centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1605

Guía de configuración y empleo seguro de la tableta GETAC F110G4

Abril 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.04.22 09:43:15 +02'00'

NIPO: 083-19-165-X

Fecha de Edición: abril de 2019

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Abril de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

La tableta GETAC modelo F110G4 y firmware GETAC R1.12.070520, es un dispositivo móvil de tipo tableta robusta diseñado para dar soporte a usuarios civiles y militares y cuyo objetivo principal es su utilización como plataforma confiable para ejecución de aplicaciones software.

Las especificaciones del hardware son las siguientes:

Elemento		*Especificación*
CPU		Kaby Lake U Platform - Intel® Core™ i7-7500U Processor, 2.7GHz up to 3.5GHz, 4M cache
Firmware		Insyde, Flash EEPROM, supporting UEFI, NIST, ACPI, TPM, Computrace, AMT11, WMI, BIOS diagnostic
RAM		8 GB DDR4 SO-DIMM
Video	Controller	UMA - Intel® HD Graphics 620
	Display Panel	11.6-inch (16:9) TFT LCD, HD 1366x768, dimmer mode, blackout mode, sunlight readable, 800 Nits maximum brightness
Touchscreen		Capacitive multi-touch screen - 10 point
Audio	Features	Azalia, High Definition audio
	Speaker	1.5W x 1
	Microphone	Integrated microphone
Hard disk drive		128GB SSD
I/O ports	Standard	USB 3.0, combo audio (4-pole TRRS 3.5mm type), HDMI, Docking
	Optional	Top side: RS232
		Rear: None
LAN (option)		10/100/1000 Mbps Ethernet
Wireless LAN + BT		IEEE 802.11ac, compatible with 802.11a/b/g/n, BT 4.2 + EDR
GPS		GPS: Locosys GPS/GLONASS: GlobalSat
Camera		Front: FHD, IR sensor. Rear: 8M pixel, autofocus, LED, video capture
Security		Kensington lock TPM 2.0
Power	AC adapter	Universal 65 W; input: 100~240 V, 50/60 Hz; output: 19V
	Battery pack x 2	Lithium-ion Prismatic type, 3-cell
Dimension (LxW×D)		314 x 207 x 18mm (12.4 × 8.1 × 0.7 inch)
Weight		1.39 kg (3 lb)

Tabla 1. Especificaciones del hardware de la GETAC F110G4.

El sistema operativo de la tableta es Windows 10 Enterprise 1607 LTSB.

Los datos almacenados en el dispositivo están protegidos mediante el cifrado de disco, utilizando la propia herramienta que proporciona el sistema operativo, BitLocker.

El dispositivo ofrece un arranque seguro mediante la tecnología *Secure Boot* del firmware UEFI.

2. OBJETO Y ALCANCE

El objeto del presente documento es definir dos manuales para el dispositivo GETAC F110G4:

- Un manual de configuración segura, sección 3, el cual describe las actividades a llevar a cabo por el usuario administrador para realizar una configuración segura de la tableta.
- Un manual de empleo seguro, sección 4, en el que se definen las actividades que permiten realizar un empleo seguro de la tableta para los usuarios administradores y usuarios estándar.

Por último, se incluyen las referencias, acrónimos, e índices de figuras y tablas utilizados en la redacción del documento.

3. MANUAL DE CONFIGURACIÓN SEGURA

Esta sección describe las actividades a llevar a cabo para realizar una configuración segura de la tableta GETAC F110G4. Dichas actividades deben realizarse en el orden establecido para asegurar un correcto funcionamiento del producto.

Los drivers, firmware y sistema operativo de la tableta durante la realización de esta guía se encuentran actualizados a fecha de enero de 2019.

Las actividades descritas en esta sección son realizadas únicamente por el usuario administrador. Además, todos los comandos mostrados en esta sección deben ejecutarse desde una consola PowerShell con privilegios de administrador.

3.1 ACTIVIDAD I: CONFIGURACIÓN DEL FIRMWARE UEFI

Para empezar, con el sistema operativo iniciado, abrimos una consola con privilegios de administrador y accedemos a la configuración del firmware UEFI mediante el comando *shutdown /r /o*.

Tras esto, se iniciará la pantalla de recuperación de Windows, desde la que seleccionaremos la opción *Solucionar problemas - Configuración de firmware UEFI – Reiniciar* con el fin de acceder a la configuración de UEFI.

Una vez dentro de la configuración de UEFI, accedemos a *Setup Utility* y seleccionamos la opción *Setup Defaults* para cargar los parámetros por defecto de UEFI.

A continuación, configuramos UEFI teniendo en cuenta los siguientes parámetros:

a. En la pestaña **Advanced**

   - Desactivamos el parámetro *Screen Tapping for Boot Options*.

b. En la pestaña **Security**: realizamos la siguiente configuración en el orden establecido a continuación:

   - Establecemos la contraseña de administrador mediante el parámetro *Set Supervisor Password.*

     Nota: es necesario establecer la contraseña de administrador para desbloquear el resto de parámetros configurados en esta pestaña, como por ejemplo la política de contraseña, el arranque seguro, etc.

   - Activamos la opción *Strong Password* para fortalecer la política de contraseña.

   - Establecemos la longitud mínima de la contraseña en **12 caracteres**[1] según el parámetro *Password Configuration*.

[1] El número de caracteres se ha definido de acuerdo a la versión vigente de la guía CCN-STIC-301 para el nivel de clasificación CONFIDENCIAL.

- Activamos el inicio seguro mediante el parámetro *Secure Boot Configuration* → *Secure Boot*.

c. En la pestaña **Boot**: desactivamos todos los elementos del inicio excepto *Hard Disk Drive*.

Una vez se han configurado los parámetros descritos anteriormente, seleccionamos la opción *Save and exit* para guardar los cambios y salir de la configuración de UEFI.

Para finalizar, volvemos a acceder a la configuración de UEFI siguiendo el mismo procedimiento descrito en el inicio de esta sección y configuramos, desde la pestaña **Security,** los parámetros *Set Supervisor Password* y *Set User Password* para asegurar el establecimiento de una contraseña fuerte en ambos roles.

3.2 ACTIVIDAD II: DESINSTALACIÓN DE APLICACIONES

Para empezar, accedemos a Panel de Control → Programas y procedemos a desinstalar las siguientes aplicaciones instaladas de serie por el fabricante:

- Adobe Acrobat Reader DC
- AverMedia CO331GT USB HD Capture Device.
- Getac Utility
- McAfee Agent
- McAfee VirusScan Enterprise
- Microsoft Office Standard 2013.
- Tecnología de almacenamiento Intel Rapid.
- Windows Driver Package - HID Global (hidglobal_cdeem).
- Winrar 4.20.

Es posible que algunas de estas aplicaciones no vengan preinstaladas en la tableta. Por ello, se ignorarán aquellas que no aparezcan listadas en la aplicación *Programas* de Windows.

A continuación, se muestran unas capturas del proceso.

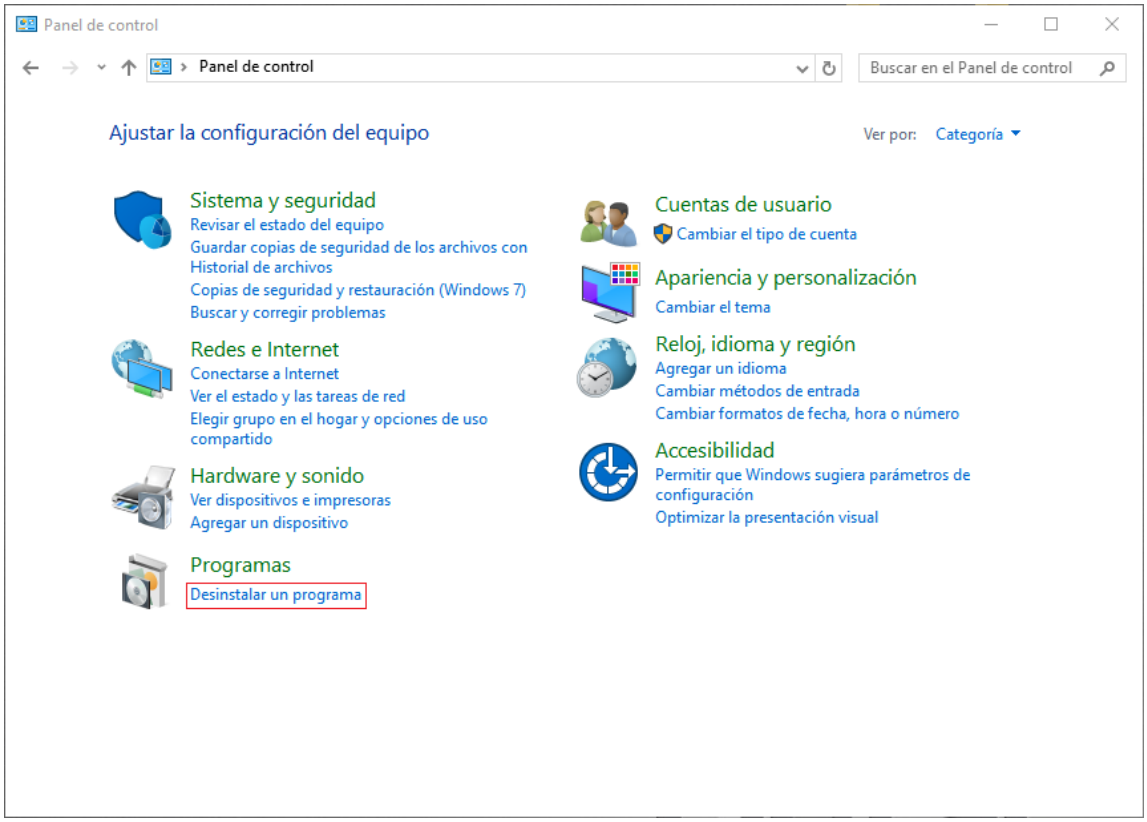
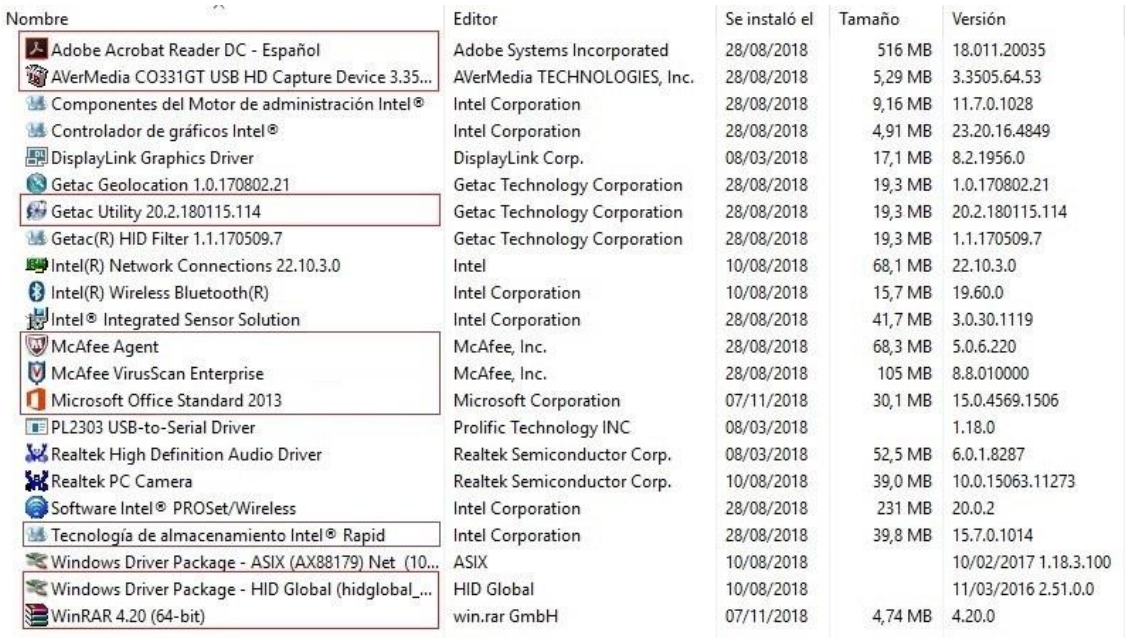


Figura 1: Desinstalar aplicaciones predeterminadas - 1.



Nombre	Editor	Se instaló el	Tamaño	Versión
Adobe Acrobat Reader DC - Español	Adobe Systems Incorporated	28/08/2018	516 MB	18.011.20035
AVerMedia CO331GT USB HD Capture Device 3.35...	AVerMedia TECHNOLOGIES, Inc.	28/08/2018	5,29 MB	3.3505.64.53
Componentes del Motor de administración Intel®	Intel Corporation	28/08/2018	9,16 MB	11.7.0.1028
Controlador de gráficos Intel®	Intel Corporation	28/08/2018	4,91 MB	23.20.16.4849
DisplayLink Graphics Driver	DisplayLink Corp.	08/03/2018	17,1 MB	8.2.1956.0
Getac Geolocation 1.0.170802.21	Getac Technology Corporation	28/08/2018	19,3 MB	1.0.170802.21
Getac Utility 20.2.180115.114	Getac Technology Corporation	28/08/2018	19,3 MB	20.2.180115.114
Getac(R) HID Filter 1.1.170509.7	Getac Technology Corporation	28/08/2018	19,3 MB	1.1.170509.7
Intel(R) Network Connections 22.10.3.0	Intel	10/08/2018	68,1 MB	22.10.3.0
Intel(R) Wireless Bluetooth(R)	Intel Corporation	10/08/2018	15,7 MB	19.60.0
Intel® Integrated Sensor Solution	Intel Corporation	28/08/2018	41,7 MB	3.0.30.1119
McAfee Agent	McAfee, Inc.	28/08/2018	68,3 MB	5.0.6.220
McAfee VirusScan Enterprise	McAfee, Inc.	28/08/2018	105 MB	8.8.010000
Microsoft Office Standard 2013	Microsoft Corporation	07/11/2018	30,1 MB	15.0.4569.1506
PL2303 USB-to-Serial Driver	Prolific Technology INC	08/03/2018		1.18.0
Realtek High Definition Audio Driver	Realtek Semiconductor Corp.	08/03/2018	52,5 MB	6.0.1.8287
Realtek PC Camera	Realtek Semiconductor Corp.	10/08/2018	39,0 MB	10.0.15063.11273
Software Intel® PROSet/Wireless	Intel Corporation	28/08/2018	231 MB	20.0.2
Tecnología de almacenamiento Intel® Rapid	Intel Corporation	28/08/2018	39,8 MB	15.7.0.1014
Windows Driver Package - ASIX (AX88179) Net (10...	ASIX	10/08/2018		10/02/2017 1.18.3.100
Windows Driver Package - HID Global (hidglobal_...	HID Global	10/08/2018		11/03/2016 2.51.0.0
WinRAR 4.20 (64-bit)	win.rar GmbH	07/11/2018	4,74 MB	4.20.0

Figura 2: Desinstalar aplicaciones predeterminadas - 2.

3.3 ACTIVIDAD III: APLICACIÓN DE LA GUÍA CCN-STIC-599B

Se debe aplicar la guía [CCN-STIC-599B] a nivel CONFIDENCIAL, teniendo en cuenta las cuestiones siguientes que permitirán mantener la funcionalidad y conectividad requeridas en la tableta:

1. Durante la realización del paso 57 de la guía, con el editor de plantillas de seguridad abierto, se debe modificar la plantilla de seguridad **CCN-STIC-599B18 Servicios** con el fin de habilitar en modo *Automático* los siguientes servicios:

    a) Audio de Windows.

    b) Compilador de extremo de audio de Windows.

    c) Conexiones de red.

    d) Configuración automática de WLAN.

    e) Energía.

    f) Identidad de aplicación.

    g) Servicio de compatibilidad con Bluetooth.

    h) Servicio de configuración de red.

    i) Servicio de geolocalización.

    j) Servicio de Panel de escritura a mano y teclado táctil.

    k) Servicio de sensores.

    l) Servicio de supervisión de sensores.

    m) Servicio de Windows Defender[2].

2. Después de realizar el paso 62 de la guía se deben modificar las siguientes directivas de la política de grupo (para acceder al editor de políticas de grupo se hará uso del comando *gpedit.msc*):

    a) Configuración de **Equipo** → Plantillas Administrativas → Componentes de Windows → Cámara → Permitir el uso de la cámara (habilitada).

    b) Configuración de **Equipo** → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación → Permitir que las aplicaciones de Windows accedan a la cámara (habilitada → El usuario tiene el control).

    c) Configuración de **Equipo** → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación → Permitir que las aplicaciones de Windows accedan al micrófono (habilitada → El usuario tiene el control).

[2] Habilitar en el caso de que el software antivirus que vaya a usarse sea Windows Defender.

d) Configuración de **Equipo** → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación → Permitir que las aplicaciones de Windows accedan a la ubicación (habilitada → El usuario tiene el control)

e) Configuración de **Equipo** → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores → Desactivar sensores (deshabilitada).

f) Configuración de **Equipo** → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores → Desactivar ubicación (deshabilitada).

g) Configuración de **Equipo** → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores → Servicio de localización de Windows → Desactivar el servicio de localización de Windows (deshabilitada).

h) Configuración de **Usuario** → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores → Desactivar sensores (deshabilitada).

i) Configuración de **Usuario** → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores → Desactivar ubicación (deshabilitada).

3. Cuando se aplique la guía STIC al completo y se reinicie la tableta, Windows pedirá al usuario utilizar la combinación de teclas CTRL+ALT+SUPR para ingresar unas credenciales. Para realizar dicha combinación de teclas en la tableta, que no tiene teclado, se mantendrá pulsado el botón **P1**.

3.4 ACTIVIDAD IV: CIFRADO DEL ALMACENAMIENTO INTERNO

Se seguirán los pasos descritos en la sección *ANEXO B.3.1 CIFRADO DE DISCO CON BITLOCKER* de la guía [CCN-STIC-599B], teniendo en cuenta que, durante la realización del **paso 19,** se cambiará la longitud mínima del PIN de 8 a **12 caracteres**[3] en el parámetro *Configurar longitud mínima de PIN para el inicio*.

3.5 ACTIVIDAD V: INSTALACIÓN GPS Y SENSORES

Debido a la configuración aplicada por la guía STIC, los sensores y el GPS de la tableta quedan bloqueados por la política de grupo de Windows. Por ello, para desbloquear y asegurar el correcto funcionamiento de estos elementos se seguirán los pasos descritos a continuación:

[3] El número de caracteres se ha definido de acuerdo a la versión vigente de la guía CCN-STIC-301 para el nivel de clasificación CONFIDENCIAL.

1. Accedemos al *Administrador de dispositivos* desde el panel de control de Windows y copiamos los ID de hardware de las propiedades de cada elemento contenido en el apartado *Sensores*.

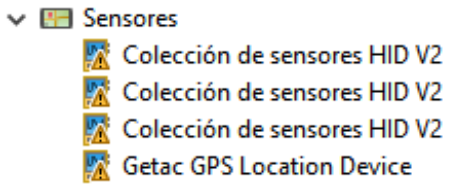


Figura 3: Administrador de dispositivos - Sensores y GPS.

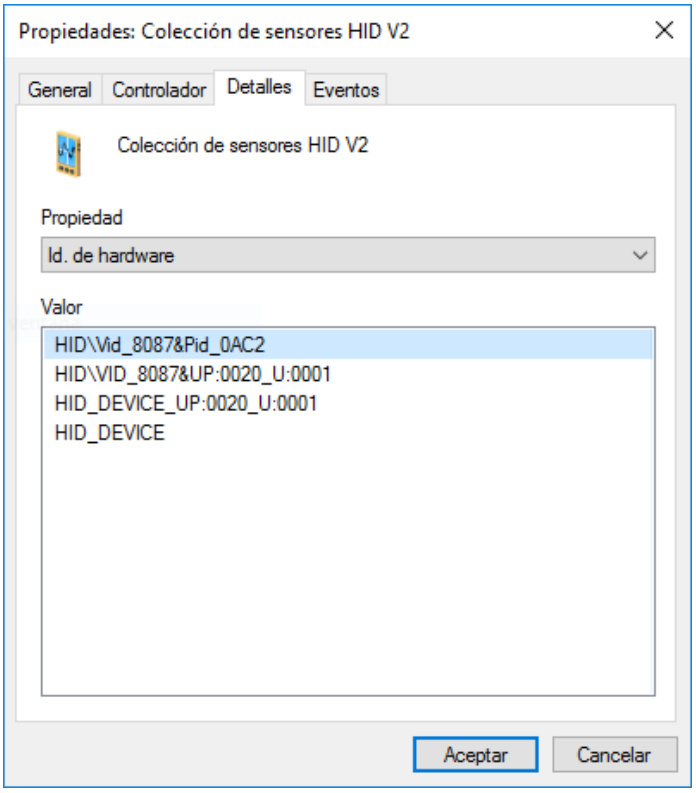


Figura 4: Id. de hardware del elemento.

2. Abrimos el editor de la política de grupo de Windows mediante el comando *gpedit.msc* y añadimos los ID de hardware de cada elemento identificado en el paso anterior, según el parámetro *Configuración de Equipo → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos → Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo*.

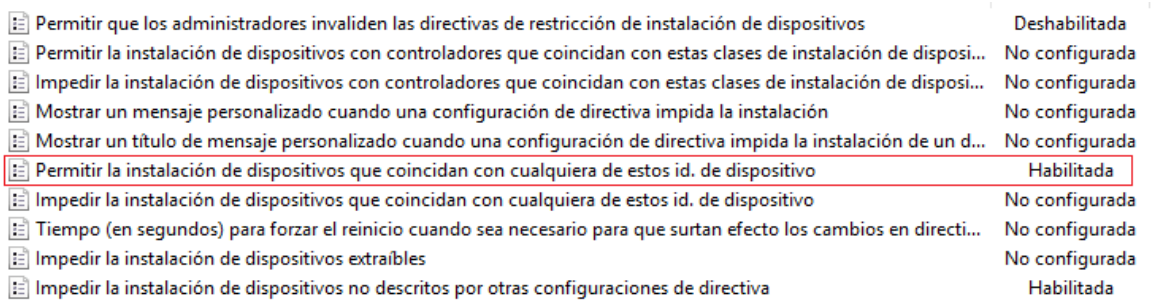


Figura 5: Habilitando dispositivos en la política de grupo - 1.

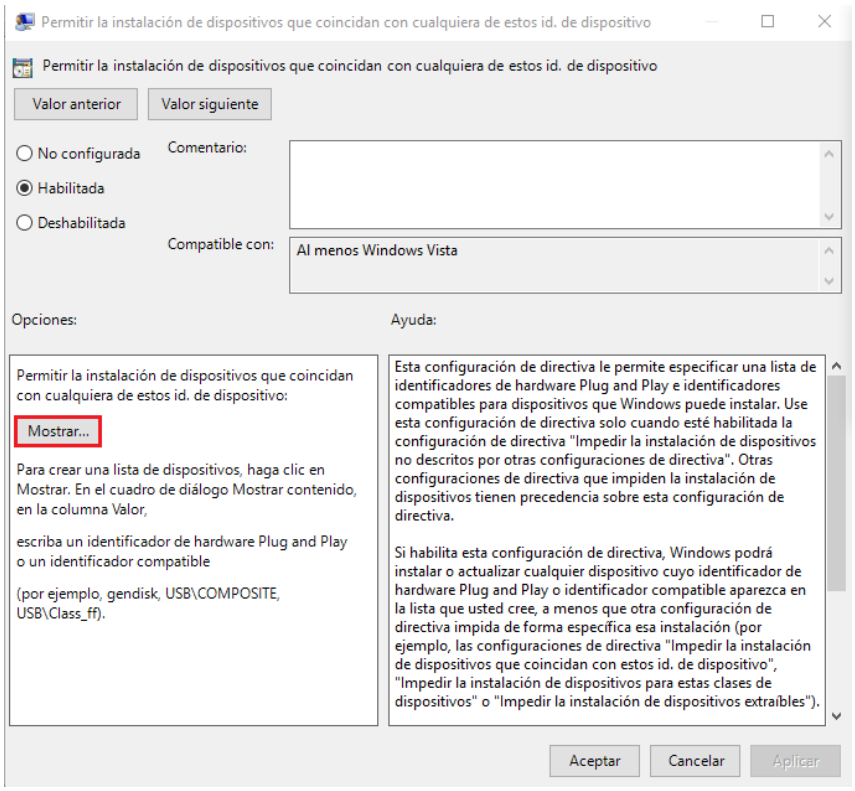


Figura 6: Habilitando dispositivos en la política de grupo - 2.

El listado de IDs mostrado en la figura a continuación puede variar según la versión del componente hardware de la tableta.

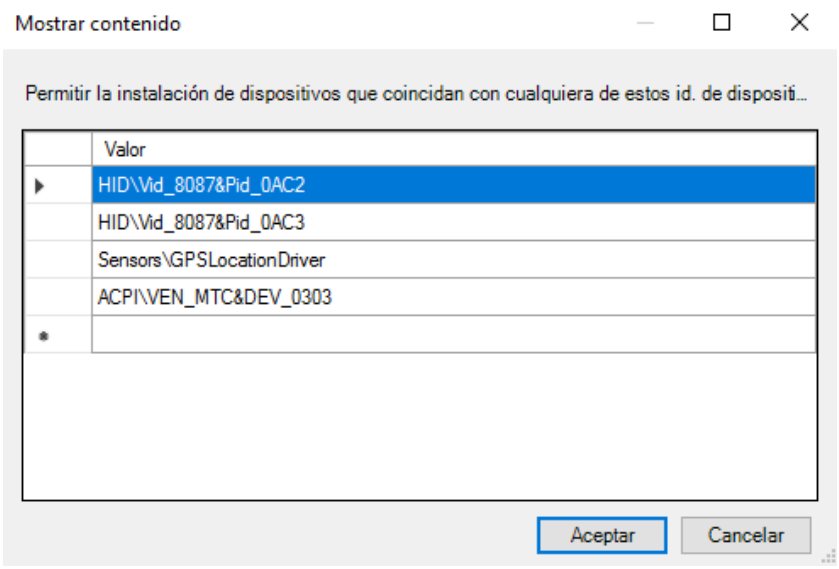


Figura 7: Habilitando dispositivos en la política de grupo - 3.

3. Desinstalamos cada uno de los dispositivos desde el administrador de dispositivos.

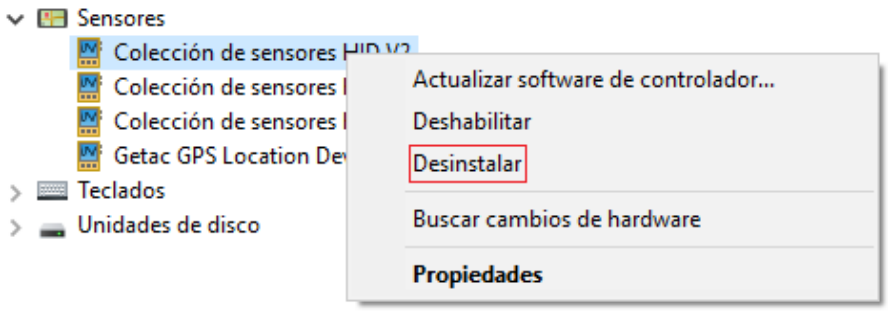


Figura 8: Desinstalando dispositivos.

4. Instalamos el driver *Getac Geolocation*.

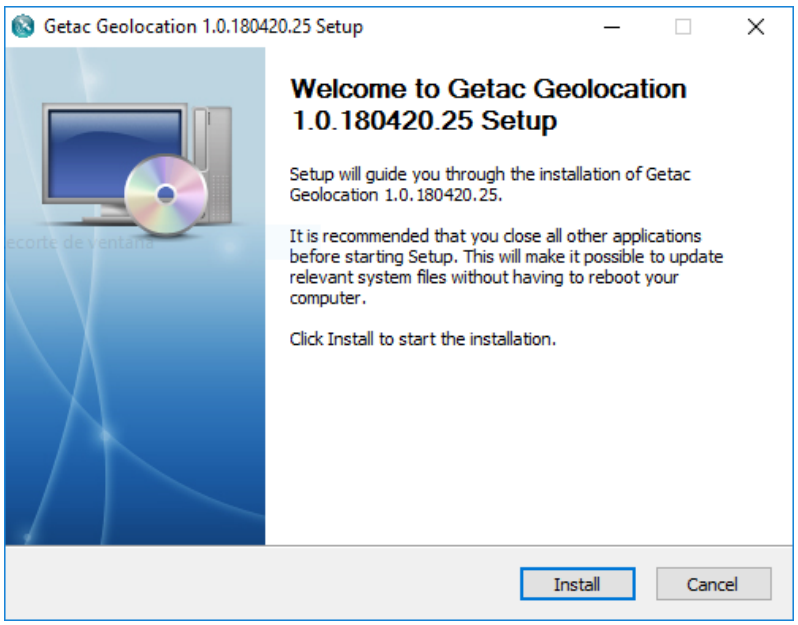


Figura 9: Instalando driver *Getac Geolocation*.

5. Actualizamos el administrador de dispositivos mediante la opción *Buscar cambios de hardware*, comprobando que el driver está correctamente instalado.

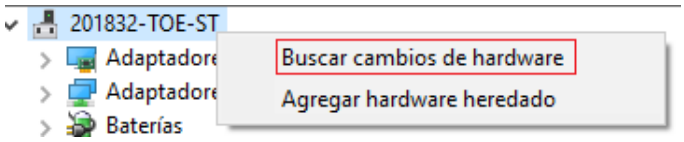


Figura 10: Buscando cambios de hardware.

3.6 ACTIVIDAD VI: ACTIVACIÓN DE LA UBICACIÓN

Para permitir a los usuarios estándar activar/desactivar la ubicación a petición, se debe habilitar antes esta funcionalidad desde la aplicación *Configuración* de Windows, tal y como se describe en los siguientes pasos:

1. Abrimos la aplicación *Configuración* desde la barra de tareas y hacemos clic en *Privacidad*.

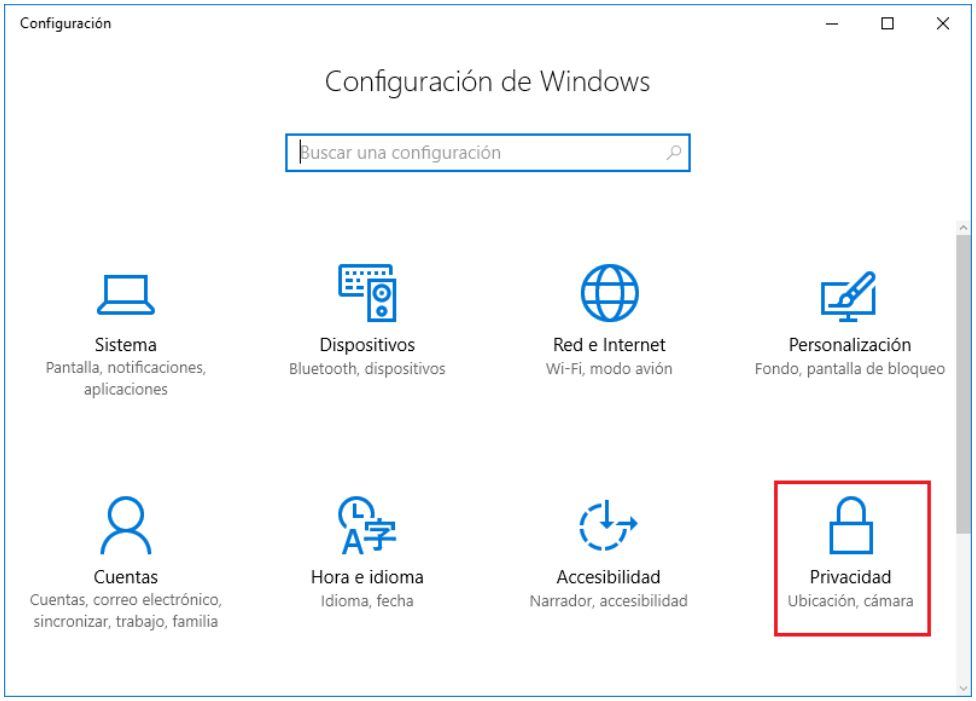


Figura 11: Activando ubicación - 1.

2. Nos dirigimos al apartado *Ubicación* y hacemos clic en *Cambiar*.

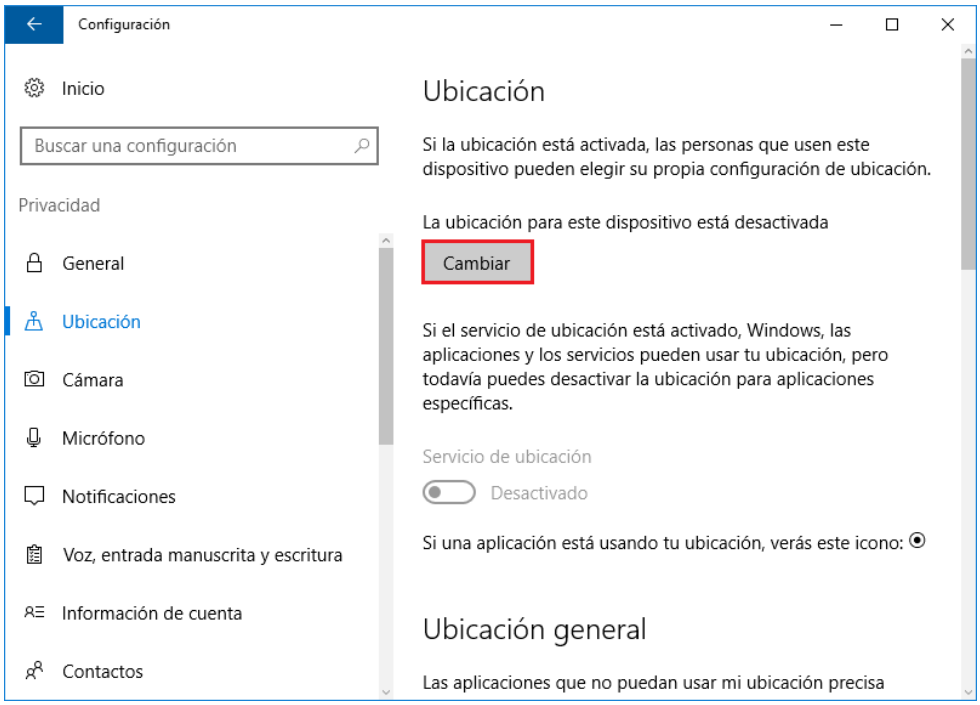


Figura 12: Activando ubicación - 2.

3. Activamos la ubicación haciendo clic en el *switch* que dice *Desactivado*.

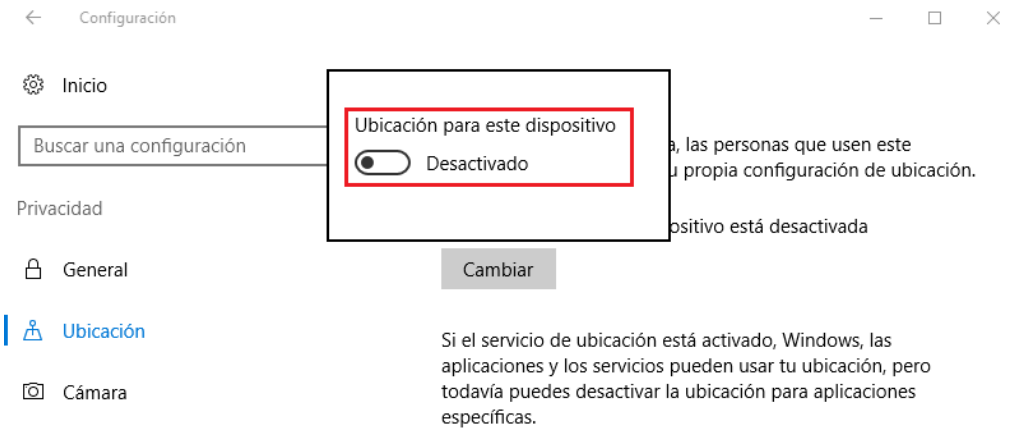


Figura 13: Activando ubicación - 3.

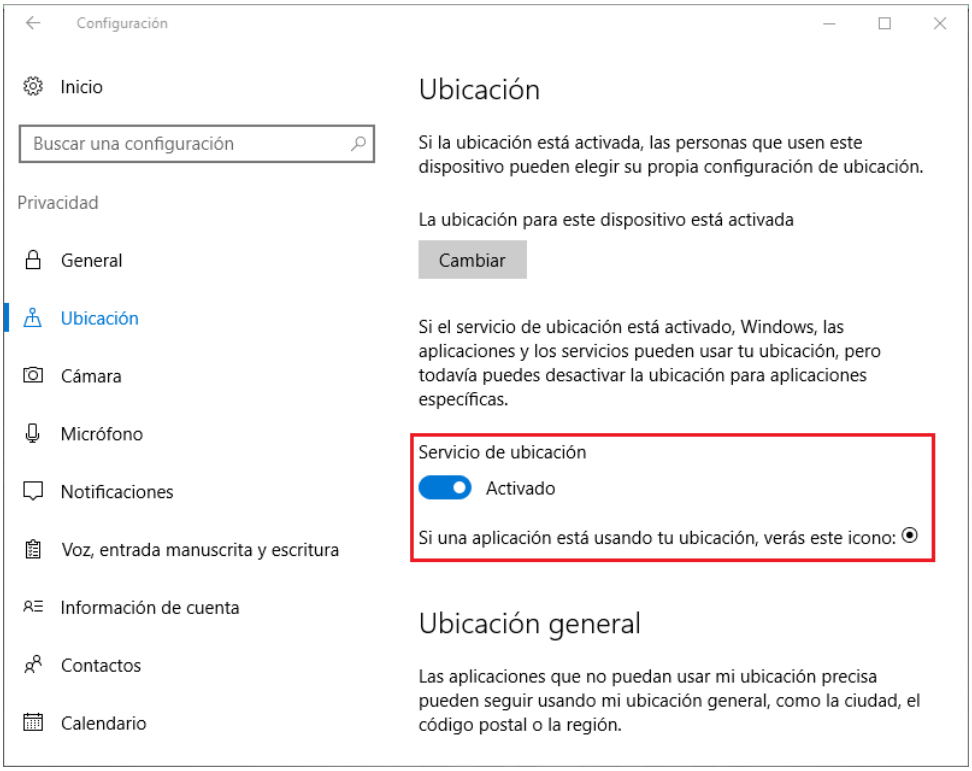


Figura 14: Ubicación activada.

3.7 ACTIVIDAD VII: CONFIGURACIÓN DE APPLOCKER

Para el control de aplicaciones y scripts que se pueden ejecutar/instalar en la tableta se configurará AppLocker de Windows.

Para llevar a cabo la configuración de AppLocker se seguirán los siguientes pasos:

1. Accedemos al editor de políticas de grupo de Windows mediante el comando gpedit.msc y deshabilitamos la política *Configuración de Usuario → Plantillas*

administrativas → Componentes de Windows → Microsoft Management Console → Restringir a los usuarios a la lista de complementos con permisos explícitos.

2. Accedemos a la directiva de seguridad local mediante el comando *secpol.msc* y nos dirigimos a *Directivas de control de aplicaciones → AppLocker*.

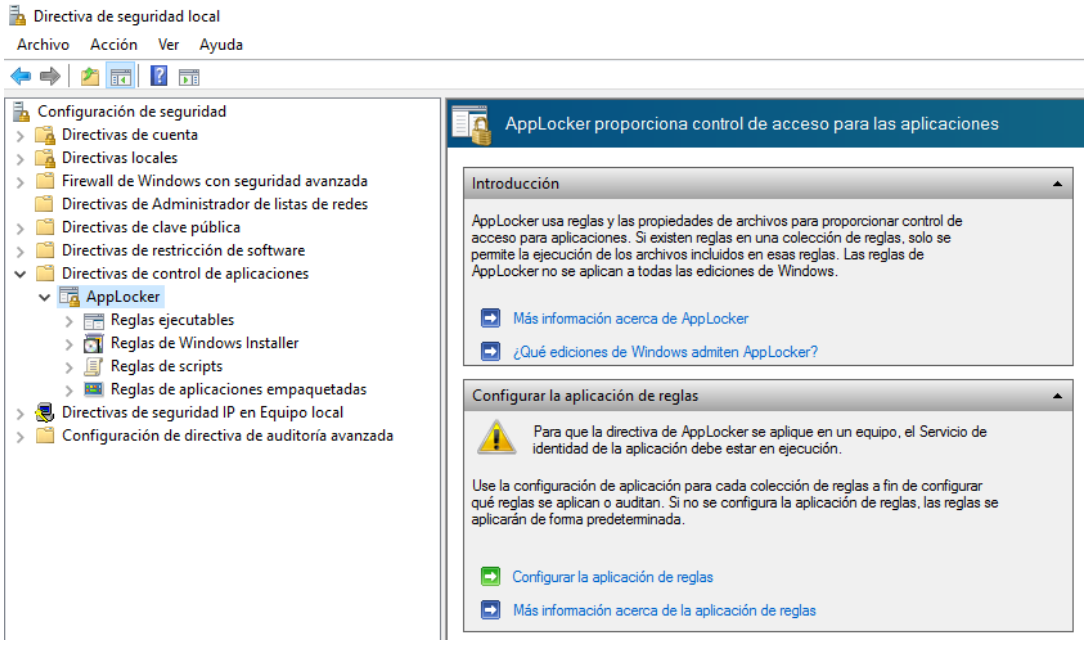


Figura 15: Directiva de seguridad local - AppLocker.

3. Desde el apartado AppLocker hacemos clic en *Configurar la aplicación de reglas*, habilitamos la *colección de reglas DLL* y hacemos clic en *Aceptar*.

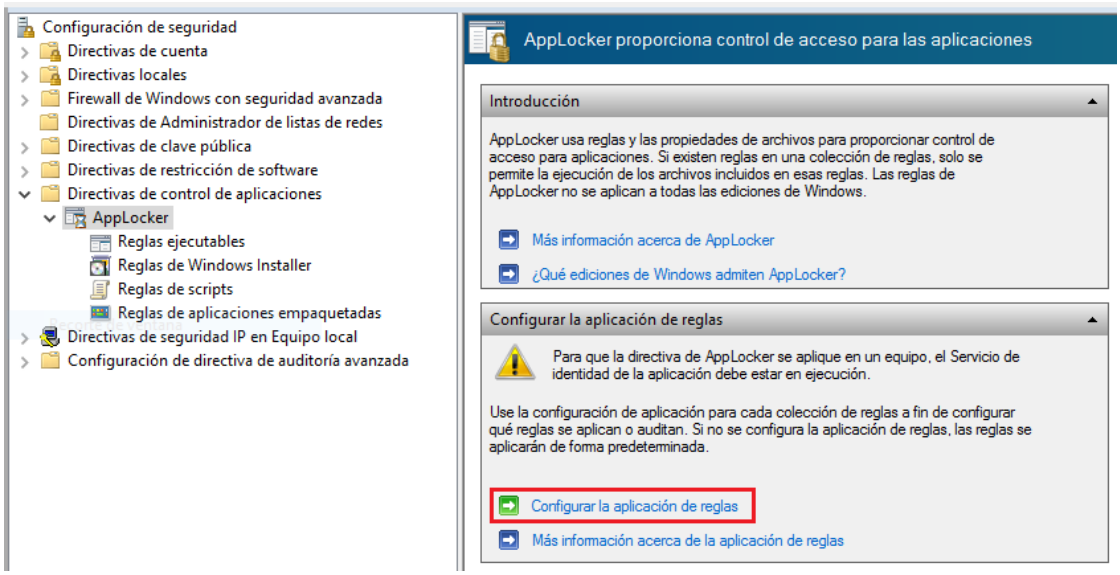


Figura 16: AppLocker – Habilitando las reglas de librerías - 1.

Figura 17: AppLocker – Habilitando las reglas de librerías - 2.

4. Creamos las reglas siguientes en cada uno de los tipos de reglas de AppLocker:

   Reglas ejecutables (.exe)

   a. Generamos las reglas predeterminadas mediante *clic derecho* → *Crear reglas predeterminadas*.

   b. Añadimos como *Excepciones* de tipo *Ruta de Acceso*, en la regla de nombre *Todos los archivos de la carpeta Windows*, los ficheros y directorios correspondientes indicados en la sección *Anexo A: Directorios y ficheros para bloquear en AppLocker* de este documento. Para ello se tendrán en cuenta los pasos descritos en la sección *4.1.10.3. Añadir excepciones en reglas* de este documento.

Acción	Usuario	Nombre	Condición	Excepcio...
Permitir	Todos	(Regla predeterminada) Todos los archivos de la carpeta Archivos de programa	Ruta de acceso	
Permitir	BUILTIN\Administradores	(Regla predeterminada) Todos los archivos	Ruta de acceso	
Permitir	Todos	Todos los archivos de la carpeta Windows	Ruta de acceso	Sí

Figura 18: AppLocker - Reglas ejecutables.

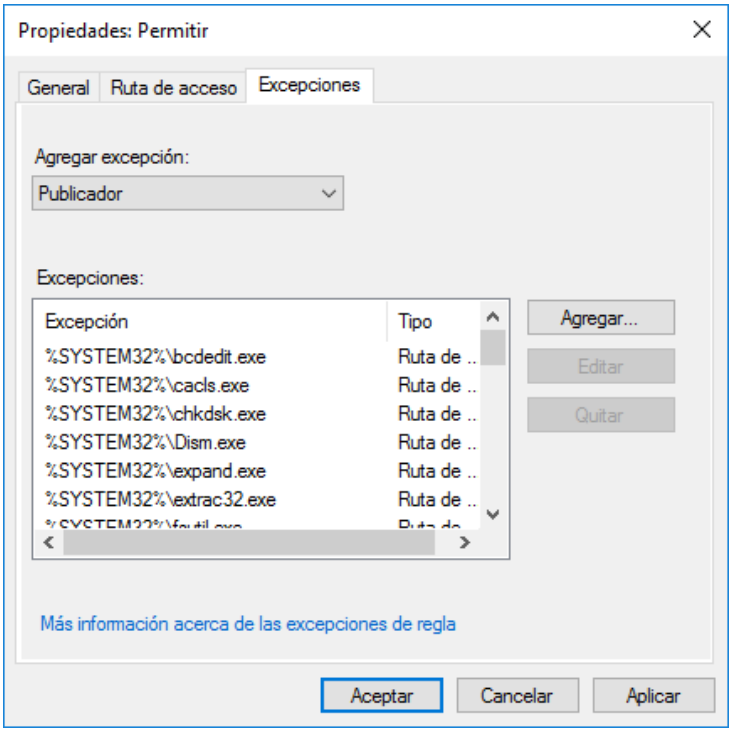


Figura 19: AppLocker - Reglas ejecutables - Excepciones de la regla *Todos los archivos de la carpeta Windows*.

Reglas de Windows Installer (.msi, .msp, .mst)

a. Generamos las reglas predeterminadas mediante *clic derecho* → *Crear reglas predeterminadas*.

b. Eliminamos las reglas predeterminadas excepto la que afecta al grupo *BUILTIN\Administradores* de forma que únicamente los usuarios administradores puedan instalar aplicaciones de este tipo.

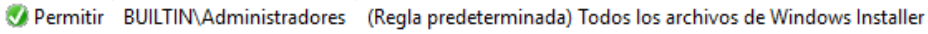


Figura 20: AppLocker - Reglas de Windows installer.

Reglas de scripts (.ps1, .bat, .cmd, .vbs, .js)

a. Generamos las reglas predeterminadas mediante *clic derecho* → *Crear reglas predeterminadas*.

b. Eliminamos las reglas predeterminadas excepto la que afecta al grupo *BUILTIN\Administradores* de forma que únicamente los usuarios administradores puedan ejecutar scripts.

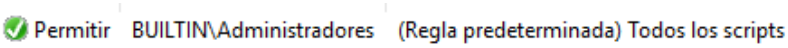


Figura 21: AppLocker - Reglas de scripts.

Reglas de DLL (.dll)

a. Generamos las reglas predeterminadas mediante *clic derecho → Crear reglas predeterminadas*.

c. Añadimos como *Excepciones* de tipo *Ruta de Acceso*, en la regla de nombre *Todos los archivos de la carpeta Windows*, los ficheros y directorios correspondientes indicados en la sección *Anexo A: Directorios y ficheros para bloquear en AppLocker* de este documento. Para ello se tendrán en cuenta los pasos descritos en la sección *4.1.10.3. Añadir excepciones en reglas* de este documento.

Acción	Usuario	Nombre	Condición	Excepcio...
Permitir	Todos	(Regla predeterminada) DLL de Microsoft Windows	Ruta de acceso	Sí
Permitir	Todos	(Regla predeterminada) Todos los archivos DLL de la carpeta Archivos de programa	Ruta de acceso	
Permitir	BUILTIN\Administradores	(Regla predeterminada) Todos los archivos DLL	Ruta de acceso	

Figura 22: AppLocker - Reglas de DLL.

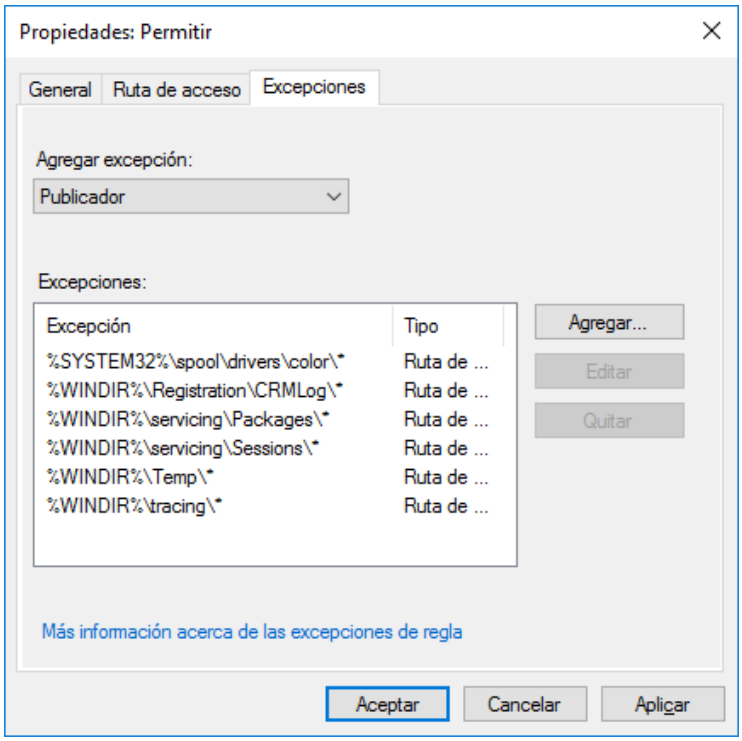


Figura 23: AppLocker - Reglas DLL - Excepciones de la regla Todos los archivos de la carpeta Windows.

Reglas de aplicaciones empaquetadas (aplicaciones universales Windows)

a. Creamos una regla para permitir únicamente aplicaciones firmadas por Microsoft. Para ello creamos una nueva regla mediante *clic derecho → Crear nueva regla* y seguimos los pasos mostrados en las figuras a continuación:

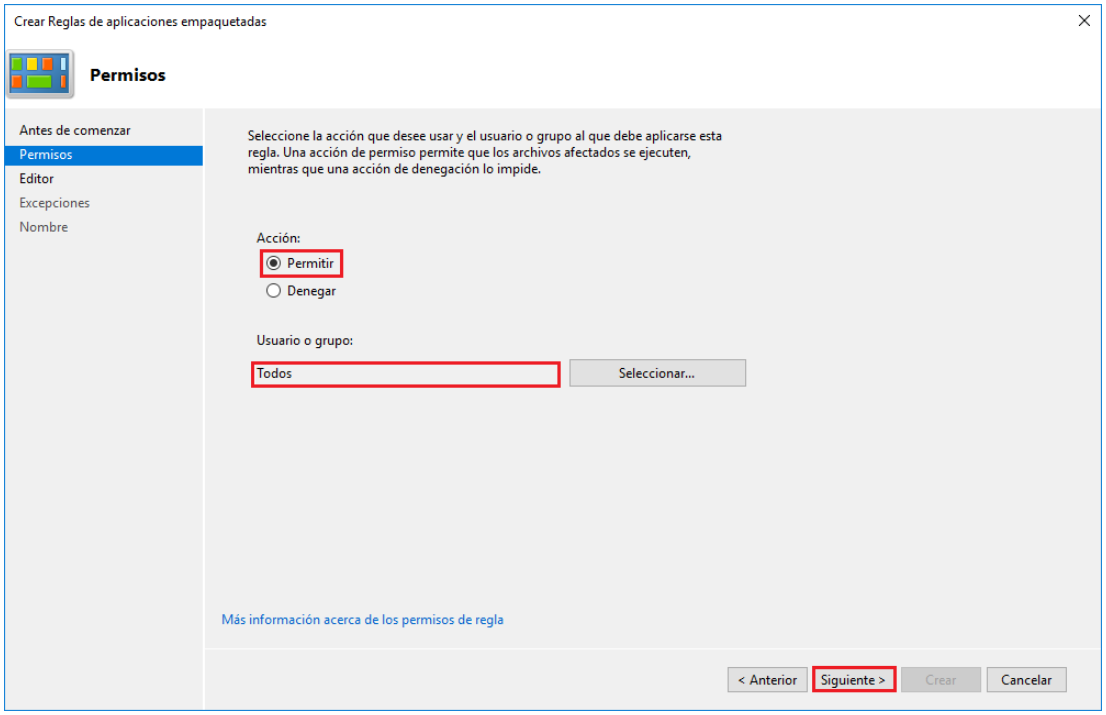


Figura 24: AppLocker - Creando regla de aplicaciones empaquetadas - 1.

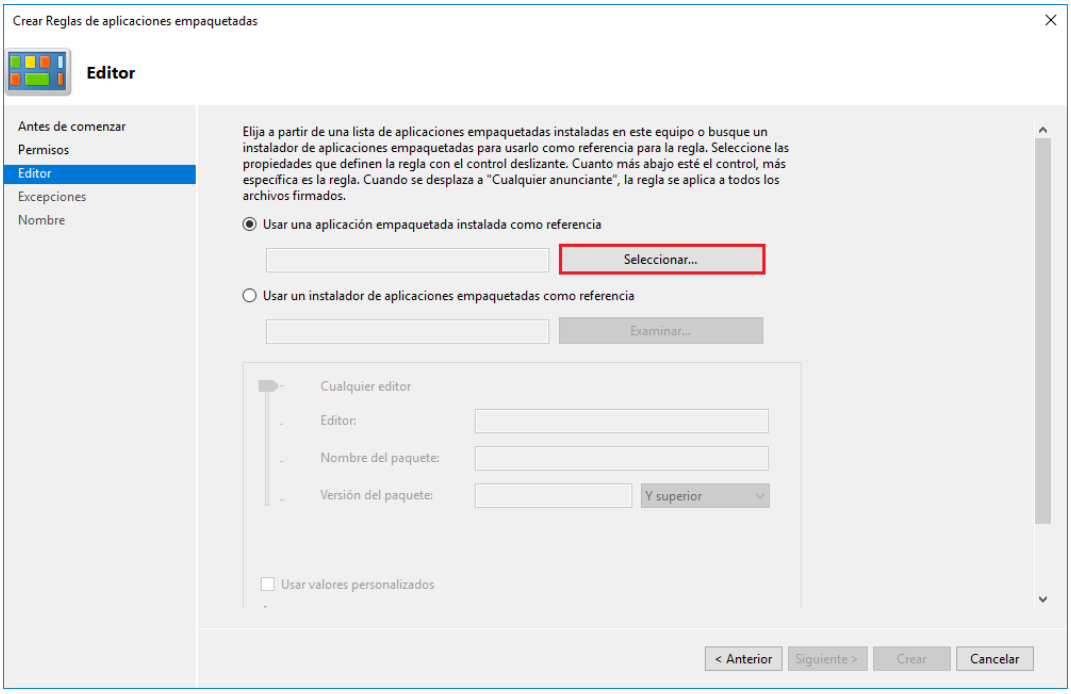


Figura 25: AppLocker - Creando regla de aplicaciones empaquetadas – 2.

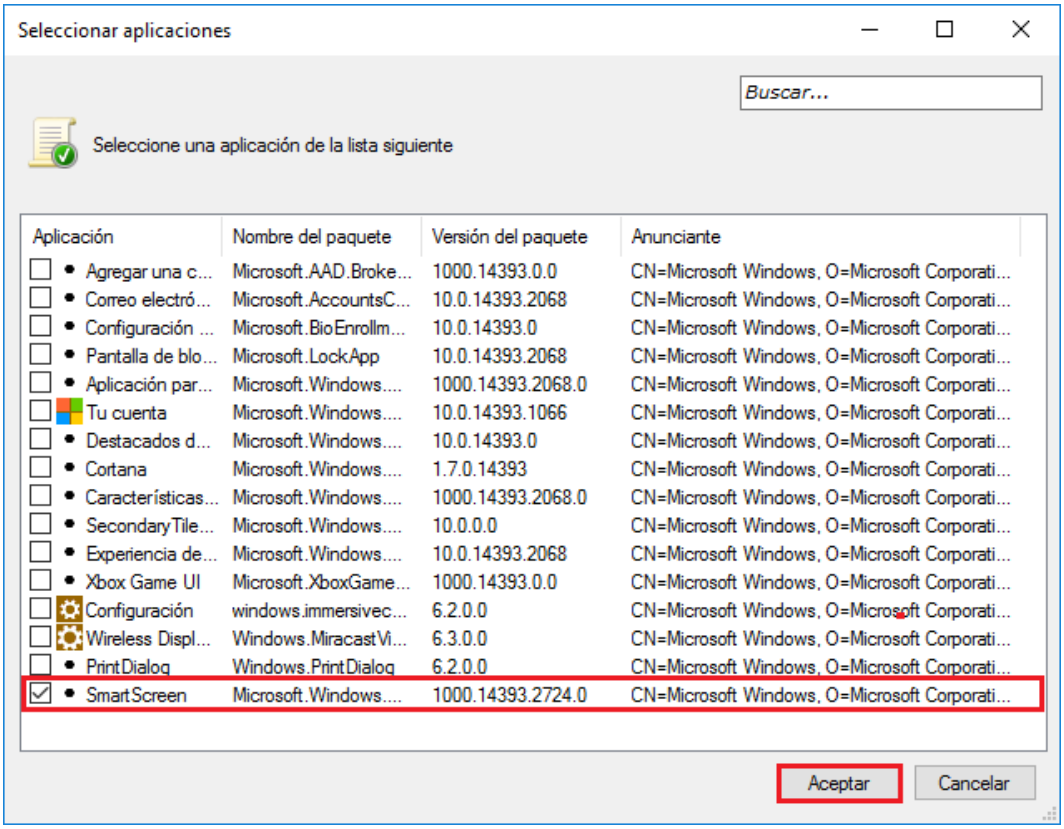


Figura 26: AppLocker - Creando regla de aplicaciones empaquetadas - 3.

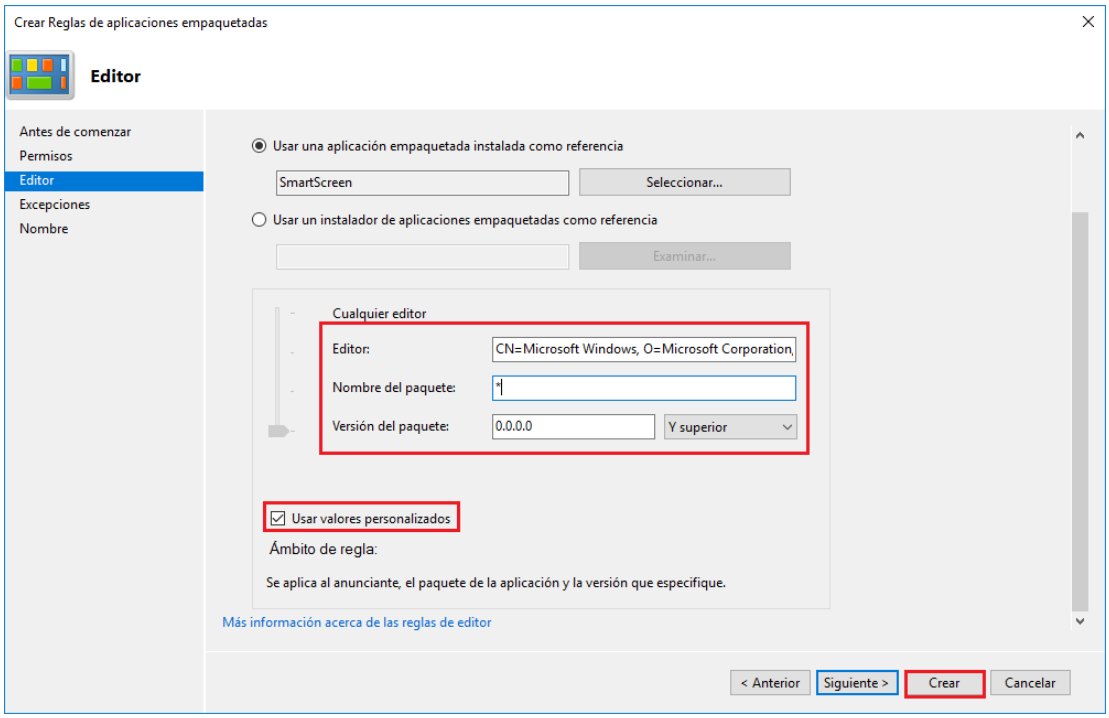


Figura 27: AppLocker - Creando regla de aplicaciones empaquetadas - 4.

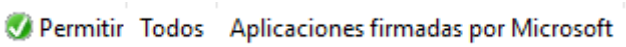


Figura 28: AppLocker - Reglas de Aplicaciones empaquetadas.

5. Tras esto, desde el apartado AppLocker hacemos clic en *Configurar la aplicación de reglas* y activamos la aplicación de reglas tal y como se muestra en las figuras a continuación:

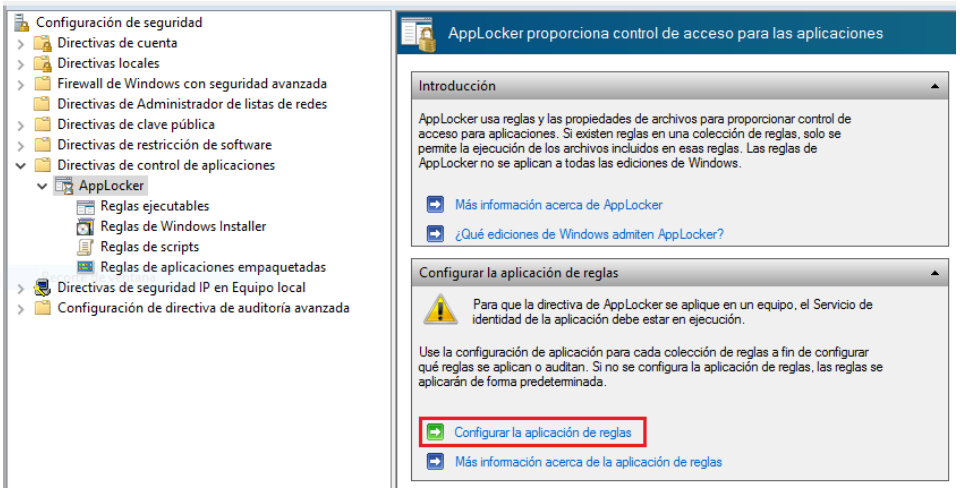


Figura 29: AppLocker - Configurando aplicación de reglas - 1.

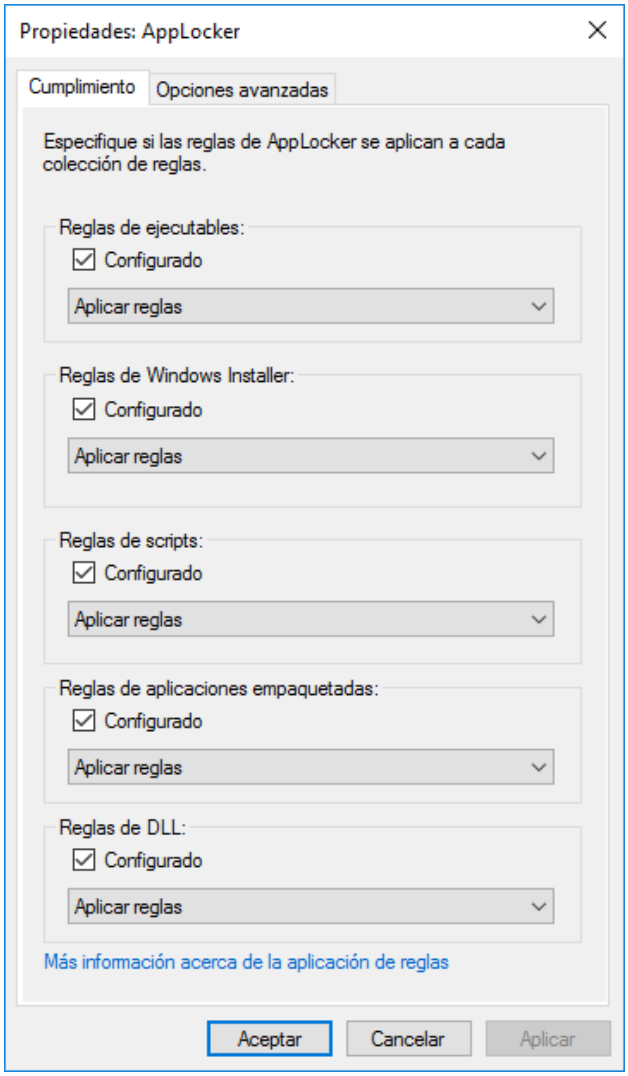


Figura 30: AppLocker - Configurando aplicación de reglas - 2.

6. Accedemos al editor de políticas de grupo de Windows mediante el comando gpedit.msc y habilitamos la política *Configuración de Usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Restringir a los usuarios a la lista de complementos con permisos explícitos*.

Para finalizar, destacar que al realizar una restauración de imagen del sistema operativo Windows de la tableta, la configuración de AppLocker puede quedar invalidada. Por ello, se recomienda guardar la configuración de AppLocker mediante el exportado de las reglas, con el fin de importarlas si se da el caso. Tanto para el exportado como el importado de las reglas de AppLocker se seguirán los pasos descritos en la sección *4.1.10.2 Exportar/Importar reglas* de este documento.

3.8 ACTIVIDAD VIII: HABILITAR TESTS CRIPTOGRÁFICOS

El sistema operativo debe ser configurado para ejecutar un conjunto de pruebas (FIPS 140-2, SP 800-56A y SP 800-90) que permiten validar los algoritmos criptográficos.

Para activar la ejecución automática en el sistema de estas pruebas accedemos al editor de políticas de grupo de Windows mediante el comando *gpedit.msc* y habilitamos la política: *Configuración de Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad → Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones de hash*.

3.9 ACTIVIDAD IX: SOFTWARE DE BORRADO SEGURO

Para asegurar el borrado seguro de la información almacenada en la tableta se debe instalar un producto de terceros de tipo herramienta de borrado seguro. Este producto será escogido por la organización o persona responsable de la tableta y deberá cumplir las siguientes características:

a. Deberá haber superado una evaluación funcional de seguridad y estar en posesión de un certificado conforme a la norma internacional Common Criteria, y/o un Certificado Nacional Esencial de Seguridad, LINCE.

b. Deberá configurarse y utilizarse de forma segura conforme a la documentación certificada del producto entregada por el fabricante.

3.10 ACTIVIDAD X: SOFTWARE ANTIVIRUS

Para asegurar la protección del sistema operativo de la tableta se debe hacer uso de un software de antivirus. Este será escogido por la organización o persona responsable de la tableta y deberá configurarse de acuerdo a la guía del fabricante.

Si se desea hacer uso del software antivirus predeterminado del sistema operativo (Windows Defender), se deben seguir los pasos descritos a continuación:

1. Accedemos al editor de políticas de grupo de Windows mediante el comando *gpedit.msc* y habilitamos la política *Configuración de Equipo → Plantillas administrativas → Componentes de Windows → Endpoint Protection → Desactivar Endpoint Protection (deshabilitada)*.

2. Abrimos Windows Defender y procedemos a activarlo mediante el botón *Activar*.

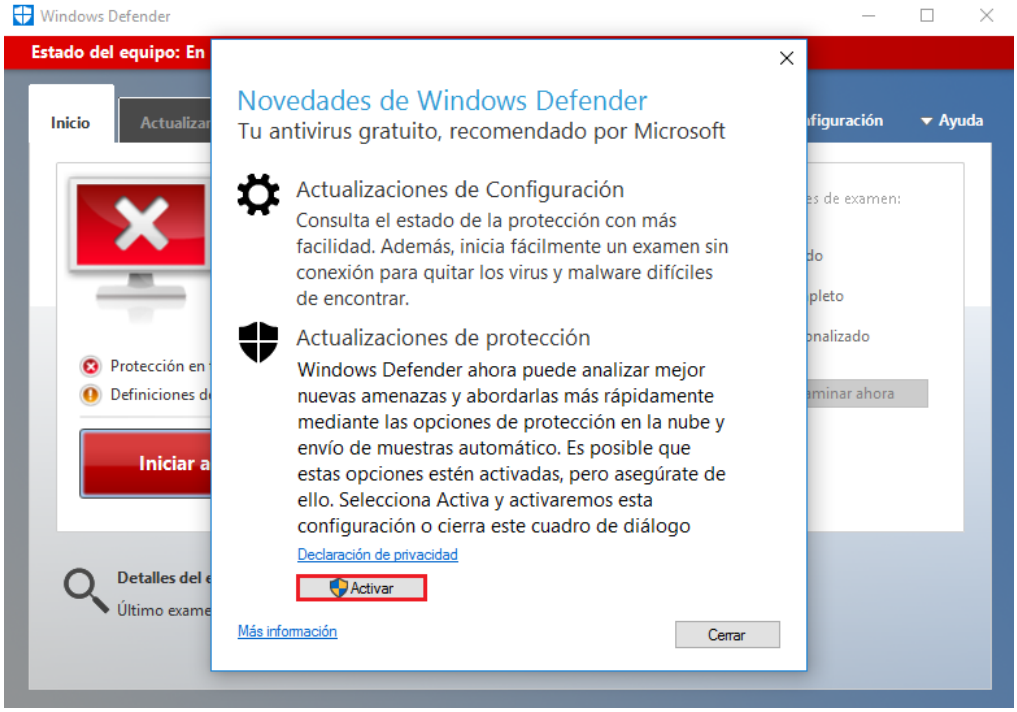


Figura 31: Activando Windows Defender - 1.

3. Iniciamos Windows Defender haciendo clic en el botón *Iniciar ahora*.

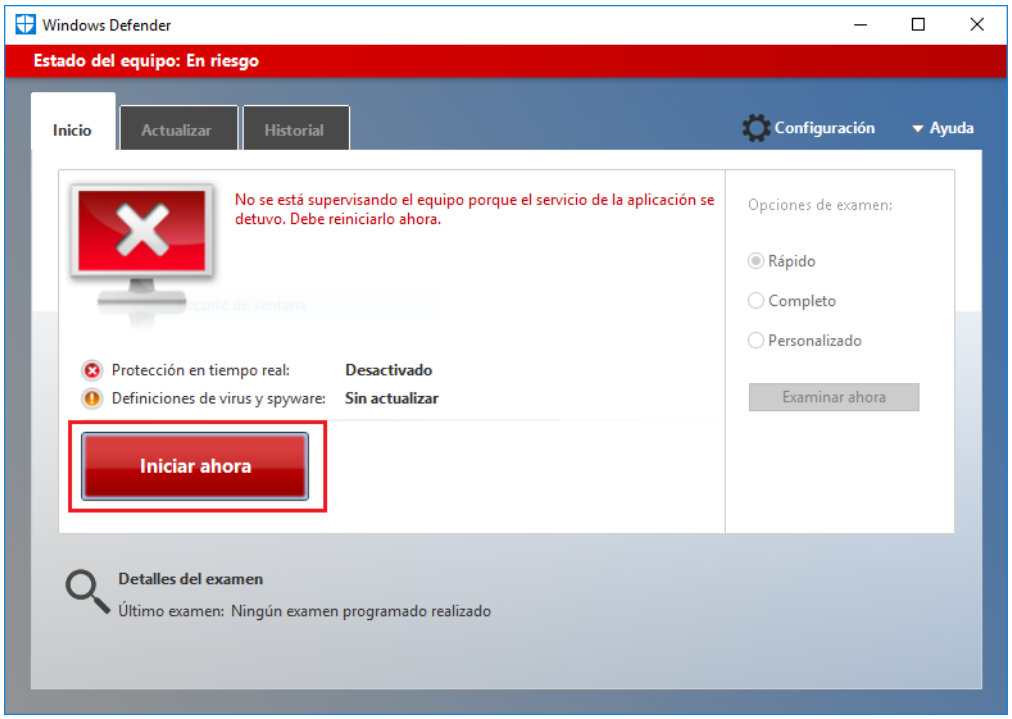


Figura 32: Activando Windows Defender - 2.

4. Observamos que se ha activado Windows Defender.

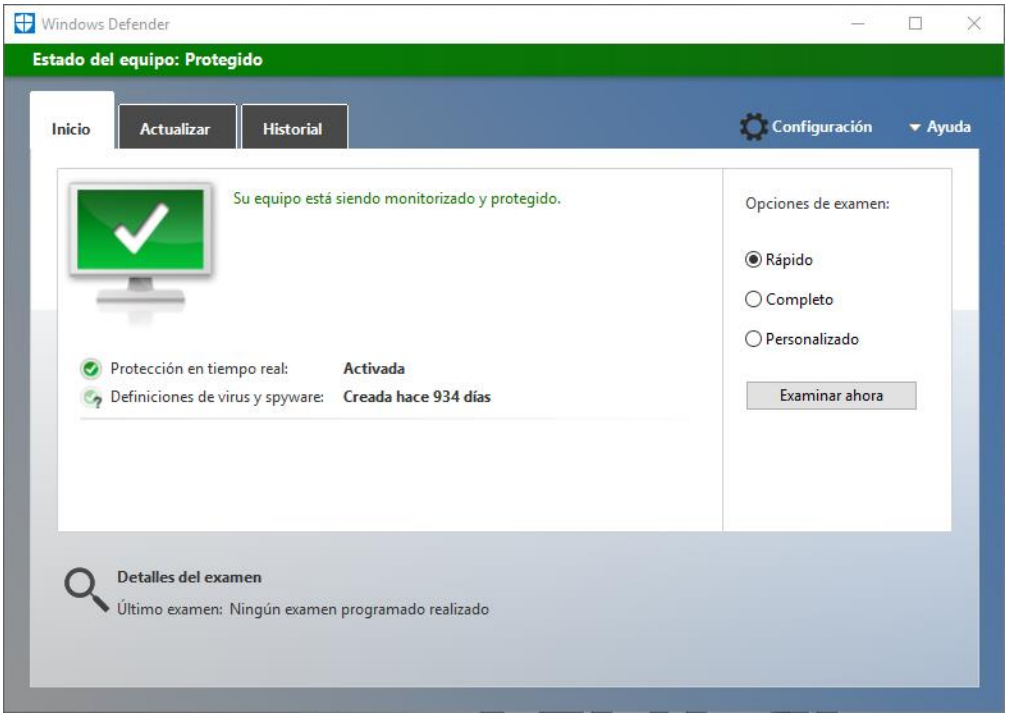


Figura 33: Activando Windows Defender - 3

3.11 ACTIVIDAD XI: PEGATINAS DE DETECCIÓN DE MANIPULACIÓN FÍSICA

Debido a que la tableta no tiene protección para detectar la manipulación física de los componentes hardware, se colocarán pegatinas de seguridad que permitan detectar la instalación/modificación de hardware no autorizada. Dichas pegatinas deberán contener un identificador único que permita disponer de un registro unívoco entre la tableta y la pegatina.

Esta actividad será realizada de acuerdo a la guía [CCN-STIC-409A].

En la figura siguiente se evidencia la colocación de una pegatina de seguridad en una zona de acceso a hardware del dispositivo:

Figura 34: Pegatina anti-tamper - 1.

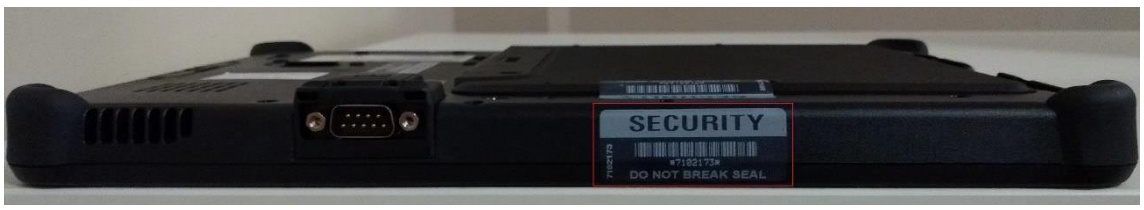


Figura 35: Pegatina anti-tamper - 2.

3.12 ACTIVIDAD XII: HABILITAR ARCHIVO DE REGISTROS DE AUDITORÍA

Es necesario configurar el sistema para habilitar el archivo de los registros de auditoria, de forma que se evite la sobrescritura de los eventos almacenados.

Para ello, accedemos al *Visor de eventos* mediante el comando *eventvwr* y configuramos las propiedades de los registros de auditoría de aplicación, seguridad, instalación y sistema, estableciendo el valor siguiente:

- Cuando alcance el tamaño máx. del reg. de eventos → Archivar el registro cuando esté lleno, no sobrescribir eventos.

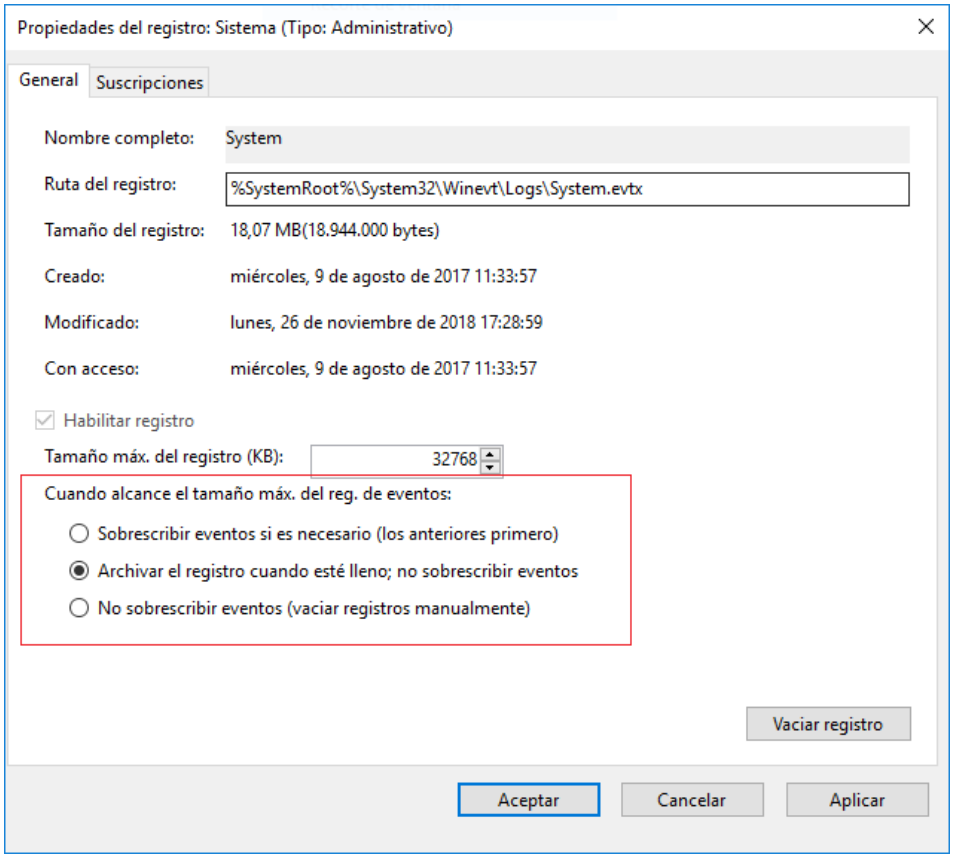


Figura 36: Propiedades de registro de eventos.

3.13 ACTIVIDAD XIII: COMPROBACIÓN DE DIRECTORIOS DE APPLOCKER

Los directorios y subdirectorios permitidos por AppLocker pueden ser utilizados por el usuario estándar para ejecutar aplicaciones no permitidas por AppLocker si el grupo *Usuarios* de Windows tiene permisos de lectura y escritura en los mismos.

Por ello, se comprobarán los permisos del grupo *Usuarios* bajo los directorios permitidos por AppLocker y se bloqueará, a nivel de ejecución de aplicaciones (.exe) y librerías (.dll), todos aquellos directorios y ficheros en los que el grupo *Usuarios* tenga permisos de lectura y escritura. Para ello, se añadirán excepciones en aquellas reglas

afectadas que permiten la ejecución de aplicaciones, teniendo en cuenta los pasos descritos en la sección *4.1.10.3 Añadir excepciones en reglas* de este documento

Además, se debe tener en cuenta la naturaleza de cada uno de los directorios detectados, ya que el bloqueo de los mismos puede alterar el comportamiento del sistema u ocasionar inestabilidad en el mismo.

Para la comprobación de los permisos se recomienda hacer uso de la herramienta *AccessChk* de SysInternals[4]. Para ello, se seguirán los siguientes pasos:

1. Se abrirá una consola PowerShell **sin privilegios de administrador**.
2. Se comprobarán los permisos de los directorios permitidos por AppLocker mediante el comando *accesschk.exe Usuarios /s [directorio] /w*, donde [directorio] hace referencia al directorio permitido por AppLocker.

[4] https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

4. MANUAL DE EMPLEO SEGURO

Esta sección describe las actividades para realizar un empleo seguro de la tableta GETAC F110G4 para cada rol de usuario.

4.1 USUARIO ADMINISTRADOR

Antes de comenzar, destacar que todos los comandos mostrados en esta sección deben ejecutarse desde una consola PowerShell con privilegios de administrador.

4.1.1. ACTIVIDAD I: AUTENTICACIÓN

Para acceder a los distintos componentes de la tableta primero hay que autenticarse. A continuación se describen los sistemas de autenticación propios del usuario administrador:

a. Autenticación de arranque del sistema, BitLocker.

Tras encender la tableta saltará la pantalla de autenticación de BitLocker, en la se escribirá la frase de paso correspondiente. Dicha pantalla mostrará un teclado en pantalla, que permitirá escribir la frase de paso, cuando se haga clic en el campo para escribir la frase.

b. Autenticación en Windows.

Tras realizar la autenticación en BitLocker, la tableta cargará el sistema operativo, y como consecuencia, la pantalla principal de autenticación de Windows, en la que el usuario deberá mantener pulsado el botón con la etiqueta **P1**, colocado a la derecha de la pantalla de la tableta, con el fin de acceder a la pantalla de ingreso de credenciales.

c. Autenticación en firmware UEFI.

Para acceder a la configuración del firmware UEFI, se deberá acceder al sistema operativo y ejecutar el comando *shutdown /r /o*. Tras esto, se iniciará la pantalla de recuperación de Windows, desde la que seleccionaremos la opción Solucionar problemas - Configuración de firmware UEFI – Reiniciar con el fin de acceder a la configuración de UEFI. Una vez dentro de la configuración de UEFI, accedemos a *Setup Utility* e ingresamos la frase de paso correspondiente. Al igual que en el caso de la autenticación de BitLocker, se mostrará un teclado en pantalla que permitirá escribir la frase de paso, cuando se haga clic en el campo para escribir la frase.

4.1.2. ACTIVIDAD II: GESTIÓN DE USUARIOS

Para gestionar los usuarios se hará uso de la herramienta *Administración de equipos* de Windows. En las siguientes subsecciones se definen los pasos a seguir.

4.1.2.1. CREACIÓN Y BORRADO DE UN USUARIO

Para crear un usuario se seguirán los siguientes pasos:

1. Abrimos la herramienta *Administración de equipos* mediante el comando compmgmt.msc.
2. Hacemos clic derecho sobre el apartado *Usuarios y grupos locales* → *Usuarios* y seleccionamos *Usuario nuevo…*.
3. Rellenamos los campos *Nombre de usuario*, *Contraseña* y *Confirmar contraseña* y hacemos clic en *Crear*.
4. Hacemos clic en *Cerrar*.

Para eliminar un usuario se seguirán los siguientes pasos:

1. Abrimos la herramienta *Administración de equipos* mediante el comando compmgmt.msc.
2. Nos dirigimos al apartado *Usuarios y grupos locales* → *Usuarios,* hacemos clic derecho sobre el usuario y seleccionamos la opción *Eliminar*.

4.1.2.2. AÑADIR O RETIRAR UN USUARIO DE UN GRUPO

Para gestionar la pertenencia de un usuario a los grupos Usuarios y Administradores se seguirán los siguientes pasos:

1. Abrimos la herramienta *Administración de equipos* mediante el comando compmgmt.msc.
2. Nos dirigimos al apartado *Usuarios y grupos locales* → *Usuarios* y hacemos doble clic sobre el usuario a gestionar.
3. Seleccionamos la pestaña *Miembro de* y…:
   a. Para añadirlo a un grupo, hacemos clic en *Agregar*, escribimos el nombre del grupo y seleccionamos *Aceptar*.
   b. Para retirar el usuario de un grupo, seleccionamos el grupo del cual se desee retirar la pertenencia del usuario y hacemos clic en *Quitar*.
4. Hacemos clic en *Aplicar* y seguidamente en *Aceptar*.

4.1.3. ACTIVIDAD III: CONTROL DE ACCESO

Todas las acciones de configuración y administración del sistema operativo requieren de autenticación previa al acceso de una herramienta de configuración y administración o bien para guardar los cambios en la configuración del sistema. Por ello, el usuario proveerá sus credenciales de administrador (usuario y contraseña) para realizar dichas acciones de forma satisfactoria. Cabe destacar que la pantalla de autenticación es mostrada automáticamente por el sistema operativo.

4.1.4. ACTIVIDAD IV: REGISTROS DE AUDITORÍA

Para acceder a los registros de auditoría se hará uso de la herramienta *Visor de eventos*. Para ejecutarla se hará uso del comando *eventvwr*.

Para administrar un registro desde dicha herramienta, se hará clic derecho sobre el mismo con el fin de acceder al menú contextual que permite exportarlo, importarlo y/o eliminarlo.

4.1.5. ACTIVIDAD V: DIAGNÓSTICO DEL MÓDULO DE PLATAFORMA SEGURA (TPM)

Para realizar un diagnóstico y obtener información sobre el TPM de la tableta se usarán los siguientes *cmdlets* de PowerShell:

- **Get-Tpm.** Muestra información sobre el TPM contenido en el equipo: si existe en el equipo, si está configurado, etc. Cabe destacar que el parámetro *OwnerAuth* devuelto por el comando no tiene valor debido a que la configuración segura del dispositivo evita que las claves privadas sean expuestas.
- **Get-TpmEndorsementKeyInfo.** Muestra información básica sobre las claves contenidas en el TPM.
- **Get-TpmSupportedFeature.** Verifica y muestra las características específicas del TPM. Si se ejecuta junto con el parámetro *Verbose*, PowerShell probará cada una de las características de manera automática.

4.1.6. ACTIVIDAD VI: DIAGNÓSTICO DEL CIFRADO DE DISCO

Para diagnosticar y comprobar el estado del cifrado de disco se hará uso del *cmdlet* de PowerShell *Get-BitlockerVolume*.

4.1.7. ACTIVIDAD VII: DIAGNÓSTICO DEL ARRANQUE SEGURO

Para comprobar el estado del arranque seguro se hará uso del *cmdlet* de PowerShell *Confirm-SecureBootUEFI.*

4.1.8. ACTIVIDAD VIII: ADMINISTRACIÓN DE MARCAS DE TIEMPO

Para administrar la fecha y hora del sistema y para configurar el servidor NTP se hará uso de las siguientes herramientas:

- **Set-Date.** Permite cambiar la fecha y hora del sistema en la tableta. Para realizar esto, se hará uso de los siguientes comandos:
    - Para cambiar únicamente la **fecha** del sistema se hará uso del comando *Set-Date –date "dd/mm/aaaa",* donde dd/mm/aaaa corresponde a la fecha en formato día/mes/año, por ejemplo:

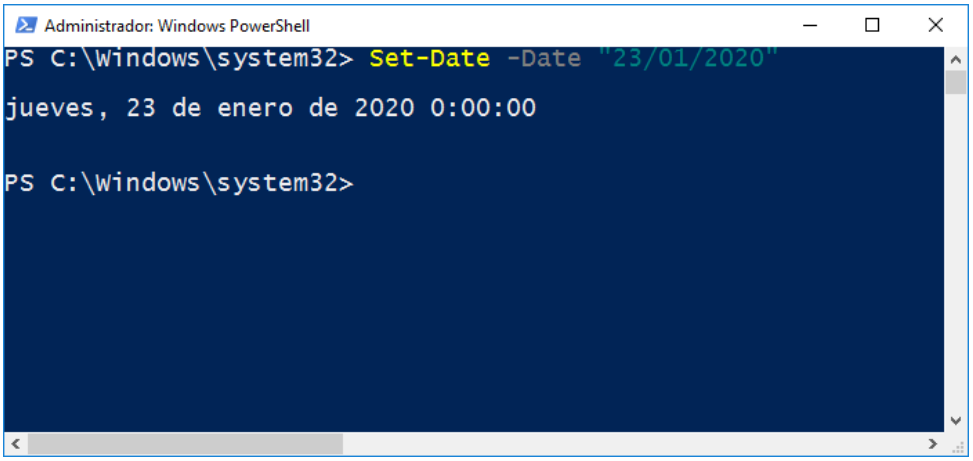


Figura 37: Cambio de fecha del sistema.

- Para cambiar únicamente la **hora** del sistema se hará uso del comando *Set-Date –date "hh:mm:ss",* donde hh:mm:ss corresponde a la hora en formato horas:minutos:segundos, por ejemplo:

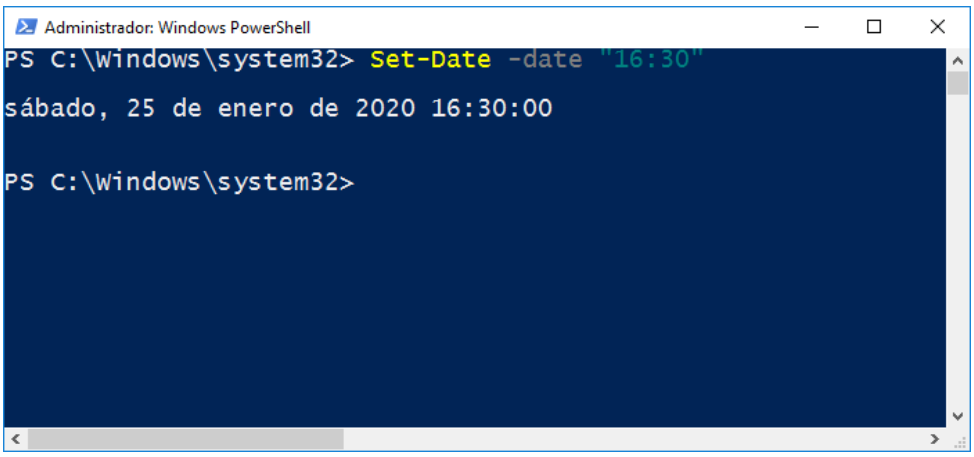


Figura 38: Cambio de hora del sistema.

- Para cambiar la **fecha y hora** del sistema al mismo tiempo se hará uso del comando *Set-Date –date "dd/mm/aaaa hh:mm:ss",* donde dd/mm/aaaa corresponde a la fecha en formato día/mes/año y hh:mm:ss corresponde a la hora en formato horas:minutos:segundos, por ejemplo:

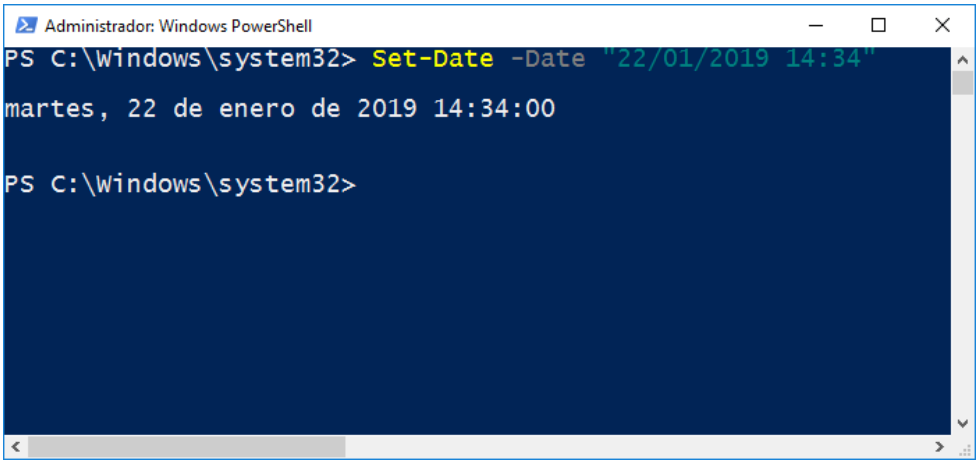


Figura 39: Cambio de fecha y hora del sistema.

Windows Time (W32TM). Permite configurar el servidor NTP del que cogerá la hora la tableta. Por un lado, para establecer dicho servidor se hará uso del comando *w32tm /config /computer:<objetivo> /update*, donde <objetivo> corresponde a la dirección IP o nombre DNS del servidor NTP. Por otro lado, para consultar la configuración actual de este servicio se hará uso del comando *w32tm /query /configuration*.

4.1.9. ACTIVIDAD IX: DIAGNÓSTICO DE PRUEBAS CRIPTOGRÁFICAS

Para comprobar si las pruebas criptográficas FIPS realizadas por el sistema operativo han obtenido resultados satisfactorios, se accederá al *Visor de eventos* de Windows y se filtrará el registro de auditoría de seguridad con el id de evento 6417.

4.1.10. ACTIVIDAD X: ADMINISTRACIÓN DE APPLOCKER

Esta actividad describe los pasos necesarios para administrar AppLocker según la necesidad.

Antes de comenzar, destacar que para configurar AppLocker se debe **deshabilitar** la siguiente política de grupo desde la herramienta *gpedit.msc*: *Configuración de Usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Restringir a los usuarios a la lista de complementos con permisos explícitos*. Asimismo, dicha política será nuevamente **habilitada** cuando se termine de configurar AppLocker.

4.1.10.1. PERMITIR O DENEGAR UNA APLICACIÓN

Para permitir o denegar una aplicación adicional a lo establecido durante la configuración segura en AppLocker, sección *Actividad VII: Configuración de AppLocker* de este documento, seguiremos los siguientes pasos:

1. Accedemos a la directiva de seguridad local mediante el comando *secpol.msc* y nos dirigimos a *Directivas de control de aplicaciones → AppLocker*.

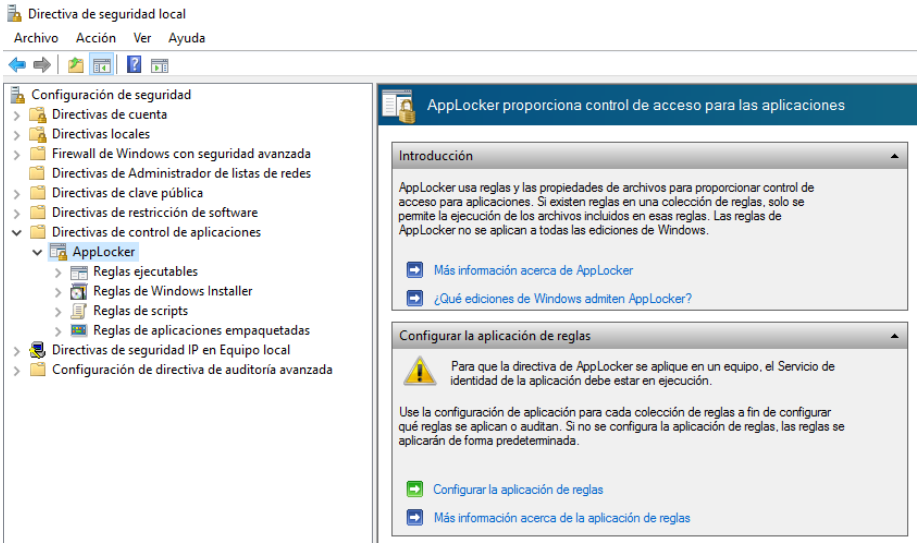


Figura 40: Directiva de seguridad local - AppLocker.

2. Hacemos clic derecho sobre *Reglas ejecutables* y seleccionamos *Crear nueva regla...*

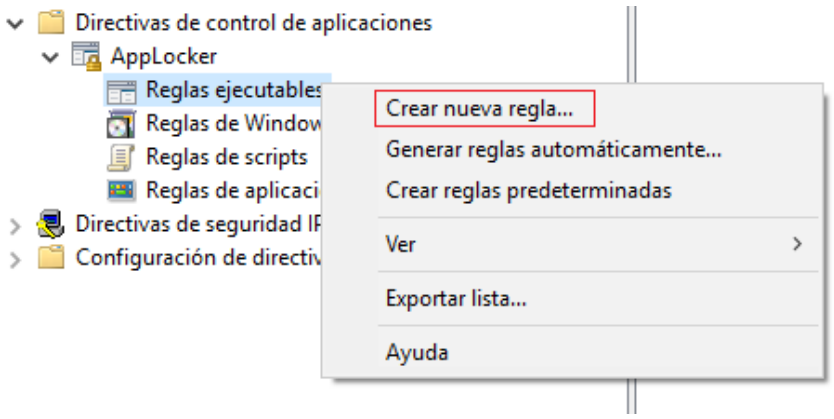


Figura 41: Permitir aplicación en AppLocker - 1.

3. Escogemos la opción *Permitir*, si se desea permitir la ejecución de la aplicación, o bien *Denegar*, si se desea denegar la ejecución de la aplicación y seleccionamos el usuario o grupo que se verá afectado por la regla.

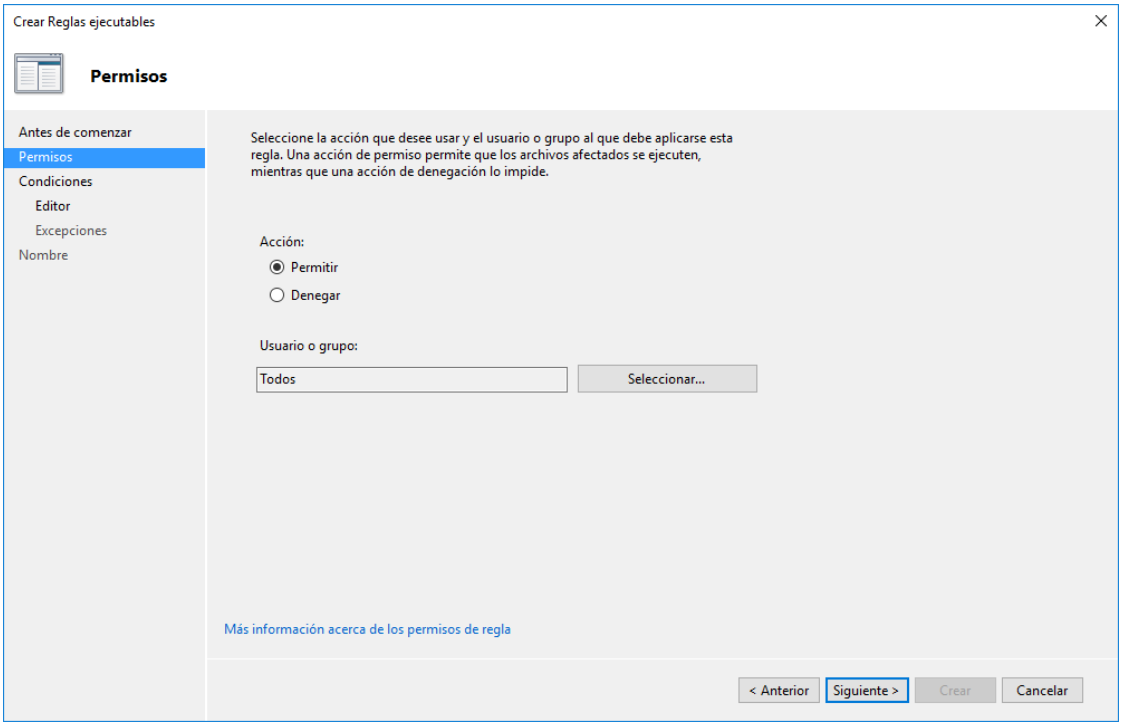


Figura 42: Permitir aplicación en AppLocker - 2.

4. Seleccionamos la opción *Ruta de acceso* como condición de la regla.

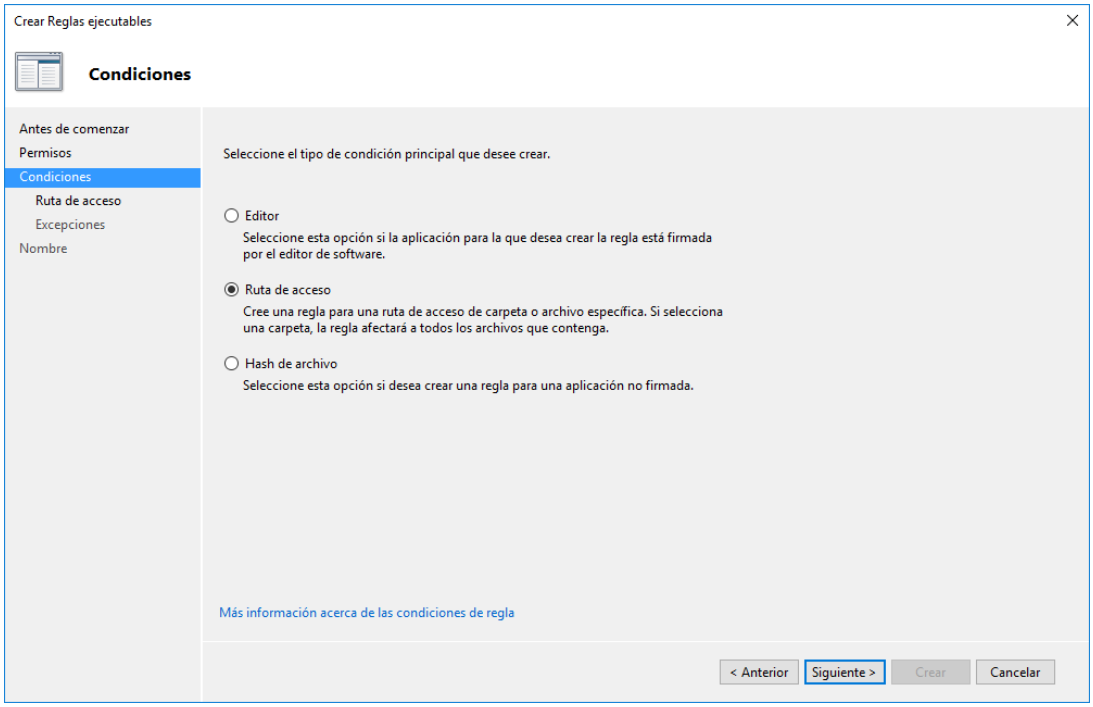


Figura 43: Permitir aplicación en AppLocker - 3.

5. Establecemos la ruta de acceso de la aplicación y hacemos clic en *Crear*.

Cabe destacar que la ruta de acceso puede establecerse para que la regla afecte a todos los ficheros que contenga un directorio, Figura 44, o bien a un fichero ejecutable específico, Figura 45.

En el caso de un directorio se debe hacer clic en *Examinar carpetas...*, mientras que, si se desea establecer un fichero ejecutable específico se debe hacer clic en *Examinar archivos...*

Si la aplicación contiene más de un ejecutable es recomendable añadir la ruta de acceso al directorio contenedor de la aplicación, en lugar de añadir el fichero ejecutable principal.

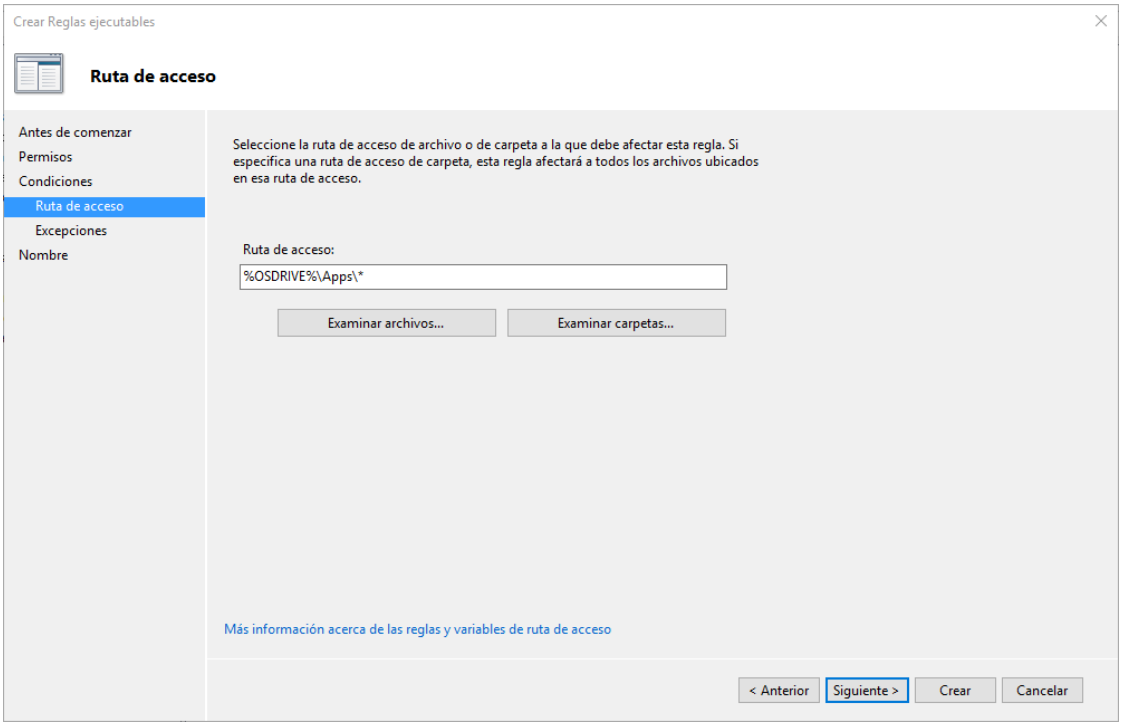


Figura 44: Permitir aplicación mediante ruta de acceso a un directorio en AppLocker - 4.

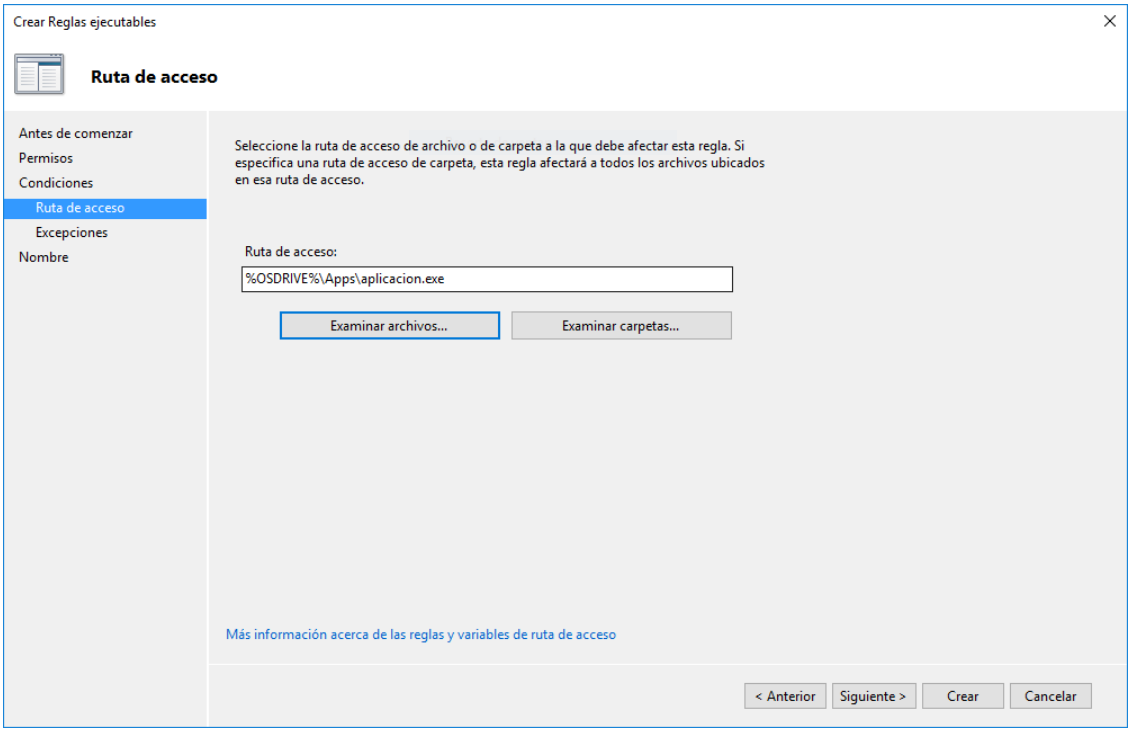


Figura 45: Permitir aplicación mediante ruta de acceso a un fichero ejecutable en AppLocker – 5.

4.1.10.2. EXPORTAR/IMPORTAR REGLAS

Para exportar e importar reglas de AppLocker se seguirán los siguientes pasos:

1. Accedemos a la directiva de seguridad local mediante el comando *secpol.msc* y nos dirigimos a *Directivas de control de aplicaciones* → *AppLocker*.

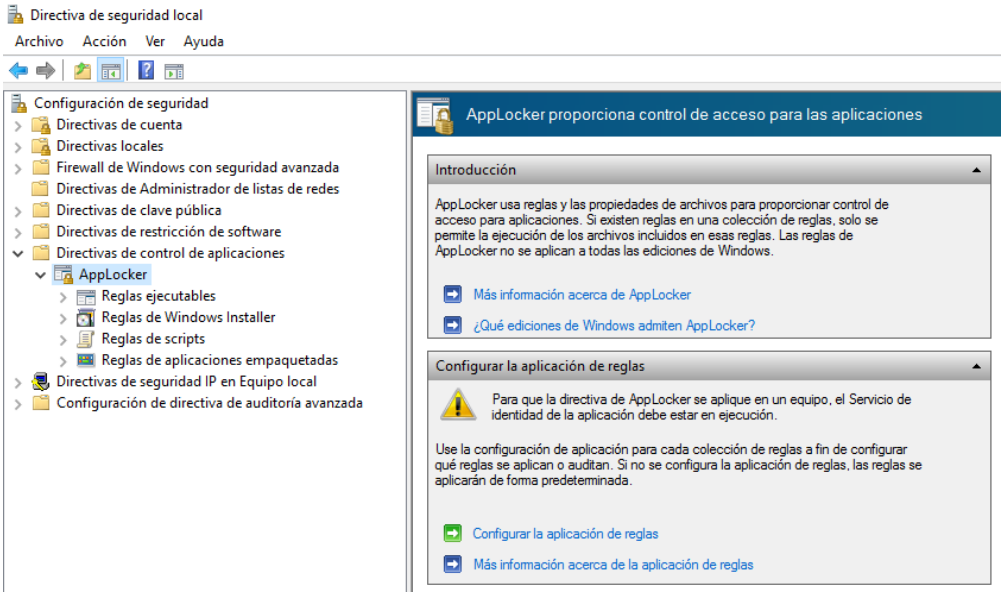


Figura 46: Directiva de seguridad local - AppLocker.

2. Hacemos clic derecho y seleccionamos *Exportar directiva…* o bien *Importar directiva…* según lo deseado, y seleccionamos la ruta donde almacenar, si se está exportando, o escoger, si se está importando, el fichero .XML que contiene las directivas de AppLocker.

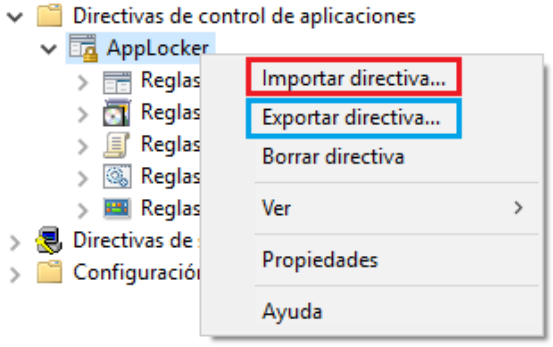


Figura 47: Importando/Exportando reglas de AppLocker - 1.

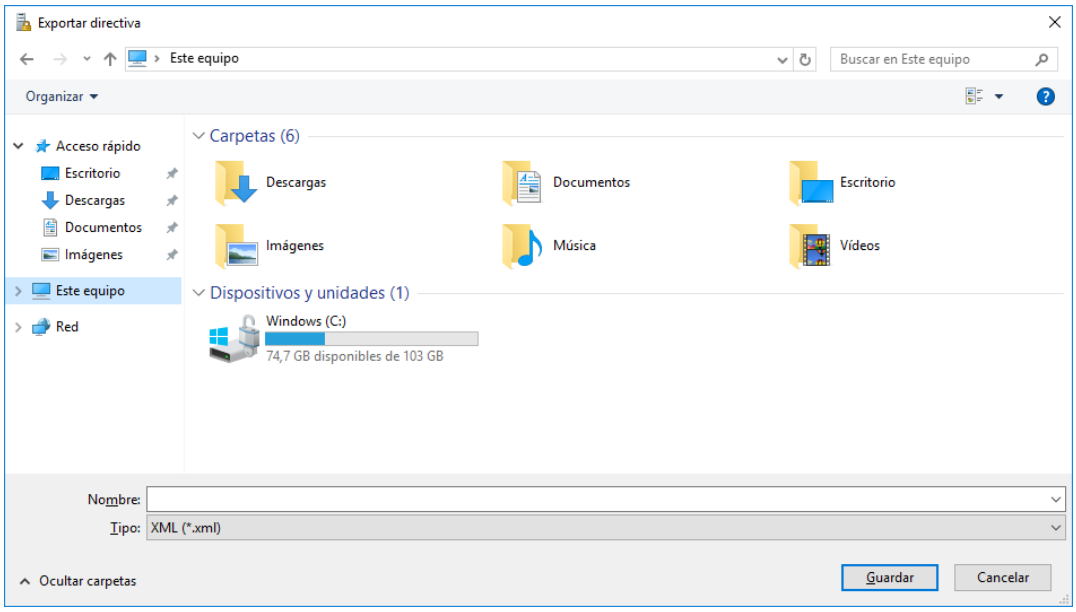


Figura 48: Importando/Exportando reglas de AppLocker - 2.

4.1.10.3. AÑADIR EXCEPCIONES EN REGLAS

Para añadir excepciones en reglas existentes de AppLocker se seguirán los siguientes pasos:

1. Accedemos a la directiva de seguridad local mediante el comando *secpol.msc* y nos dirigimos a *Directivas de control de aplicaciones* → *AppLocker*.

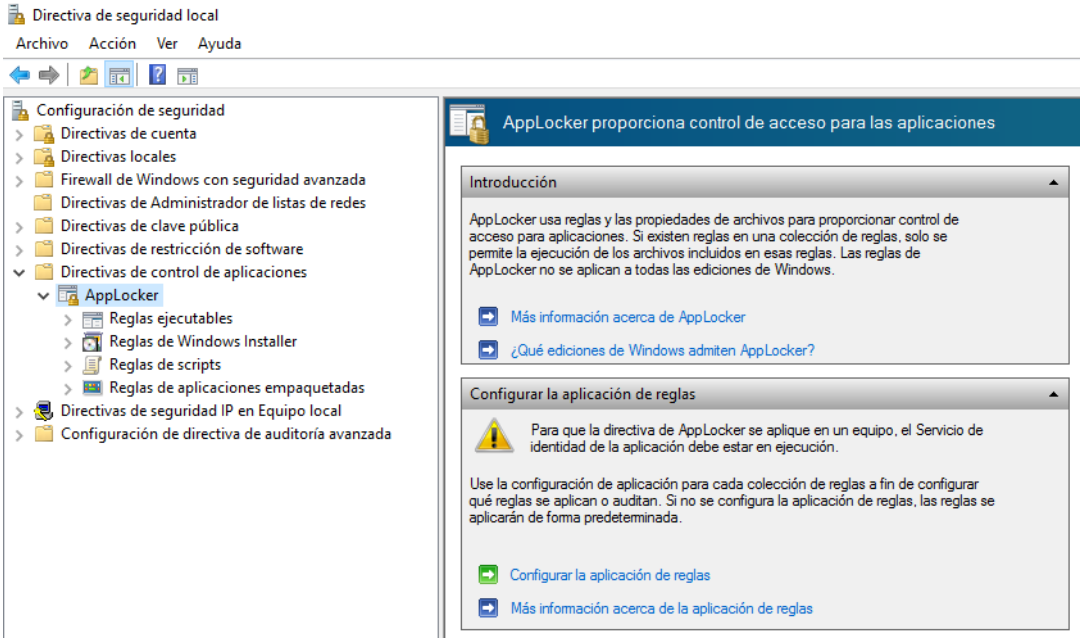


Figura 49: Directiva de seguridad local - AppLocker.

2. Hacemos doble clic sobre la regla en la que se desea agregar excepciones, nos dirigimos a la pestaña *Excepciones,* nos aseguramos que el tipo de regla *Ruta de acceso* se encuentra seleccionada y hacemos clic en *Agregar*.

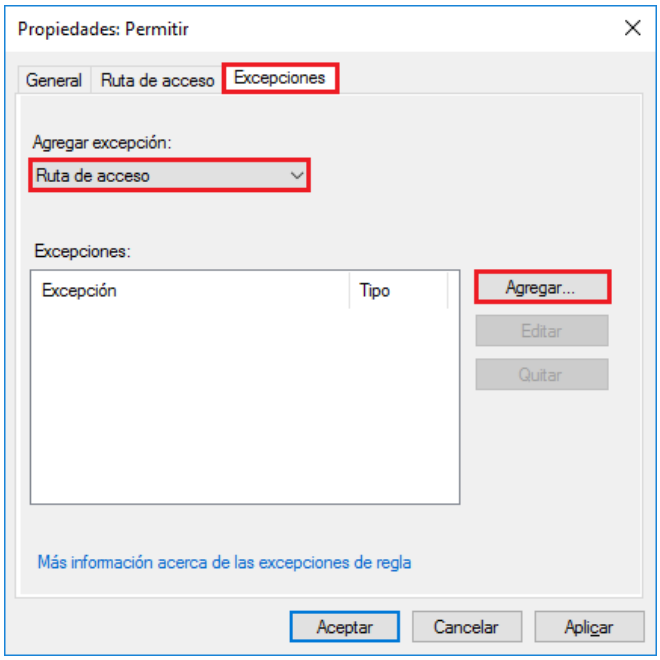


Figura 50: Agregando excepción - 1.

3. Hacemos clic en *Examinar archivos,* para agregar un archivo, o bien *Examinar carpetas*, para agregar un directorio.

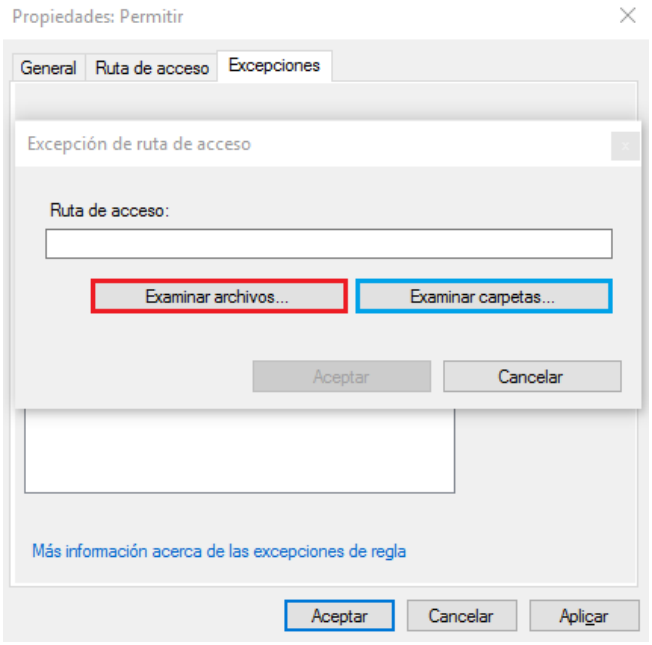


Figura 51: Agregando excepción - 2.

4. Seleccionamos el fichero o directorio deseado.

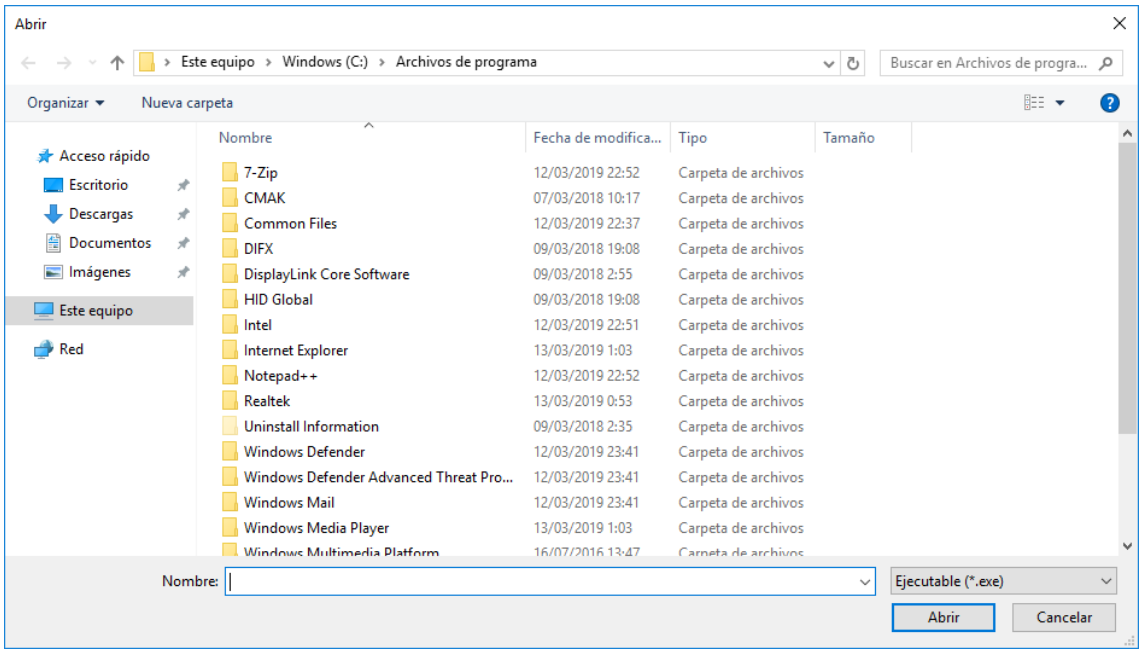


Figura 52: Agregando excepción - 3.

5. Hacemos clic en Aceptar.

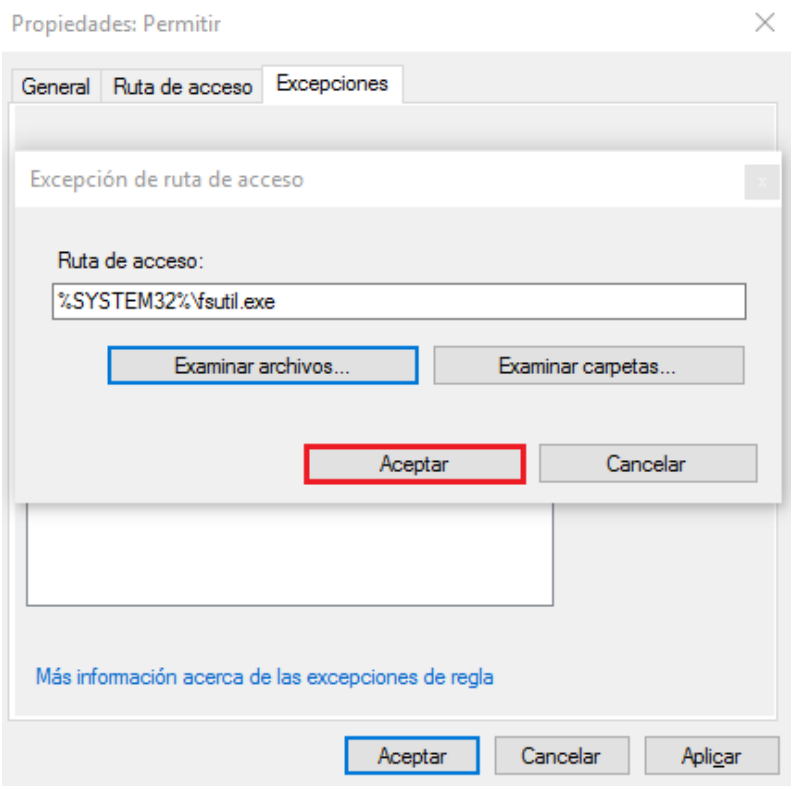


Figura 53: Agregando excepción - 4.

6. Hacemos clic en *Aplicar* y seguidamente en *Aceptar*.

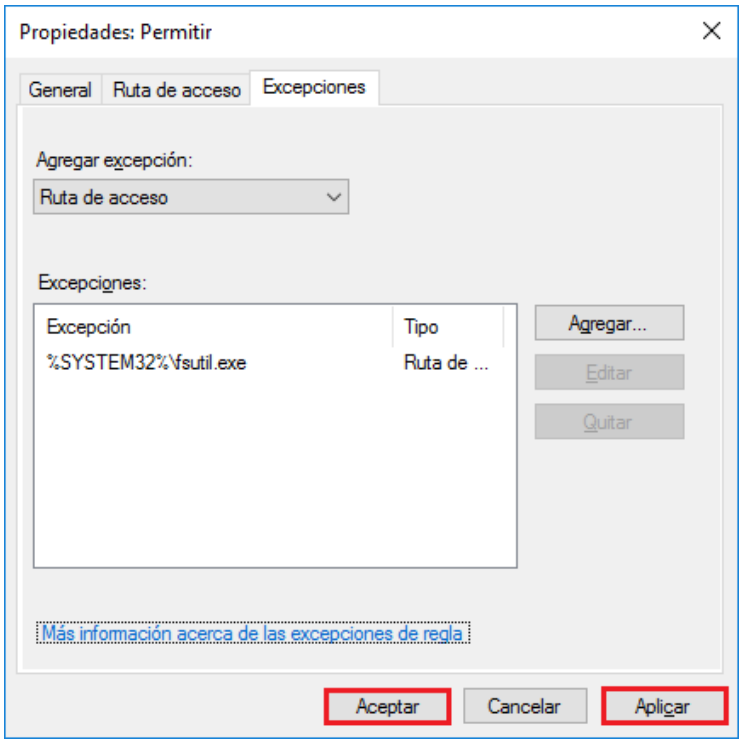


Figura 54: Agregando excepción - 5.

4.1.11. ACTIVIDAD XI: ACTUALIZACIÓN DEL SISTEMA OPERATIVO

Para escoger el método de distribución y entrada de actualizaciones se tendrá en cuenta la guía [CCN-STIC-512].

Antes de instalar actualizaciones, se deben activar los servicios *Windows Update* y *Preparación de aplicaciones.* Para realizar esto, se llevarán a cabo las siguientes acciones:

1. Abrimos la herramienta *Servicios* mediante el comando *services.msc*.

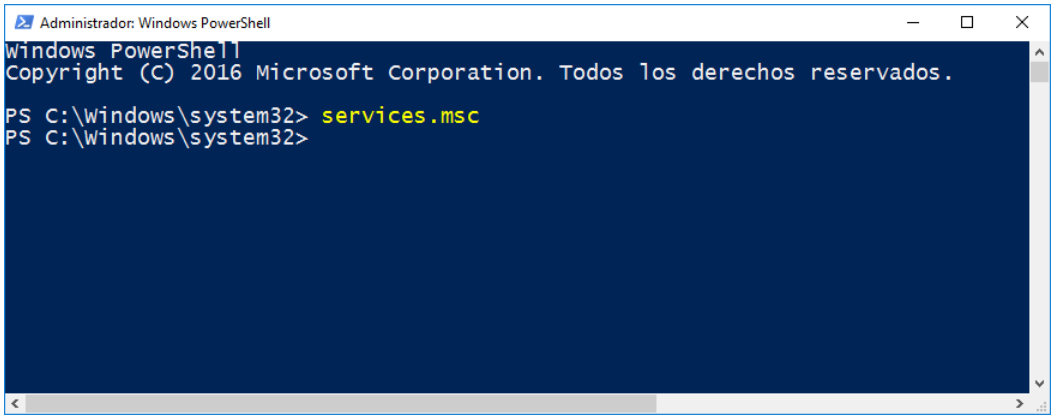


Figura 55: Actualizaciones, activando servicios necesarios - 1.

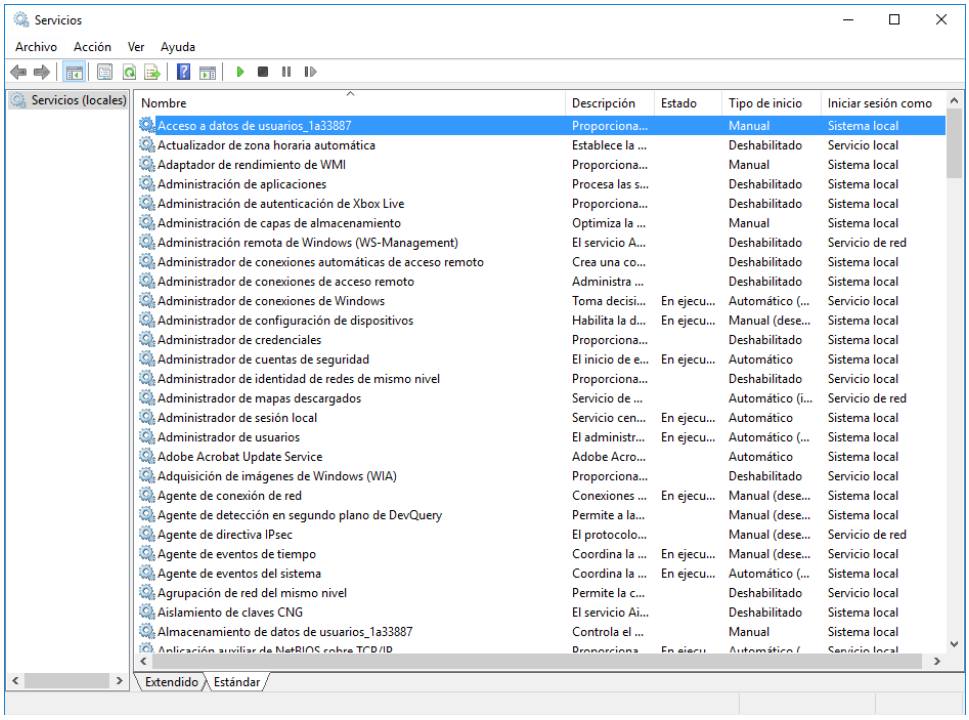


Figura 56: Actualizaciones, activando servicios necesarios – 2.

2. Iniciamos y configuramos en modo *Automático* cada uno de los servicios nombrados anteriormente.

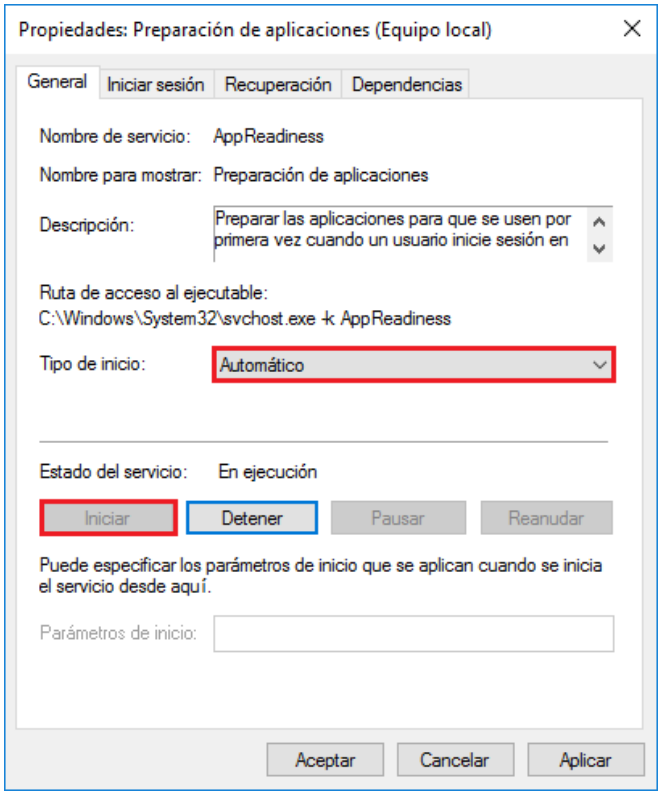


Figura 57: Actualizaciones, activando servicios necesarios – 3.

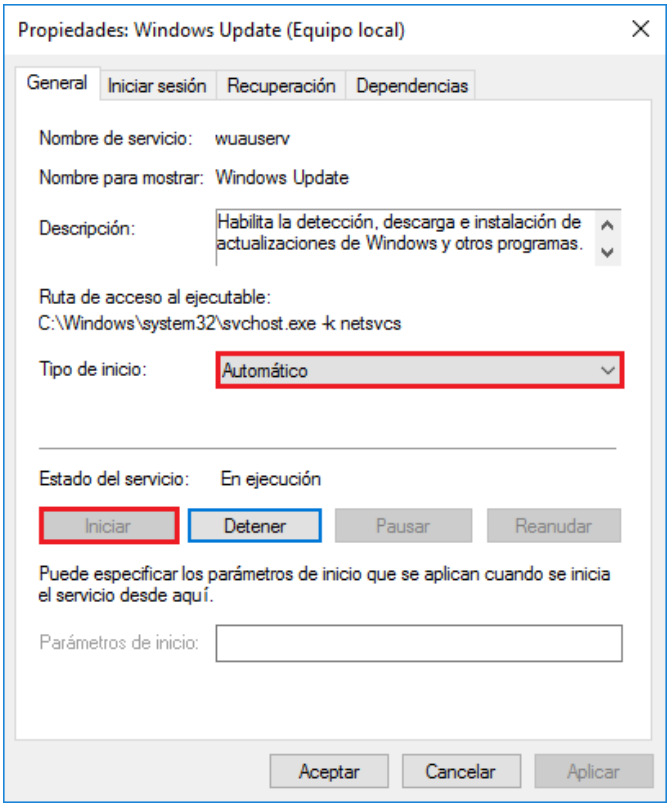


Figura 58: Actualizaciones, activando servicios necesarios – 4.

Cabe destacar que cuando finalicen las actualizaciones, se deshabilitarán y detendrán dichos servicios siguiendo el mismo procedimiento.

Para finalizar, cuando se realice la actualización se tendrá en cuenta lo descrito en la sección *3.13 Actividad XIII: Comprobación de directorios de AppLocker* de este documento, con el fin de evitar que los nuevos ficheros y directorios generados por la aplicación permitan a un usuario estándar saltarse AppLocker.

4.1.12. ACTIVIDAD XII: MANIPULACIÓN FÍSICA

Si surge la necesidad de acceder al hardware de la tableta se deberán reemplazar las etiquetas afectadas por unas nuevas y se actualizará el registro de etiquetas mantenido por la organización.

4.1.13. ACTIVIDAD XIII: BLOQUEO Y DESBLOQUEO DE SESIÓN

Para bloquear la sesión se hará uso de la combinación de teclas *Windows + L* o bien de la función *Bloquear* accesible desde la combinación de teclas *CTRL + ALT + SUPR*.

Por otro lado, para desbloquear la sesión, se mantendrá pulsado el botón con la etiqueta **P1**, colocado a la derecha de la pantalla de la tableta, para acceder a la pantalla de autenticación, en la que se ingresarán las credenciales.

4.1.14. ACTIVIDAD XIV: TIEMPO DE INACTIVIDAD PARA EL BLOQUEO DE SESIÓN

La configuración aplicada en la sección *3.3 Actividad III: Aplicación de la guía CCN-STIC-599B* establece el tiempo de inactividad en 900 segundos de forma predeterminada. Si se desea modificar este tiempo de inactividad se realizarán los siguientes pasos:

1. Accedemos al editor de políticas de grupo mediante el comando *gpedit.msc.*
2. Establecemos el tiempo de inactividad (en segundos) en la política contenida en *Configuración de equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad → Inicio de sesión interactivo: límite de inactividad del equipo*.

4.1.15. ACTIVIDAD XV: HABILITAR LA INSTALACIÓN DE UN DISPOSITIVO

La guía STIC 599B aplicada en la sección *3.3 Actividad III: Aplicación de la guía CCN-STIC-599B* establece el bloqueo de instalación de dispositivos hardware mediante lista blanca.

Para permitir la instalación de un dispositivo en concreto, se debe modificar la política de grupo de Windows. Para ello, se seguirán los siguientes pasos:

1. Accedemos al *Administrador de dispositivos* mediante el comando *devmgmt.msc* y copiamos los ID de hardware de las propiedades del dispositivo a instalar:

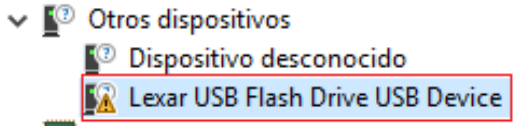


Figura 59: Habilitar instalación de dispositivo - 1.

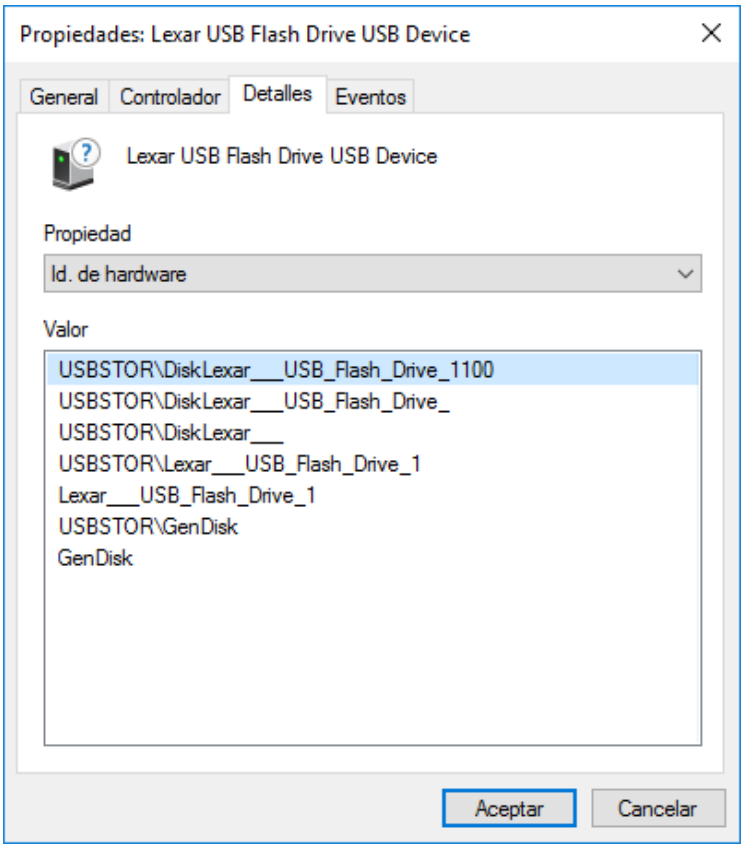


Figura 60: Habilitar instalación de dispositivo - 2.

2. Abrimos el editor de la política de grupo de Windows mediante el comando *gpedit.msc* y añadimos los ids. de hardware al listado del parámetro *Configuración de Equipo → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos → Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo*.

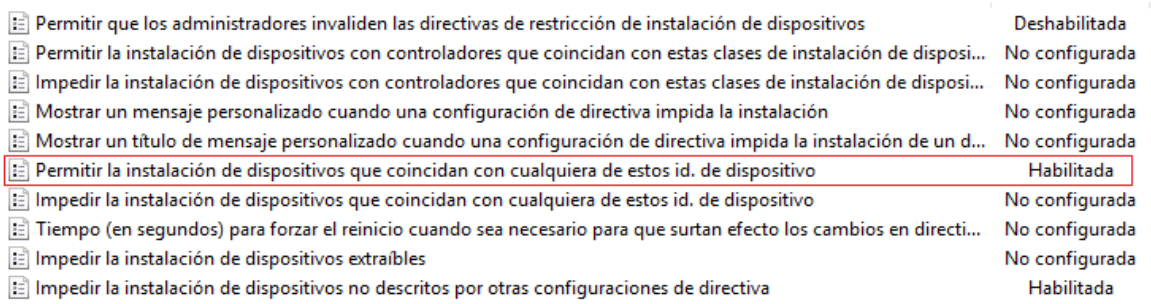


Figura 61: Habilitar instalación de dispositivo - 3.

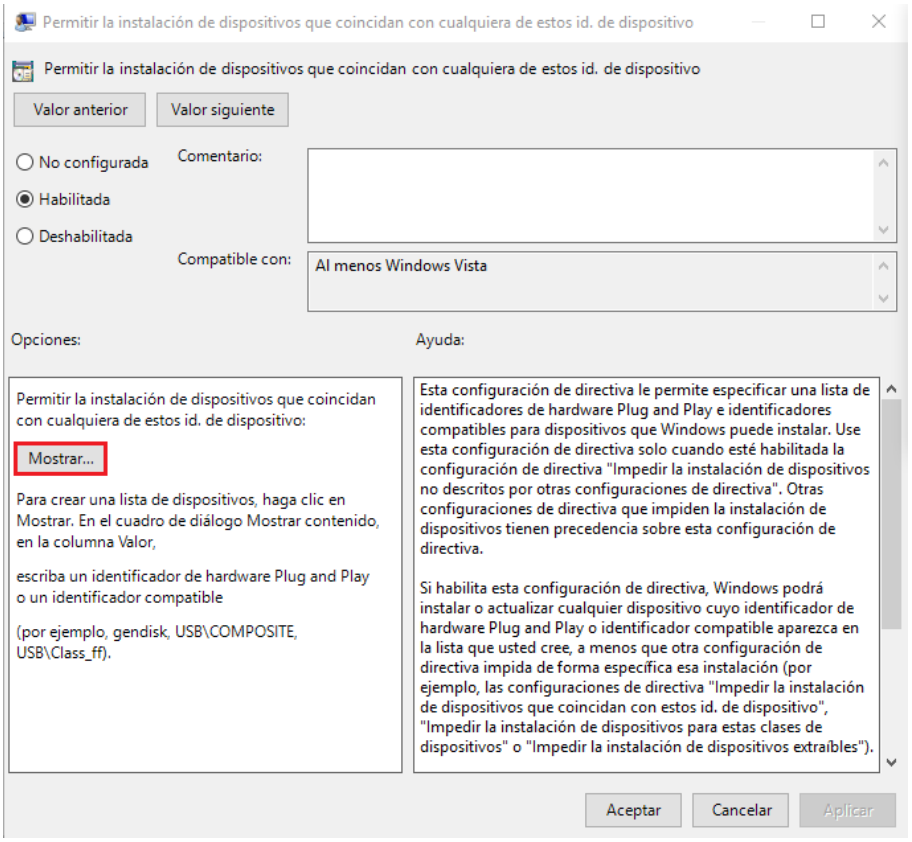


Figura 62: Habilitar instalación de dispositivo - 4.

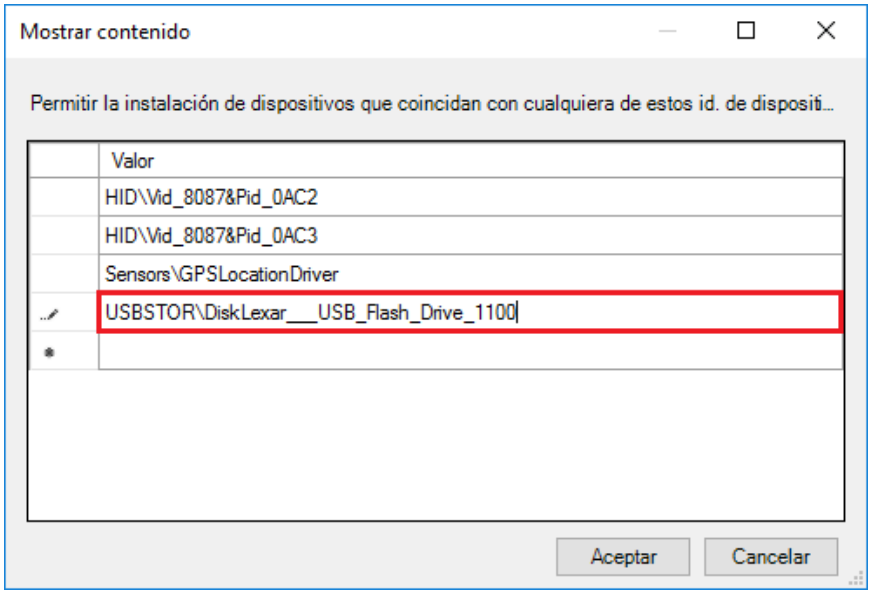


Figura 63: Habilitar instalación de dispositivo - 5.

3. Observamos que el dispositivo se ha instalado correctamente y categorizado automáticamente en el administrador de dispositivos.

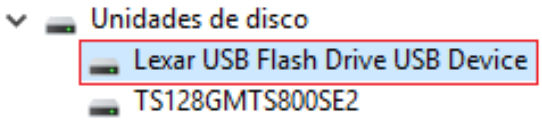


Figura 64: Habilitar instalación de dispositivo – 6.

4.1.16. ACTIVIDAD XVII: INSTALACIÓN DE APLICACIONES

Cuando se realice la instalación de una aplicación se tendrá en cuenta lo descrito en la sección *3.13 Actividad XIII: Comprobación de directorios de AppLocker* de este documento, con el fin de evitar que los nuevos ficheros y directorios generados por la aplicación instalada permitan a un usuario estándar ejecutar aplicaciones no permitidas.

4.2 USUARIO ESTÁNDAR

4.2.1. ACTIVIDAD I: AUTENTICACIÓN

Para acceder a los distintos componentes de la tableta primero hay que autenticarse. A continuación se describen los sistemas de autenticación propios del usuario estándar:

a. Autenticación de arranque del sistema, BitLocker.

Tras encender la tableta saltará la pantalla de autenticación de BitLocker, en la se escribirá la frase de paso correspondiente. Dicha pantalla mostrará un teclado en pantalla cuando se pulse en el campo para escribir la frase.

b. Autenticación en Windows.

Tras realizar la autenticación en BitLocker, la tableta cargará el sistema operativo, y como consecuencia, la pantalla principal de autenticación de Windows, en la que el usuario deberá mantener pulsado el botón con la etiqueta **P1**, colocado a la derecha de la pantalla de la tableta, con el fin de acceder a la pantalla de ingreso de credenciales.

4.2.2. ACTIVIDAD II: REGISTROS DE AUDITORÍA

Para acceder a los registros de auditoría se hará uso de la herramienta *Visor de eventos*. Para ejecutarla se hará uso del comando *eventvwr*.

Para administrar un registro desde dicha herramienta, se hará clic derecho sobre el mismo con el fin de acceder al menú contextual que permite exportarlo y/o importarlo.

4.2.3. ACTIVIDAD III: BLOQUEO Y DESBLOQUEO DE SESIÓN

Para bloquear la sesión se hará uso de la combinación de teclas *Windows + L* o bien de la función *Bloquear* accesible desde la combinación de teclas *CTRL + ALT + SUPR*.

Por otro lado, para desbloquear la sesión, se mantendrá pulsado el botón con la etiqueta **P1**, colocado a la derecha de la pantalla de la tableta, para acceder a la pantalla de autenticación, en la que se ingresarán las credenciales.

5. LISTADO DE REFERENCIAS

Esta sección contiene el listado de las referencias utilizadas en este documento:

[CCN-STIC-559B]	Implementación De Seguridad Sobre Microsoft Windows 10 (Cliente Independiente)
[CCN-STIC-512]	Gestión de Actualizaciones de Seguridad
[CCN-STIC-409A]	Colocación de etiquetas de seguridad

Tabla 2. Referencias.

6. LISTADO DE ACRÓNIMOS

En la siguiente tabla se listan los acrónimos utilizados en este documento:

Acrónimo	Descripción
CCN	Centro Criptológico Nacional
FIPS	Federal Information Processing Standard
HDMI	High-Definition Multimedia Interface
LTSB	Long-Term Servicing Branch
NTP	Network Time Protocol
SSD	Solid State Drive
STIC	Seguridad de las Tecnologías de la Información y Comunicaciones
TPM	Trusted Platform Module - Módulo de Plataforma Segura
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
WSUS	Windows Server Update Services

Tabla 3. Listado de acrónimos.

ANEXO A. DIRECTORIOS Y FICHEROS PARA BLOQUEAR EN APPLOCKER

En la tabla a continuación se lista cada uno de los ficheros y directorios a bloquear mediante AppLocker durante las actividades correspondientes:

Regla en la que se aplica	Tipo	Ruta del elemento
Reglas ejecutables	Ficheros	C:\Windows\System32\bdechangepin.exe
		C:\Windows\System32\bcdboot.exe
		C:\Windows\System32\BdeHdCfg.exe
		C:\Windows\System32\bitsadmin.exe
		C:\Windows\System32\bootcfg.exe
		C:\Windows\System32\bootsect.exe
		C:\Windows\System32\certutil.exe
		C:\Windows\System32\cipher.exe
		C:\Windows\System32\cmdkey.exe
		C:\Windows\System32\credwiz.exe
		C:\Windows\System32\dxdiag.exe
		C:\Windows\System32\esentutl.exe
		C:\Windows\System32\Fondue.exe
		C:\Windows\System32\label.exe
		C:\Windows\System32\makecab.exe
		C:\Windows\System32\manage-bde.exe
		C:\Windows\System32\mobsync.exe
		C:\Windows\System32\msiexec.exe
		C:\Windows\System32\msra.exe
		C:\Windows\System32\mstsc.exe
		C:\Windows\System32\netcfg.exe
		C:\Windows\System32\netstat.exe
		C:\Windows\System32\netsh.exe
		C:\Windows\System32\odbcad32.exe
		C:\Windows\System32\odbcconf.exe
		C:\Windows\System32\rekeywiz.exe
		C:\Windows\System32\repair-bde.exe
		C:\Windows\System32\schtasks.exe
		C:\Windows\System32\wevtutil.exe
		C:\Windows\System32\xwizard.exe
		C:\Windows\System32\bcdedit.exe
		C:\Windows\System32\cacls.exe
		C:\Windows\System32\chkdsk.exe
		C:\Windows\System32\Dism.exe
		C:\Windows\System32\expand.exe
		C:\Windows\System32\extract32.exe

		C:\Windows\System32\fsutil.exe
		C:\Windows\System32\getmac.exe
		C:\Windows\System32\icacls.exe
		C:\Windows\System32\msconfig.exe
		C:\Windows\System32\msinfo32.exe
		C:\Windows\System32\nslookup.exe
		C:\Windows\System32\regsvr32.exe
		C:\Windows\System32\runas.exe
		C:\Windows\System32\sc.exe
		C:\Windows\System32\services.exe
		C:\Windows\System32\sethc.exe
		C:\Windows\System32\sfc.exe
		C:\Windows\System32\slui.exe
		C:\Windows\System32\taskkill.exe
		C:\Windows\System32\tasklist.exe
		C:\Windows\System32\wbem\WMIC.exe
Reglas ejecutables y Reglas DLL	Directorios	C:\Windows\System32\spool\drivers\color\
		C:\Windows\Registration\CRMLog\
		C:\Windows\servicing\Packages\
		C:\Windows\servicing\Sessions\
		C:\Windows\Temp\
		C:\Windows\tracing\

Tabla 4: Directorios y ficheros para bloquear en AppLocker.