proteger la información en nuestras computadoras. Los TPMs son chips de seguridad que proporcionan una plataforma de confianza en la computadora, permitiendo el almacenamiento seguro de información y la realización de operaciones criptográficas seguras. A lo largo de este documento explicaremos en detalle cómo funcionan los TPMs, sus características, su importancia para la seguridad de la información.

## Exactamente, ¿Qué es el TMP?

Entendamos primeramente que el TPM es principalmente un chip, no es Software ni un programa inscrito en la UEFI. TPM es un acrónimo de *"Trusted Platform Module"* Lo que se traduce como módulo de plataforma de confianza, No se trata más de un criptoprocesador (Un procesado enfocado en realizar operaciones criptográficas), su objetivo obviamente es el cifrado, ¿Pero qué cifra exactamente?

Este chip cifra tanto claves de Windows, como archivos personales que tengas en tu PC con TPM activado.

Quizá como usuario final sea bueno para proteger nuestros archivos importantes, pero el chip está enfocado en el ámbito laboral y profesional, gente que maneja cantidades industriales de información delicada de gente, como bancos, hospitales, gerencias, entre otras.

Dato curioso: El sistema TPM fue creado en 2003, pero se hizo un estándar hasta su versión 2.0, gracias a la norma ISO/IEC 11889.

## ¿Cómo funciona TPM?

Cuando se enciende una PC, sabemos que entran varios dispositivos y software encienden también, entre los muchos se encuentra este chip, lo que hace este chip es revisar la integridad de tu PC, TPM toma como una PC "Confiable" Si esta no ha sido manipulada de alguna de estas formas:

- El Almacenamiento de la PC se ha colocado en otra computadora.
- El ordenador se ha encendido y una entidad remota tiene el control del equipo (De manera no autorizada)
- El equipo tiene algún tipo de malware detectado
- Si se está usando un ataque de fuerza bruta para acceder a estos archivos.

Si el TPM detecta alguna de estas situaciones, mandará una señal para que la PC no arranque, haciendo que no sea posible acceder a los datos dentro de la computadora.

Si pensabas que solo quitando o desactivando de alguna forma se puede vulnerar, los códigos de cifrado se guardan en el almacenamiento de la PC, como en el microprocesador, el cual este está programado para nunca liberar su parte de cifrado, por lo que hará que sin el chip, el equipo tampoco arrancará.

También su seguridad radica en que la comunicación solamente es entre el procesador y el chip mismo, ningún componente externo debe tener acceso, por lo que un virus la tendrá más difícil para poder acceder a tus archivos.

## ¿Y si es tan bueno?, ¿Por qué tiene tanta polémica este chip?

Si bien, las ventajas que se observan son bastante beneficiosas, (Además de que este chip no es nuevo, ya que desde 2016 se les han pedido a las marcas

de cómputo que implementen este chip) el epicentro de una serie de quejas y dudas radica en Windows 11, aunque, no es la única razón, es una de las más sonadas. Algunas cuestiones que hace que esto no sea tan beneficioso se enfocan en 2 problemas principales:

## Primer Problema: Obligatoriedad en Windows 11

El 5 de octubre de 2021 salió al mercado una nueva versión de Windows, que más que traernos beneficios, lo que nos otorgó en sus inicios fue incompatibilidades y bugs, pero en esta ocasión nos enfocaremos en un problema que viene desde los requisitos.

Cuando se mostró a público los requisitos mínimos para poder ejecutar Windows 11, resaltó inmediatamente un componente: TPM en su versión 2.0

¿Recuerdan que mencionamos que empezaron a implementar TPM en 2016? Pues resulta que en ese entonces no todos implementaron este chip, y los que lo hicieron, resulta que venía de forma desactivada en el equipo, de tal forma que al intentar revisar si cumplias los requisitos, vieras la terrible noticia de que tu PC no era compatible con el nuevo sistema operativo de Microsoft.

Aquí el problema radica en que no solo las computadoras del 2015 o antes, no pudieron actualizar al nuevo sistema por falta del chip, y los que tienen el chip, no pueden usarlo porque las empresas decidieron desactivar el chip de fábrica.

“Hey ¿Pero quién tiene PCs de hace más de 5 años?” Tenemos que entender que mucha gente en México es un país en vías de desarrollo, por lo que no pueden costearse una PC actual, así que siguen usando PCs más antiguas. De hecho, el promedio de uso de una Computadora es alrededor de 3 a 5 años, por lo que no es loco pensar que aún exista gente con equipo del 2016 o de años anteriores.

Si bien esto solo es una parte de esta problemática, la otra es que las computadoras que si tienen el chip integrado en las placas madres no lo

tienen activado, ¿Cómo podemos activar el TPM? Simple, debes entrar a la UEFI del sistema.
Tenebroso, ¿No? Siempre decimos que no debemos entrar al UEFI del sistema porque el más mínimo cambio puede corromper todo. Es importante tener precaución al entrar en la UEFI de una PC. Si no se tiene experiencia en el tema, es mejor no hacer cambios en la configuración, si para muchos programadores y técnicos es complicado hacer modificaciones desde la UEFI, el usuario final realmente no toca ese espacio del sistema, por lo que la última opción para disfrutar del nuevo sistema de Microsoft es comprando otra PC (Hablando de un usuario final).

## Segundo problema: TPM no es "Invulnerable" como lo pintan

Anteriormente habíamos mencionado que TPM era un cifrado seguro para todos tus archivos, la realidad es que no todo en el mundo de la informática es 100% invulnerable, y como podrás imaginar, TPM tampoco se salva.
Comenzando con 2 vulnerabilidades muy peligrosas (No resueltas al momento de hacer esta investigación). Están etiquetadas como errores de escritura fuera de los límites y lectura fuera de los límites respectivamente. La vulnerabilidad afecta a la biblioteca de módulos TPM 2.0, lo que permite que los comandos maliciosos explotan estas vulnerabilidades y dejen inutilizable el módulo TPM 2.0. Además, esto permite la ejecución de código arbitrario dentro de la memoria protegida de TPM 2.0 y el acceso a datos confidenciales almacenados en el criptoprocesador que debería estar aislado.
Otro problema radica en que: ¿Y si fuera posible pasar de largo el arranque seguro para iniciar Windows 11?
La respuesta la tiene BlackLotus: un malware UEFI que se vende como kit en foros de hacking por 5.000 dólares y que destaca por ser el primero conocido con capacidad para omitir el arranque seguro de Windows. El malware es

capaz de eludir las defensas de seguridad incluso cuando estén habilitadas en las BIOS/UEFI.

La pregunta es: ¿Por qué tanta insistencia en tener este chip como obligatorio si es vulnerable?

Dato extra: También TPM ocasiona problemas en el juego de Riot Games: Valorant, con su sistema anticheat Vanguard, haciendo obligatorio activar el chip, otra vez, para activarlo debemos adentrarnos al UEFI.

## ¿Esto no huele como a…Estrategia de Microsoft?

Dejando de lado los problemas de vulnerabilidad, el hecho de hacer que el paso de Windows 10 a Windows 11 sea muy complicado, ¿No será una maña de Microsoft para generar más ganancias?

No es de sorprenderse que Microsoft haya hecho muchas cosas bien, pero como empresa, sus actos al borde del Monopolio son bastante sucias en muchas ocasiones., no olvidemos las tácticas de los 80s y 90s que usaba para que el usuario usará sus propios programa y no de las competencia, y si no podía ganarle a la competencia, compraba la competencia.

También recuerda, Las PCs vienen con Windows, no porque sea el mejor, sino porque Microsoft tiene tantos convenios con tantas marcas de cómputo que es raro no encontrar una con Windows.

Con este historial, no sería sorprendente que Microsoft aumentará los requisitos de su sistema operativo, para que muchas PCs quedarán "obsoletas", y las pocas que quedaran, fueran difíciles de actualizar, obligando al usuario común a comprar una nueva PC para seguir al corriente en el mundo de tecnología.

Uno podría pensar que esta medida podría traer muchas consecuencias, bajas ventas y quizá una crisis en una época donde la pandemia seguía vigente.

Y contra todo pronóstico, funcionó. Según un artículo de DPL News, en 2021 se vendieron un total de 341 millones de computadoras de escritorio,

portátiles y estaciones de trabajo en todo el mundo, lo que representa un 14.6% más que en 2020 y la cifra más alta desde 2012.

Dato curioso: Un insider de Microsoft menciona que hay archivos en el código del sistema que indicarían que Windows 10 también requerirá TPM activado para seguir recibiendo actualizaciones.

## Finalmente… Conclusiones

Muchas veces los temas de ciberseguridad son muy importantes en estos tiempos donde casi toda nuestra información está en algunos bytes y megas de información.

Siempre hay que agradecer que mientras mejor se puedan proteger y respaldar nuestros datos será un alivio, pero, esta seguridad no debe estar condicionada a procesos complejos o compra de equipo nuevo que en la gran parte de las veces no es necesario, en un mundo donde el usuario final, por desgracia, no posee el conocimiento suficiente de informática para realizar cambios. El uso del TPM y Secure Boot ha sido problemático para algunos usuarios y organizaciones debido a que limita la capacidad de los usuarios para personalizar y modificar el software y el hardware de sus dispositivos. A pesar de estos problemas, muchos fabricantes y proveedores de servicios siguen implementando TPM y Secure Boot como medidas de seguridad esenciales para proteger sus sistemas y dispositivos contra amenazas de seguridad.

Como comentario final, la ciberseguridad debe adaptarse a las necesidades y expectativas de los usuarios, evitando soluciones complejas o inseguras que afecten a su confianza o comodidad.

Fuentes.


- Fernández, Y. (2022, 16 mayo). Qué es el TPM y cómo comprobar si tu ordenador lo tiene para poder instalar Windows 11. Xataka. https://www.xataka.com/basics/que-tpm-como-comprobar-tu-ordenador-tiene-para-poder-instalar-windows-11
- Larocca, N. (2022, 4 febrero). #DigitalMetrics | Se vendieron 341 millones de computadoras en 2021, la cifra más alta desde 2012. DPL News. https://dplnews.com/se-vendieron-341-millones-de-computadoras-en-2021-en-el-mundo-la-cifra-mas-alta-desde-2012/
- OpenSystems Media. (s. f.). What is Trusted Platform Module? Embedded Computing Design. https://embeddedcomputing.com/technology/security/what-is-trusted-platform-module-2
- Pardo, L. (2021, 13 octubre). ¿Por qué es necesario usar TPM 2.0 y Secure Boot en Windows 11? https://www.neoteo.com/por-que-es-necesario-usar-tpm-2-0-y-secure-boot-en-windows-11/
- Ranchal, J. (2023, 2 marzo). BlackLotus, primer malware UEFI capaz de omitir el arranque seguro de Windows. MuyComputer. https://www.muycomputer.com/2023/03/02/blacklotus-primer-malware-uefi-capaz-de-omitir-el-arranque-seguro-de-windows/
- Statista. (2022, 1 febrero). PCs (mobile & desktop) average age 2017-2022. https://www.statista.com/statistics/267474/average-life-of-pc-and-tablets/
- The Wild Project. (2021, 19 noviembre). Programador informático cuenta por qué NO debemos actualizar nuestro ordenador a WINDOWS 11. YouTube. https://www.youtube.com/watch?v=V1ht9JT-B3M
- Torres, I. R. (2023, 7 marzo). TPM 2.0 tiene dos importantes vulnerabilidades. Profesional Review. https://www.profesionalreview.com/2023/03/07/tpm-2-0-dos-vulnerabilidades/
- What is a Trusted Platform Module? TPM Computer Definition | Teguar. (2022, 10 mayo). Teguar Computers. https://teguar.com/what-is-a-tpm-computer-chip/
- W. (2023, 25 febrero). Módulo de plataforma de confianza (TPM) 2.0. Microsoft Learn. https://learn.microsoft.com/es-es/windows-hardware/design/device-experiences/oem-tpm