centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1609

Procedimiento de Empleo Seguro
GETAC F110G7 + firmware GETAC 16.1.32.2418

Julio 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 09:34:21 +02'00'

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

1. La tableta GETAC modelo F110G7 y firmware GETAC 16.1.32.2418, 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.

2. Las especificaciones del hardware del TOE son:

Elemento		Especificación
CPU		13th Gen - Intel® Core™ i7-1355U @ 1.70GHz
Firmware		Phoenix, Flash EEPROM, UEFI, soporte TPM, vPro, NIST, Absolute DDS, Herramienta de eliminación de seguridad, autodiagnósticos de la BIOS, Device Guard & Credential Guard, Paso a través de dirección MAC, ACPI, AMT12, y WMI
RAM		8 DDR5 SO-DIMM
Video	Controladora	Intel® UHD Graphics
	Controladora	LCD TFT de 11,6" 16:9, FHD 1920x1080, modo de dimmer, modo de apagón, poder leer a la luz del sol, brillo estándar 1200 nits, antirreflectante
Pantalla tactil		Pantalla multitáctil capacitiva de 10 puntos
Audio	Características	Audio de Alta Definición
	Altavoz	Interno x 1
	Micrófono	Interno x 2, Mic Array
Disco duro		PCIe SSD (Solid-State Drive - unidad de estado sólido), 256GB, extraíble por el usuario
Puertos E/S	Estándar	USB 3.2 Gen 2, USB-C Thunderbolt 4, audio combinado (4- pole TRRS 3,5mm), Docking
	Opcional	Arriba: RS232
Wireless LAN + BT		Intel® WiFi 6E AX211 + Bluetooth 5.3 combo
GPS		Discrete GPS
Cámara		Frontal: Resolución de 5MP, sensor de infrarrojos (opcional) Inferior: Resolución de 8MP, enfoque automático, LED, captura de vídeo
Seguridad		Candado Kensington, TPM 2.0
Energía	Adaptador corriente	65 W universal; entrada: 100-240 VAC, 50/60 Hz; salida: 19 V
	Batería x2	Batería estándar: Litio-ion prismático, 3 celdas Batería de alta capacidad: Litio-ion prismático, 6 celdas
Dimensiones		314 x 207 x 25mm (12.4 × 8.15 × 0.98 inch)
Peso		1.55 kg (3.3 lb)
Condiciones medioambientales	**Temperatura**	Funcionamiento: -29 °C ~ 63 °C (-20 °F ~ 145 °F) Almacenamiento: -51 °C ~ 71 °C (-60 °F ~ 160 °F)
	Humedad	95% humedad relativa, sin condensación

	Caída	Resistente a caídas de 1,8 m (6 ft)

Tabla 1: Especificaciones del hardware del TOE.

3. El sistema operativo de la tableta es Windows 11 IoT Enterprise 24H2 LTSC.
4. Los datos almacenados en el dispositivo están protegidos mediante el cifrado de disco, utilizando la propia herramienta que proporciona el sistema operativo, BitLocker.
5. El dispositivo ofrece un arranque seguro mediante la tecnología *Secure Boot* del firmware UEFI.

2 OBJETO Y ALCANCE

6. El objeto del presente documento consiste en definir dos manuales para el dispositivo GETAC F110G7:
    a) Un manual de configuración segura, sección 6 FASE DE CONFIGURACIÓN, el cual describe las actividades a llevar a cabo por el usuario administrador para realizar una configuración segura de la tableta.
    b) Un manual de empleo seguro, sección 7 FASE DE EMPLEO SEGURO, en el que se definen las actividades que permiten realizar un empleo seguro de la tableta para los usuarios administradores y usuarios estándar
7. El producto GETAC F110G7 ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del [**CPSTIC**].
8. Por último, se incluyen las referencias, acrónimos, e índices de figuras y tablas utilizados en la redacción del documento.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
d) Apartado 7. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de empleo seguro del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Dado que el producto evaluado corresponde a un dispositivo hardware (appliance), se establece el siguiente procedimiento para garantizar la **recepción segura del equipo** y verificar que no ha sido manipulado durante el transporte o almacenamiento previo a su instalación.

4.1.1 RECEPCIÓN INICIAL DEL ENVÍO

10. A la llegada del envío, el personal responsable de la recepción deberá verificar que el paquete corresponde al pedido realizado.
11. Se comprobará que el número de paquetes recibidos coincide con el indicado en la documentación de transporte o albarán.
12. Se registrará la fecha de recepción, el proveedor y la persona responsable de la recepción.

4.1.2 VERIFICACIÓN DEL EMBALAJE EXTERNO

13. Se inspeccionará visualmente el **embalaje externo** del dispositivo.
14. Se comprobará que:
    a) La caja no presenta golpes, deformaciones, perforaciones o signos de apertura.
    b) No existen cortes en las cintas adhesivas originales del fabricante.
    c) No hay indicios de manipulación, sustitución o reembalaje.
15. En caso de observar daños o indicios de manipulación:
    a) Se documentará mediante fotografías.
    b) Se notificará inmediatamente al responsable del proyecto o de seguridad.
    c) No se procederá a la instalación hasta aclarar la incidencia con el proveedor.

4.1.3 VERIFICACIÓN DEL EMBALAJE INTERNO

16. Una vez validado el embalaje externo:
    a) Se procederá a la apertura del paquete.
    b) Se comprobará que el **embalaje interno** se encuentra intacto y correctamente protegido mediante los materiales de protección del fabricante (espumas, separadores, bolsas protectoras, etc.).
    c) Se verificará que:
        i. El dispositivo está correctamente alojado en su embalaje.
        ii. No existen signos de manipulación o apertura previa.
        iii. Todos los componentes están debidamente protegidos.

4.1.4 VERIFICACIÓN DE SELLOS Y ETIQUETAS DE GARANTÍA

17. Se revisará que los **sellos de garantía del fabricante** no estén rotos o manipulados.
18. Se comprobará que las **etiquetas de seguridad y números de serie** del dispositivo están presentes y son legibles.
19. Se verificará que el número de serie coincide con el indicado en la documentación de compra o entrega.

4.1.5 REGISTRO DE LA RECEPCIÓN

20. Finalmente, se documentará el resultado del proceso de verificación, incluyendo:
    a) Fecha de recepción.
    b) Identificación del equipo (modelo y número de serie).
    c) Resultado de las comprobaciones de embalaje y sellos.
    d) Nombre del responsable que realiza la verificación.
21. Este registro se conservará como evidencia del proceso de **recepción segura del equipo previo a su instalación o puesta en funcionamiento**.

4.2 CONSIDERACIONES PREVIAS

22. Esta sección describe las actividades a llevar a cabo para realizar una configuración segura de la tableta GETAC F110G7. Dichas actividades deben realizarse en el orden establecido para asegurar un correcto funcionamiento del producto.
23. Los drivers, firmware y sistema operativo de la tableta se encuentran actualizados a la última versión aprobada.
24. 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.

5 FASE DE INSTALACIÓN

25. El dispositivo **Getac F110 G7** no requiere un proceso de instalación previo para su puesta en funcionamiento.
26. Una vez realizadas las comprobaciones de recepción descritas anteriormente, el equipo puede ponerse en marcha mediante el encendido del dispositivo. Tras iniciar la tablet, se podrá proceder directamente a la **fase de configuración del sistema**, en la que se realizarán los ajustes iniciales necesarios para su uso.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

6.1.1 CONFIGURACIÓN DEL FIRMWARE UEFI

27. En primer lugar, 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
```

28. Tras esto, se iniciará la pantalla de recuperación de Windows, desde la que seleccionaremos la opción *Solucionar problemas – Opciones avanzadas - Configuración de firmware UEFI – Reiniciar* con el fin de acceder a la configuración de UEFI.
29. 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.
30. 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:
        i. Establecemos la contraseña de administrador mediante el parámetro *Set Supervisor Password.*

           Nota: es necesario establecer la contraseña de administrador para desbloquear el resto de los parámetros configurados en esta pestaña, como por ejemplo la política de contraseña, el arranque seguro, etc.
        ii. Activamos la opción *Strong Password* que establece que la contraseña debe contener al menos una mayúscula, una minúscula y un digito.
        iii. Establecemos la longitud mínima de la contraseña en **12 caracteres**[1] según el parámetro *Password Configuration.*
    c) En la pestaña **Boot** desactivamos todos los elementos del inicio excepto Hard Disk Drive.

[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.

31. 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.
32. 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.

6.1.2 DESINSTALACIÓN DE APLICACIONES

33. Para empezar, accedemos a Panel de Control → Programas y procedemos a desinstalar las siguientes aplicaciones instaladas de serie por el fabricante
    a) Getac Utility
    b) Getac KeyWedgeUtility
    c) Conexión a Escritorio remoto
    d) Herramienta de recortes
    e) Microsoft 365 Apps for enterprise
    f) Microsoft OneNote
    g) Paint

    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.
34. A continuación, se muestran unas capturas del proceso:

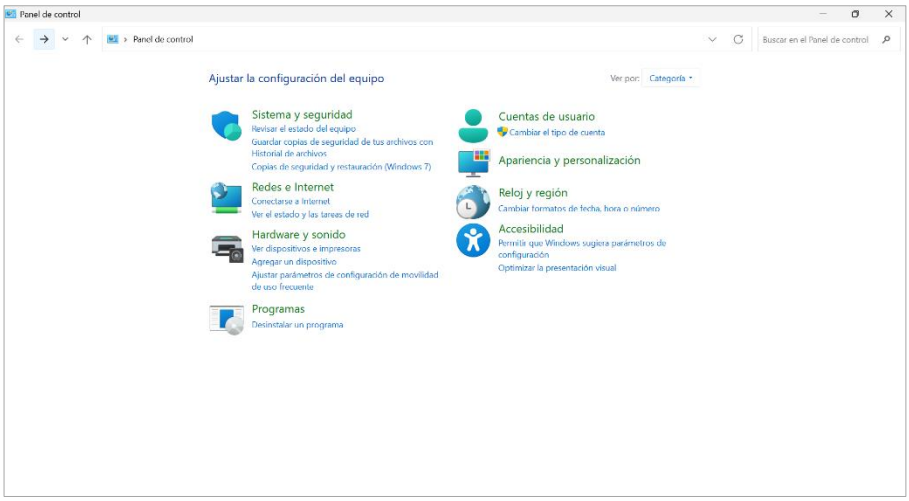

Figura 1: Desinstalar aplicaciones predeterminadas - 1.

Nombre	Editor	Se instaló el	Tamaño	Versión
Componentes del Motor de administración Intel®	Intel Corporation	06/05/2025	150 MB	2413.5.68.0
Conexión a Escritorio remoto	Microsoft Corporation	07/05/2025		
Getac Driving Safety Utility	Getac Technology Corporation	07/05/2025	4,63 MB	1.4.1.2
Getac Geolocation 2.0.0.21	Getac Technology Corporation	06/05/2025		2.0.0.21
Getac Utility 30.0.161.0	Getac Technology Corporation	06/05/2025		30.0.161.0
GetacKeyWedgeUtility	Getac Technology Corporation	07/05/2025	13,1 MB	2.1.9.0
Herramienta Recortes	Microsoft Corporation	07/05/2025		
Microsoft 365 Apps for enterprise - en-us	Microsoft Corporation	06/05/2025		16.0.17328.20206
Microsoft Edge	Microsoft Corporation	06/05/2025		136.0.3240.50
Microsoft OneNote - en-us	Microsoft Corporation	06/05/2025		16.0.17328.20206
Paint	Microsoft Corporation	07/05/2025		

Figura 2: Desinstalar aplicaciones predeterminadas - 2.

6.1.3 APLICACIÓN DE LA GUÍA [CCN-STIC-599AB23]

35. Se deben seguir los pasos de implementación de la guía [**CCN-STIC-599AB23**], **ANEXO B** CONFIGURACIÓN SEGURA DE CLIENTES WINDOWS INDEPENDIENTES. De este ANEXO B solo se deben aplicar los **ANEXOS B.1.** PASO A PASO DE CONFIGURACIÓN BASE DE SEGURIDAD SOBRE CLIENTES INDEPENDIENTES, del **ANEXO B.2.** CONFIGURACIONES ADICIONALES se aplicarán los siguientes puntos **(B.2.3, B.2.3.2, B.2.5 y B.2.7)** y **ANEXO B.3.3.** PROTECCIÓN FRENTE A CÓDIGO DAÑINO (CONFIGURACIÓN DE LA HERRAMIENTA DE DETECCIÓN DE CÓDIGO DAÑINO**)** teniendo en cuenta las siguientes cuestiones.

36. Puede ocurrir que, al tratar de ejecutar los scripts incluidos en la guía, aparezca un error de tipo “UnauthorizedAccess” durante la ejecución. Si esto ocurre, se debe desbloquear la ejecución haciendo **Click derecho > “Propiedades” > Desbloquear** en el apartado Security de cada uno de ellos.

37. Durante la realización de los pasos de la guía, con el editor de plantillas de seguridad abierto (gpedit.msc), se debe modificar la plantilla de seguridad [**CCN-STIC-599AB23**] **Servicios** (Servicios del sistema) con el fin de habilitar en modo *Automático* los siguientes servicios:

    a) Conexiones de red.

    b) Configuración automática de WLAN.

    c) Identidad de aplicación.

    d) Servicio de compatibilidad con Bluetooth.

    e) Servicio de configuración de red.

    f) Servicio de geolocalización.

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

    h) Servicio de sensores.

    i) Servicio de supervisión de sensores.

    j) Servicio Seguridad de Windows2.

    k) Servicio Antivirus de Microsoft Defender.

    l) Servicio Cifrado de unidad Bitlocker

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

38. A continuación, 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).

    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).

39. En el paso 3 del Anexo B.1.2.1. a la hora de ejecutar el archivo "CCN-STIC-599B23 Cliente Independiente – Paso 1 – Servicios.bat" es posible que nos aparezca un error de tipo **Acceso denegado**, al intentar cambiar el tipo de inicio de alguno de los servicios. Este error aparece escrito al final del todo en el archivo "servicios_windows.log" que se genera. El error es el siguiente "Acceso denegado. La tarea se ha completado con un error". Si nos surge este error debemos realizar los siguientes pasos para solucionarlo.

    a) En primer lugar, es necesario comparar el tipo de Inicio de los servicios en nuestro dispositivo, con el tipo de Inicio que deberían tener según la guía. Para hacer esto accedemos al archivo "C:\Scripts\Materias Clasificadas\CCN-STIC-599B23 Incremental Servicios (Materias Clasificadas).inf", en este archivo se puede comparar la configuración de inicio de cada servicio, en la tabla 2 del apartado 4.2 se puede encontrar una explicación de cada inicio con su número asociado.

    b) A continuación, debemos abrir el administrador de servicios del sistema, para hacer esto escribimos "services.msc" en el buscador de Windows y abrimos el programa.

    c) Una vez tenemos ambos (el archivo y el administrador de servicios) abiertos, debemos ir comprobando que el tipo de Inicio de nuestros servicios es igual al que se estipula en el archivo, salvo los servicios que hemos modificado en el punto 37 de esta guía, donde hemos cambiado la plantilla y hemos puesto algunos servicios en Inicio Automático), estos servicios en el archivo aparecerán con otro tipo de

Inicio pero debemos dejarlos en modo Automático. Si alguno de nuestros servicios no tiene el mismo tipo Inicio que en el archivo, hacemos doble clic sobre el servicio y lo cambiamos al tipo de Inicio que debería tener. Existe la posibilidad de que al intentar cambiar el tipo de Inicio de estos servicios obtengamos un error de **Acceso denegado**, si nos ocurre esto debemos seguir los pasos que se explican a continuación. Una vez todos los servicios en nuestro dispositivo se encuentren con el mismo tipo de Inicio que en la tabla, podemos seguir a delante con la aplicación de la guía.

d) En este apartado, se van a explicar los pasos a seguir en el caso de que no se haya podido cambiar el tipo de Inicio de algún servicio. Si no es esta la situación, se debe ignorar este apartado.

   i. Lo primero que debemos hacer es comprobar que tenemos abiertos tanto el archivo de comprobación de los servicios como la aplicación "services.msc", tal y como se ha explicado en los apartados a) y b).

   ii. A continuación, procederemos a editar manualmente el servicio o servicios que nos han dado el error. Para hacer esto, abrimos el Editor de Registros desde Powershell con permisos de administrador (escribimos "regedit.exe" en la Powershell). Dentro de la aplicación, escribimos la siguiente dirección: "Equipo\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services*". Donde el "*" en esta dirección simboliza el nombre del servicio que queremos editar, este nombre lo obtenemos abriendo las propiedades del servicio, dentro de la pestaña de General. Una vez tengamos el servicio abierto con todas sus características, nos desplazamos hasta la propiedad "Start" del servicio y hacemos doble clic. A continuación, debemos editar el valor de Inicio, acorde con el que se estipula en la siguiente tabla. Para hacer esto, debemos seguir la siguiente tabla que asocia el valor numérico que debemos escribir con el tipo de inicio deseado.

   Nota: Al registro de WinDefend no se le puede cambiar el tipo de inicio, por lo que lo dejaremos en automático

Información del valor	Tipo de inicio
2	Automático
3	Manual
4	Deshabilitado

Tabla 2: Valores de registro para el tipo de Inicio del proceso.

   iii. Una vez hayamos cambiado el valor de Inicio, volvemos a la aplicación de Servicios y actualizamos los servicios pulsando F5, buscamos el servicio que hemos modificado y comprobamos que su tipo de inicio es el mismo que el tenemos en el archivo. Realizamos este mismo proceso para todos los servicios que nos den el error estipulado en el apartado anterior.

   iv. Existe la posibilidad de que no encontremos el servicio que estamos buscando desde la tabla en el administrador de servicios de nuestro dispositivo. Esto se debe a que el servicio, o ya no existe, o ha cambiado de nombre. Si nos encontramos con esta situación debemos acceder al

registro y desplazarnos a la siguiente dirección: "Equipo\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services*". En este caso el "*" simboliza donde se va a escribir el nombre corto del servicio, que podremos encontrar en la segunda columna de la tabla de comprobación de la guía STIC. Una vez hayamos hecho esto, y en caso de que la dirección exista, comprobaremos que el tipo de inicio establecido (ver Tabla 2) coincida con el estipulado en la guía STIC y, en caso de que no coincida, lo actualizaremos en consecuencia.

40. A la hora de realizar los pasos del Anexo B.2.4 se bloquearán todas las conexiones de entrada tanto TCP como UDP por lo que hay que crear una regla para cada uno con la misma configuración como se muestra a continuación en **gpedit.msc:**

    a) Despliegue el nodo: "**Directiva Equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Windows Defender Firewall con seguridad avanzada → Windows Defender Firewall con seguridad avanzada – Objeto de directiva de grupo local**", Clic derecho en Reglas de entrada y seleccionamos en el desplegable la opción Nueva regla:

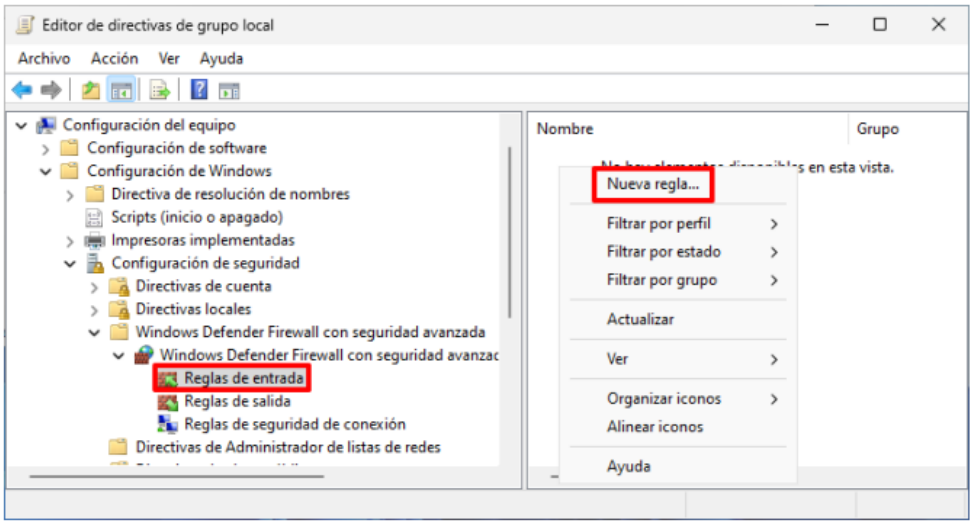

Figura 3: Configuración de regla firewall – 1.

    b) Seleccionamos el tipo de regla Puerto:

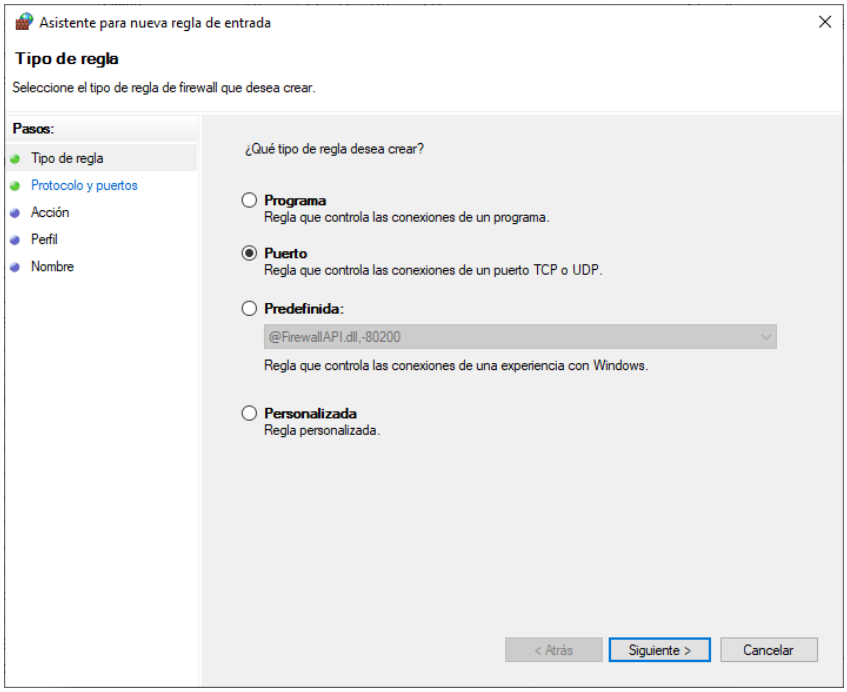

Figura 4: Configuración de regla firewall – 2.

c) Seleccionamos la opción TCP y Todos los puertos locales:

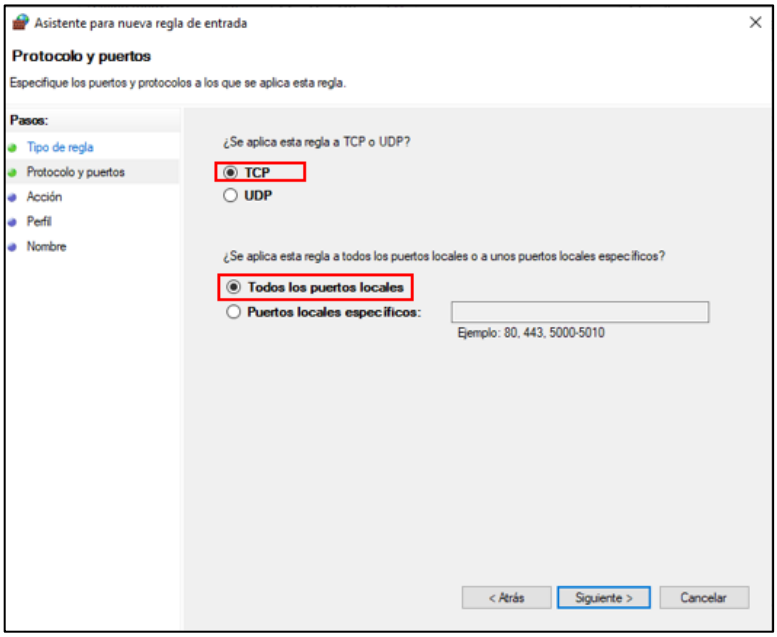

Figura 5: Configuración de regla firewall – 3.

d) Bloqueamos todas las conexiones:

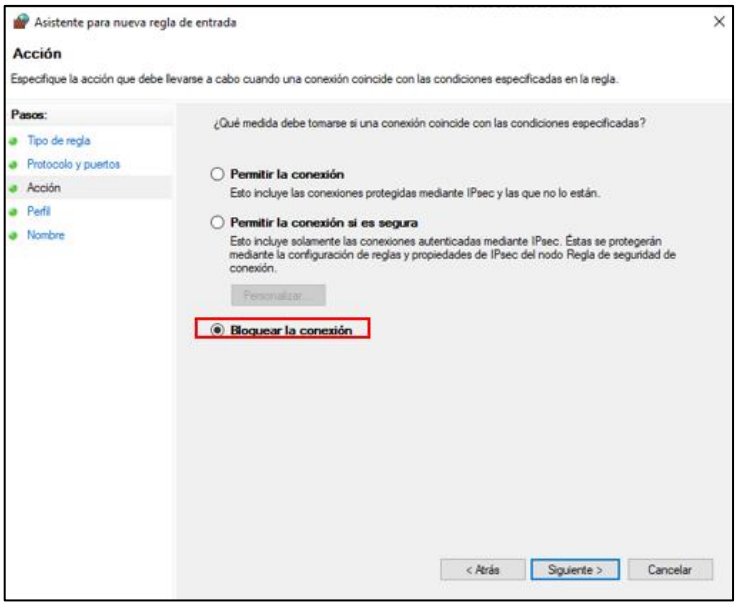

Figura 6: Configuración de regla firewall – 4.

e) Seleccionamos todo tipo de redes:

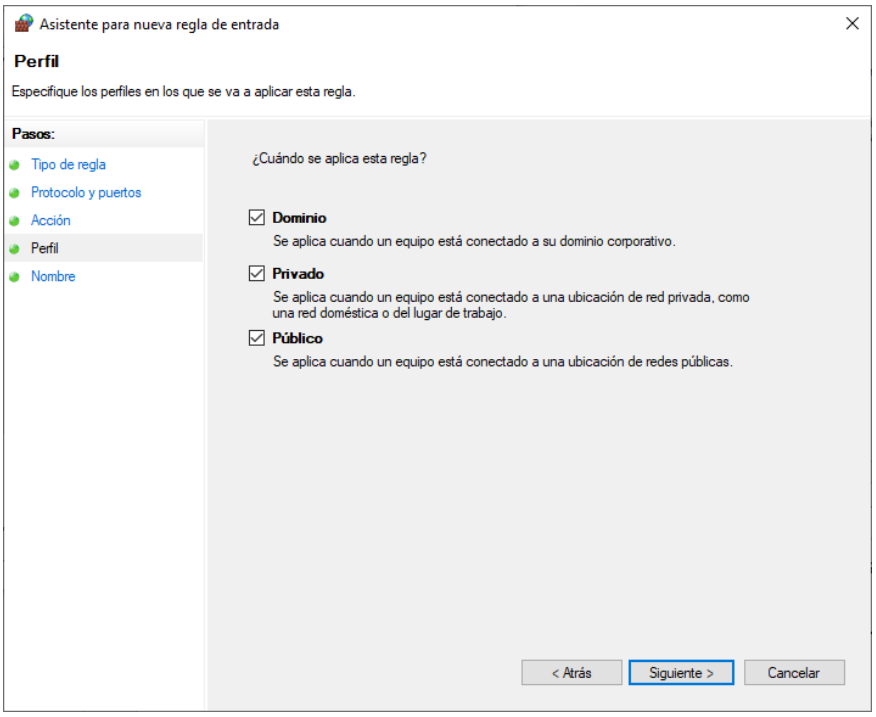

Figura 7: Configuración de regla firewall – 5.

41. 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 las credenciales. Para realizar dicha combinación de teclas en la tableta, que no tiene teclado, se mantendrá pulsado el botón **P2.**

6.1.4 CIFRADO DEL ALMACENAMIENTO INTERNO

42. Se seguirán los pasos descritos en la sección *ANEXO B.2.6 PROTECCIÓN DE DISPOSITIVOS PORTÁTILES* de la guía [**CCN-STIC-599AB23**]

    a) En caso de que se bloquee la escritura en un dispositivo extraíble al guardar la clave de recuperación, se tendrá que editar una política de **gpedit.msc.**

    b) Tras ejecutar el comando gpedit.msc con Win+R, nos dirigimos a **"Directiva Equipo local > Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Cifrado de unidad Bitlocker > Unidades de datos extraíbles"** y deshabilitamos la directiva **"Controlar el uso de Bitlocker en unidades extraíbles"**:

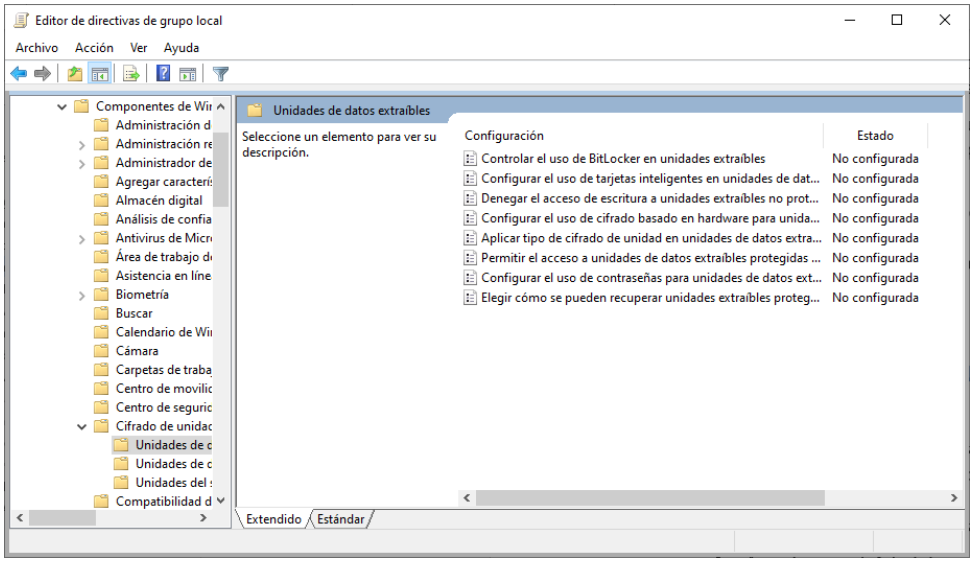

Figura 8: Directiva de unidades extraíbles – 1.

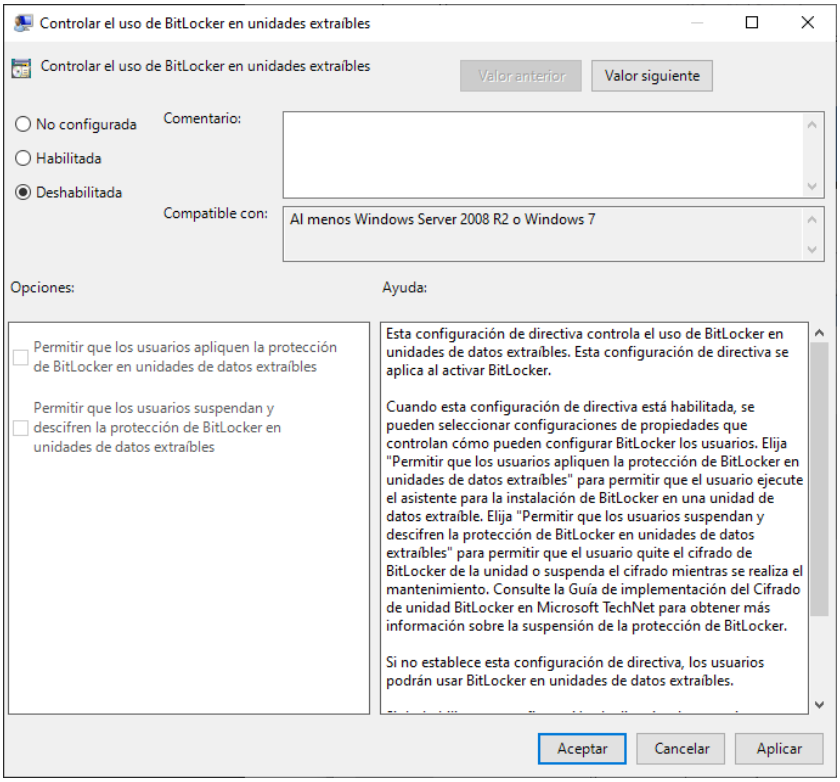

Figura 9: Directiva de unidades extraíbles – 2.

6.1.5 INSTALACIÓN GPS Y SENSORES

43. Debido a la configuración aplicada por la guía STIC, los sensores y el GPS de la tableta pueden quedar bloqueados por la política de grupo de Windows. Si se da este caso debemos desbloquear y asegurar el correcto funcionamiento de estos elementos. Si, por el contrario, los sensores y el GPS no están bloqueados, no es necesario realizar esta actividad.

    a) 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.*

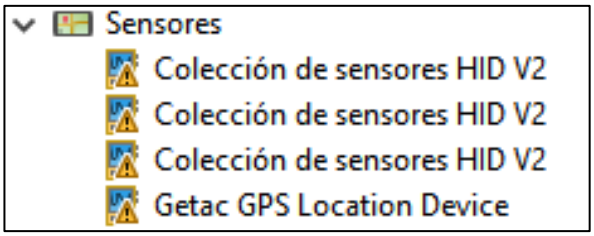

Figura 10: Administrador de dispositivos - Sensores y GPS.

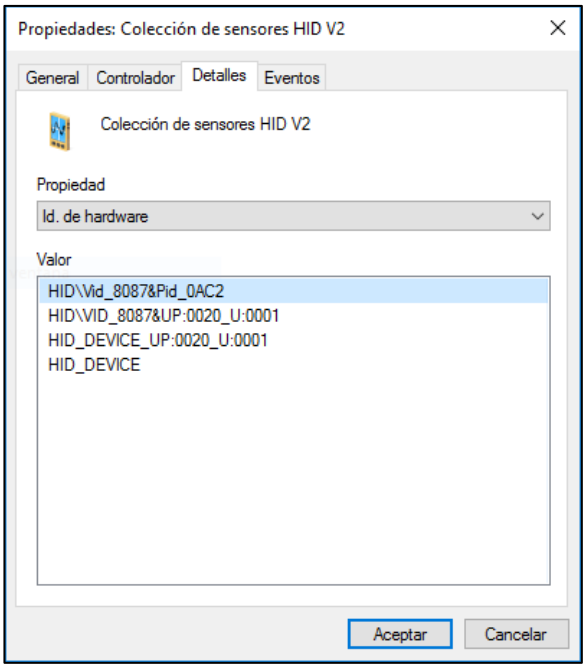

Figura 11: Id. de hardware del elemento.

b) 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 (tanto sensores como GPS), según el parámetro Configuración de Equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos → Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo.

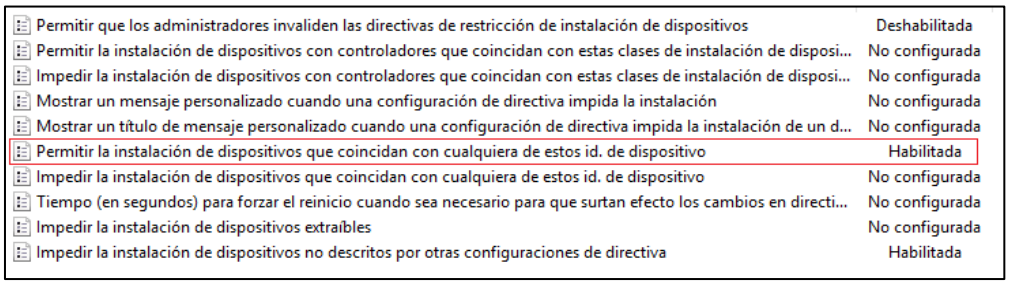

Figura 12: Habilitando dispositivos en la política de grupo - 1.

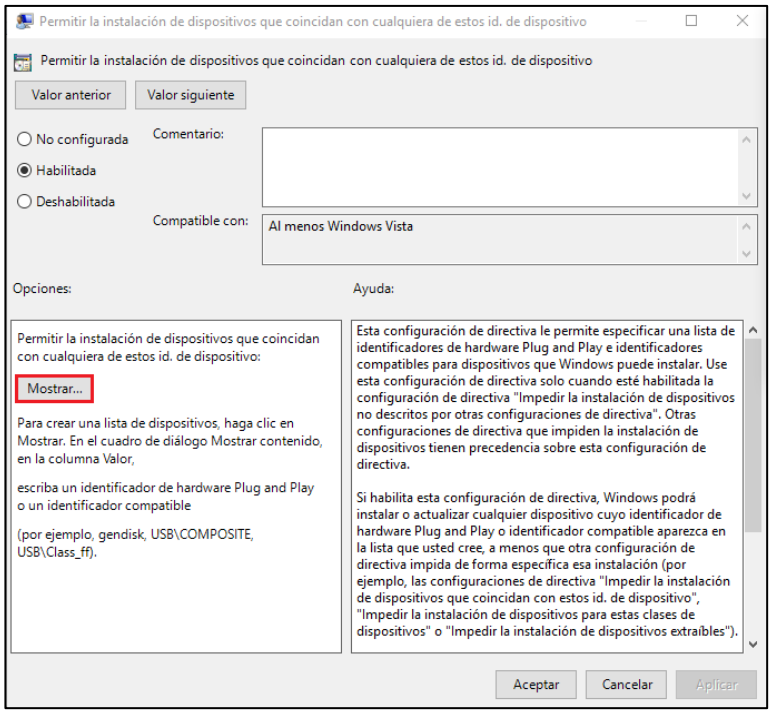

Figura 13: Habilitando dispositivos en la política de grupo - 2.

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

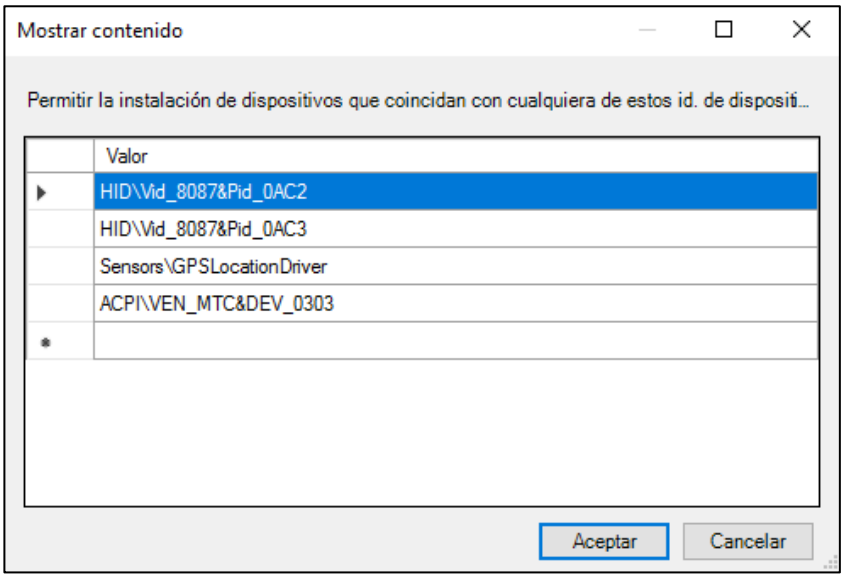

Figura 14: Habilitando dispositivos en la política de grupo - 3.

d) Desinstalamos cada uno de los dispositivos desde el administrador de dispositivos.

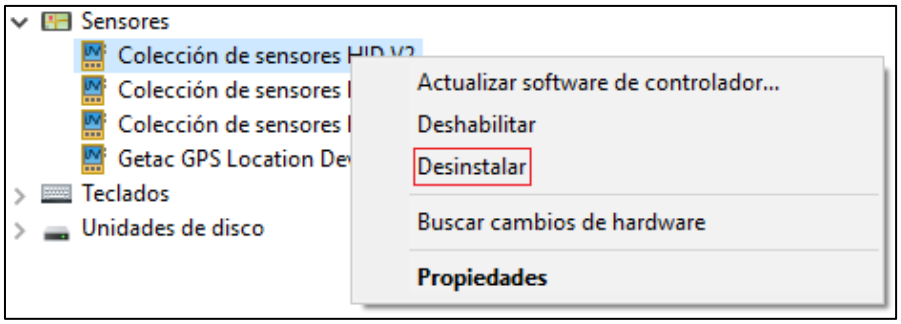

Figura 15: Desinstalando dispositivos.

e) Instalamos el driver Getac Geolocation.

Figura 16: Instalando driver *Getac Geolocation*.

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

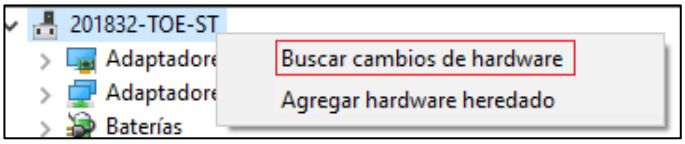

Figura 17: Buscando cambios de hardware.

6.1.6 ACTIVACIÓN DE LA UBICACIÓN

44. 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.

    a) Abrimos la aplicación *Configuración* desde la barra de tareas y hacemos clic en *Privacidad y seguridad*.

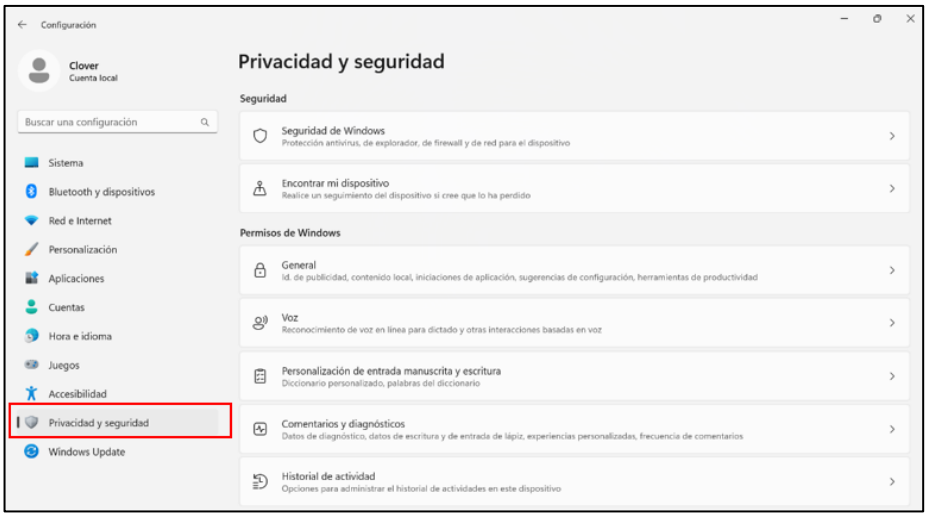

Figura 18: Activando ubicación - 1.

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

Figura 19: Activando ubicación - 2.

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

Figura 20: Activando ubicación - 3.

Figura 21: Ubicación activada.

45. Existe la posibilidad de que no se nos permita cambiar la ubicación, como se muestra en la Figura 22. Si nos encontramos con este problema debemos realizar los siguientes pasos para solucionarlo:

    a) Escribimos en el buscador "gpedit.msc" e introducimos las credenciales para abrir el *Editor de directivas de grupo local*.

    b) Deshabilitamos la siguiente directiva: Configuración del equipo → Plantillas administrativas → Componentes de Windows → Ubicación y sensores → Desactivar ubicación.

    c) Reiniciamos el dispositivo.

    d) Realizamos los pasos que se han explicado al principio de esta actividad para activar la ubicación de este dispositivo (desde la Figura 18 hasta la Figura 21).

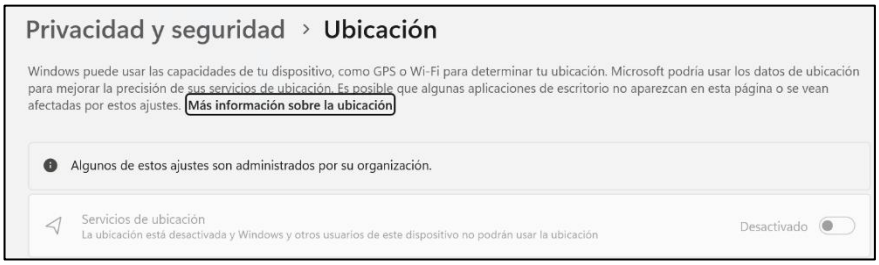

Figura 22: No se puede cambiar la ubicación

46. Si con esto no se hubiese solucionado debemos modificar los estados de las directivas igual que como muestra la Figura 17. Para hacer esto seguimos los siguientes pasos.

    a) Escribimos en el buscador "gpedit.msc" e introducimos las credenciales para abrir el *Editor de directivas de grupo local*.

    b) Accedemos al siguiente directorio: Configuración del equipo → Plantillas administrativas.

    c) Una vez aquí debemos hacer clic en **Ver** (opción que se encuentra arriba en el menú), cuando se abra esta opción hacemos clic en **Opciones de filtro…**

d) Se nos abre una pantalla donde vamos a poder filtrar las directivas por palabras. Para hacer esto cambiamos la sección de *Configurado* a **Sí**. Marcamos la opción de *Habilitar filtro de palabra clave* y dentro de *Filtrar por las palabras* escribimos: "ubicación", tal y como muestra la siguiente figura.

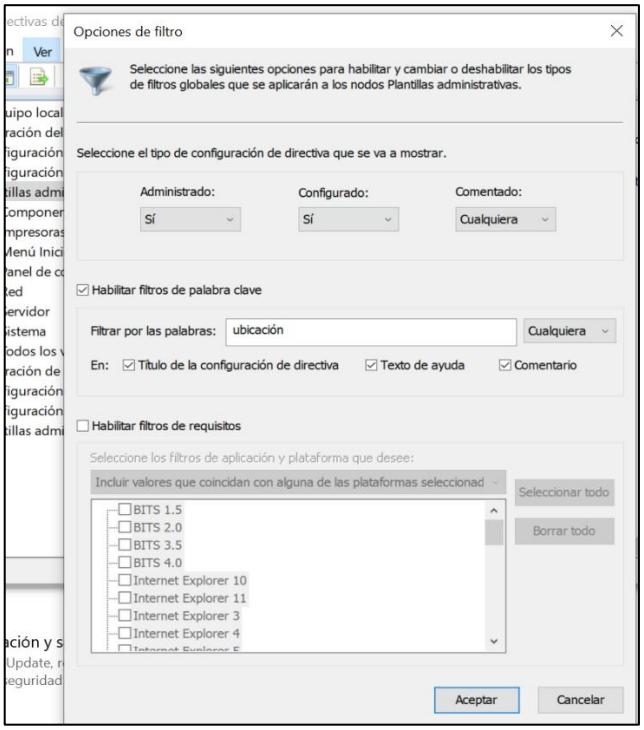

Figura 23: Configuración opciones de filtro

e) A continuación, dentro de la directiva de *Plantillas administrativas* tendremos una nueva subdirectiva llamada *Todos los valores*. Abrimos esta nueva directiva y comprobamos que el estado de cada directiva en nuestro dispositivo es igual a los que aparecen reflejados en la Figura 17, modificando aquellos que no lo sean.

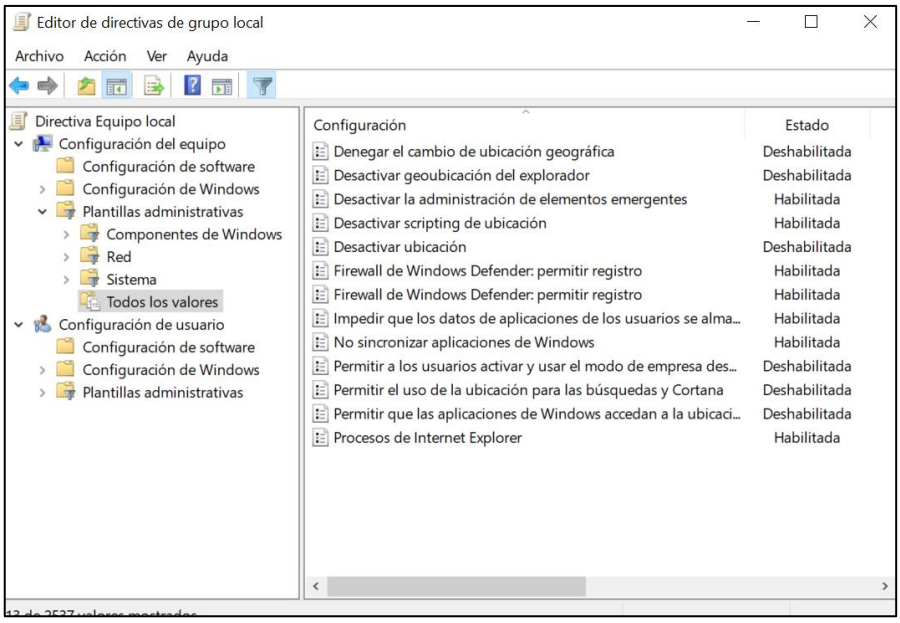

Figura 24: Estados de directivas

f) Reiniciamos el dispositivo.

g) Realizamos los pasos que se han explicado al principio de esta actividad para activar la ubicación de este dispositivo (desde la Figura 18 hasta la Figura 21).

6.1.7 CONFIGURACIÓN DE APPLOCKER

47. 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:

    a) 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.

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

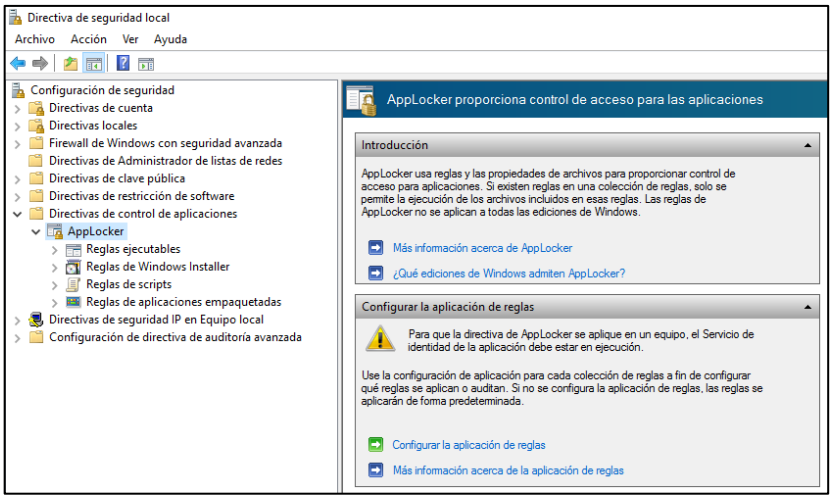

Figura 25: Directiva de seguridad local - AppLocker.

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

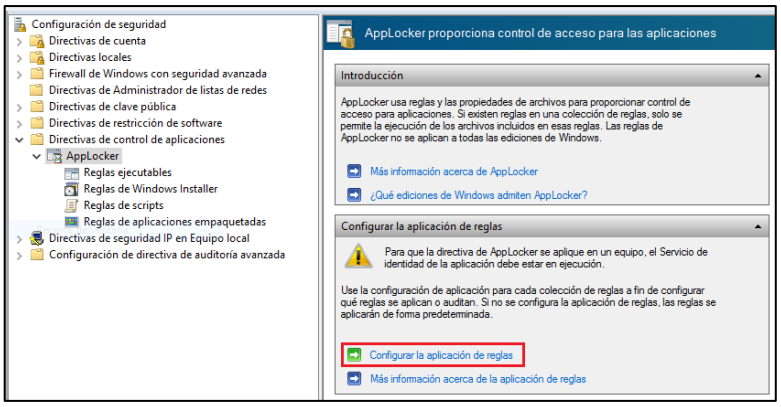

Figura 26: AppLocker – Habilitando las reglas de librerías - 1.

Figura 27: AppLocker – Habilitando las reglas de librerías - 2.

d) Creamos las reglas siguientes en cada uno de los tipos de reglas de AppLocker:

Reglas ejecutables (.exe)

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

ii. 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 el Anexo A: Directorios y ficheros para bloquear en AppLocker de este documento. Para ello se tendrán en cuenta los pasos descritos en la sección 6.4.3 Añadir excepciones en reglasde 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 28: AppLocker - Reglas ejecutables.

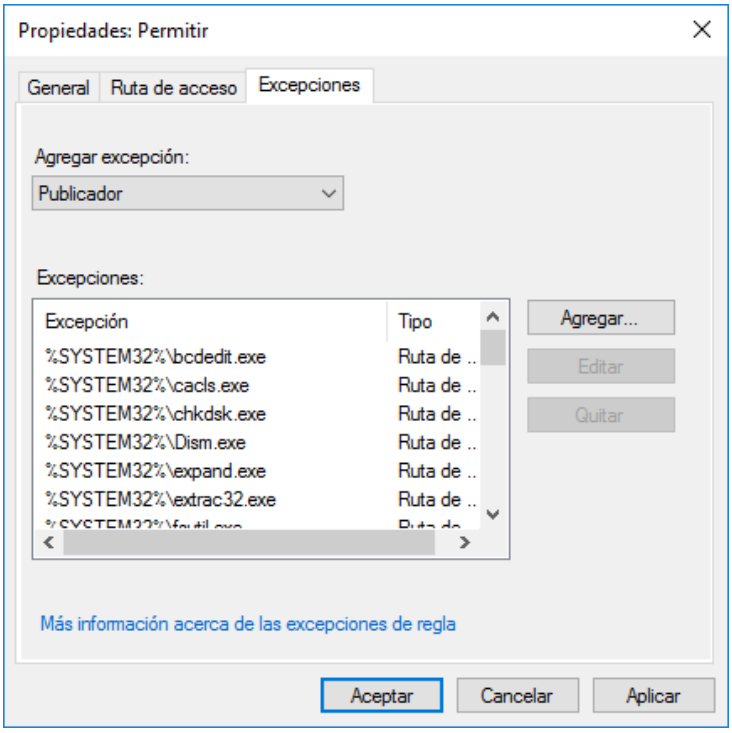

Figura 29: AppLocker - Reglas ejecutables - Excepciones de la regla *Todos los archivos de la carpeta Windows*.

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

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

ii. 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.

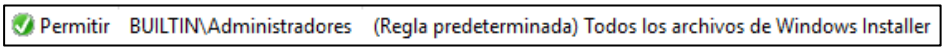

Figura 30: AppLocker - Reglas de Windows installer.

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

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

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

Figura 31: AppLocker - Reglas de scripts.

Reglas de DLL (.dll)

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

ii. Añadimos como *Excepciones* de tipo *Ruta de Acceso*, en la regla de nombre *DLL de Microsoft Windows*, los ficheros y directorios correspondientes indicados en la sección Anexo A: Directorios y ficheros para bloquear en AppLocker.Anexo A: Directorios y ficheros para bloquear en AppLocker de este documento. Para ello se tendrán en cuenta los pasos descritos en la sección 6.4.3 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 32: AppLocker - Reglas de DLL.

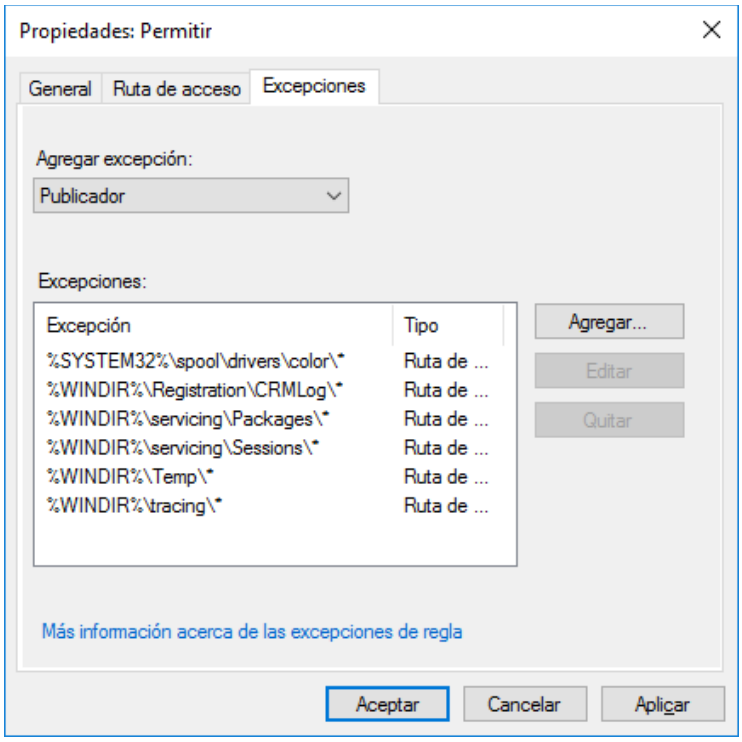

Figura 33: AppLocker - Reglas DLL - Excepciones de la regla Todos los archivos de la carpeta Windows.

Reglas de aplicaciones empaquetadas (aplicaciones universales Windows)

i. 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:

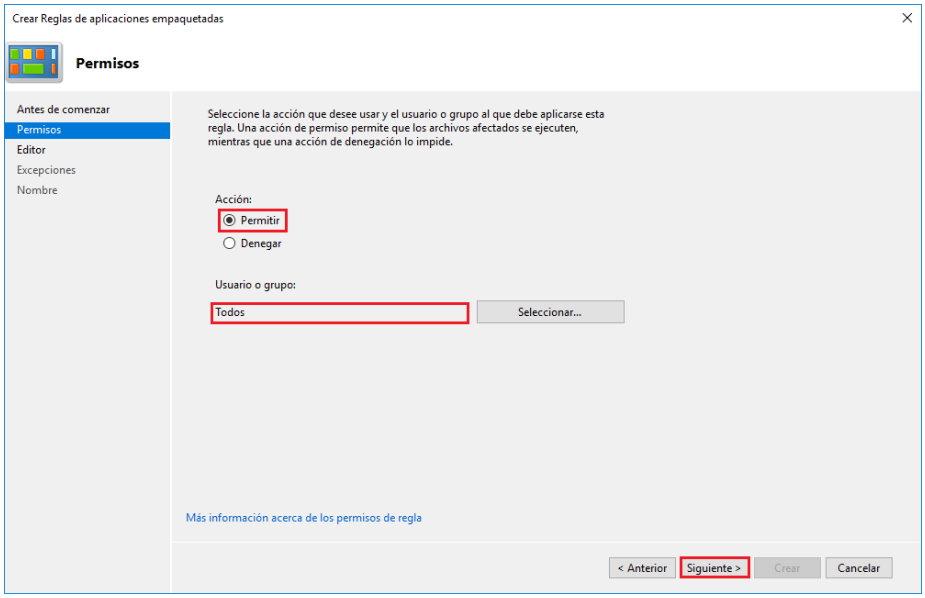

Figura 34: AppLocker - Creando regla de aplicaciones empaquetadas - 1.

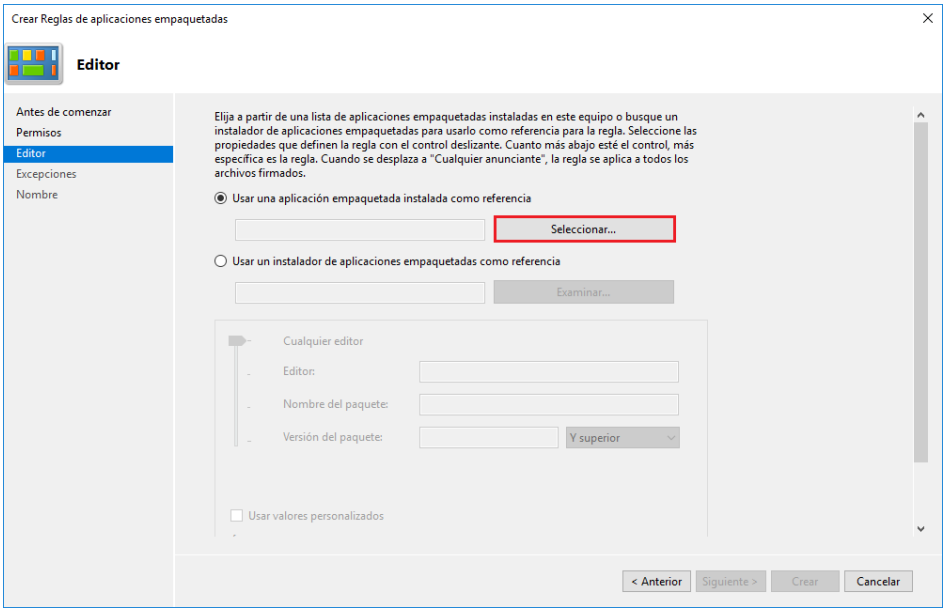

Figura 35: AppLocker - Creando regla de aplicaciones empaquetadas – 2.

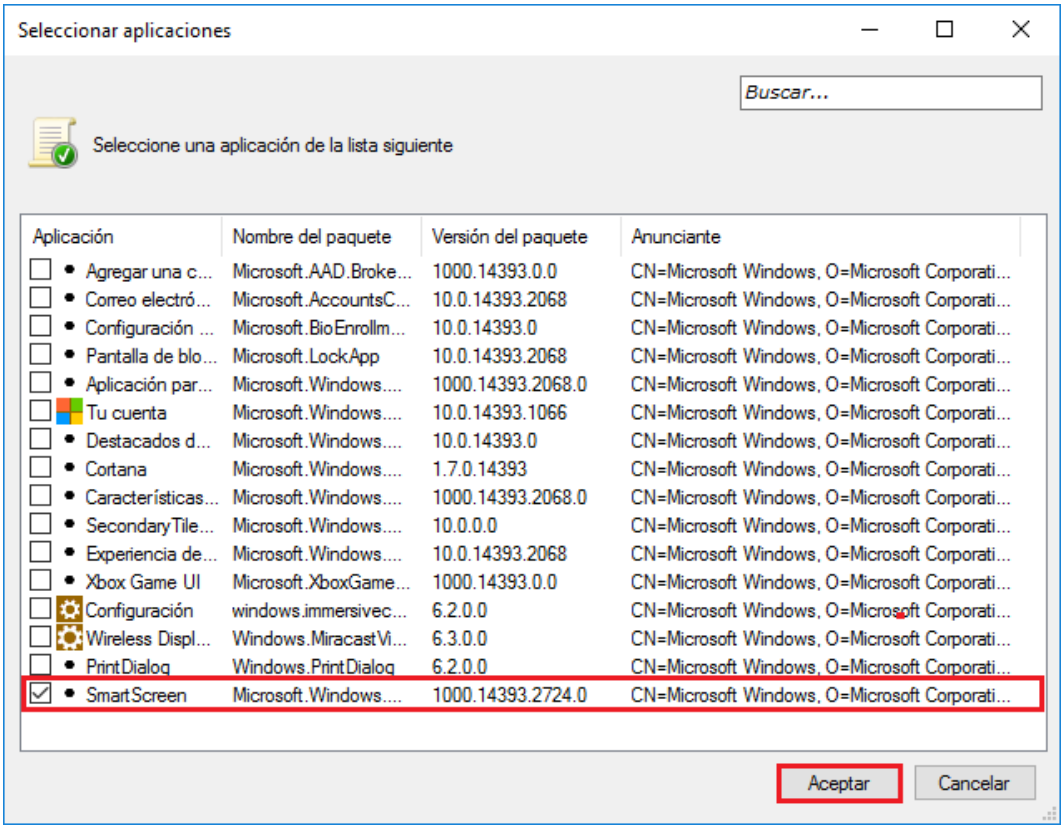

Figura 36: AppLocker - Creando regla de aplicaciones empaquetadas - 3.

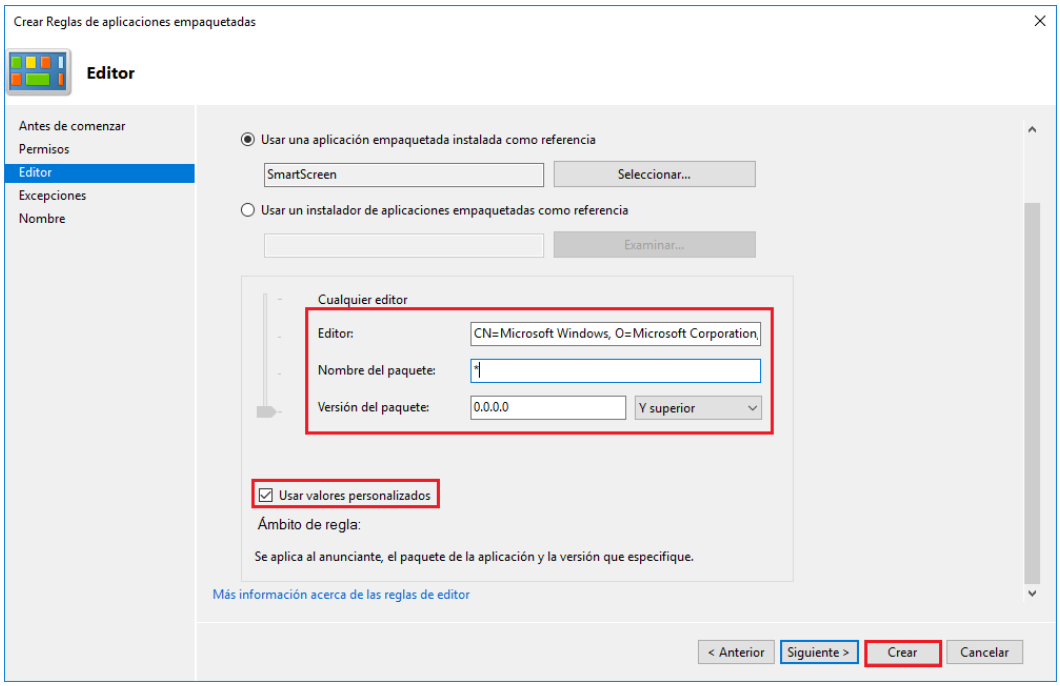

Figura 37: AppLocker - Creando regla de aplicaciones empaquetadas - 4.

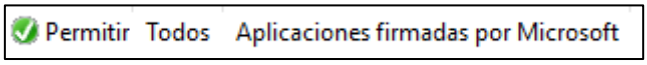

Figura 38: AppLocker - Reglas de Aplicaciones empaquetadas.

e) Tras crear las reglas, 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 39: AppLocker - Configurando aplicación de reglas - 1.

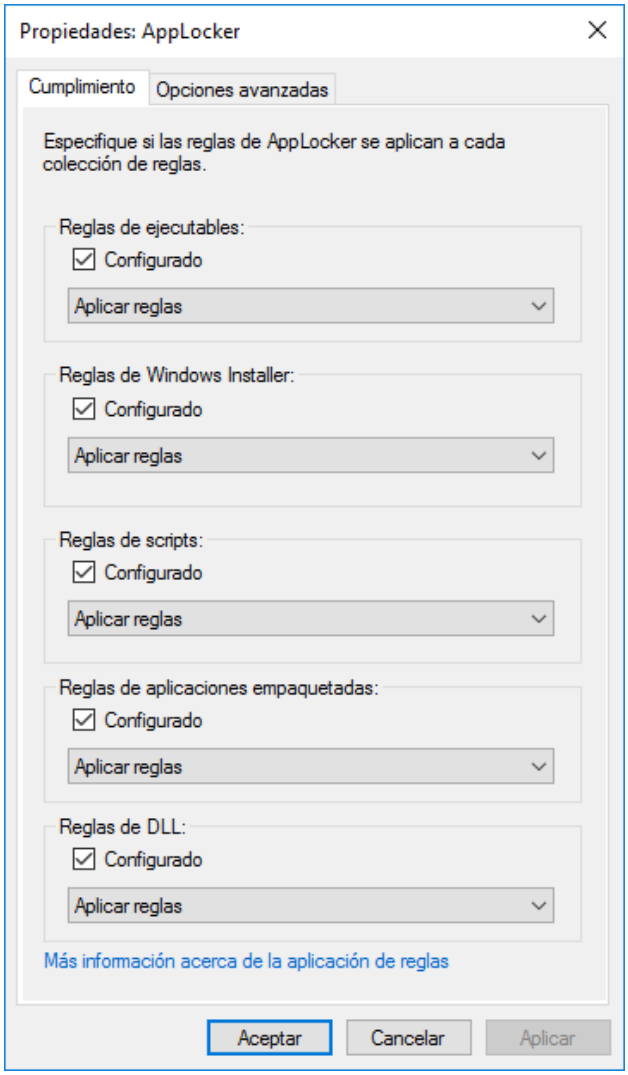

Figura 40: AppLocker - Configurando aplicación de reglas - 2.

f) 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.

48. 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 será descrito en la sección "**6.4.2 Exportar/Importar reglas**" de este documento.

6.1.8 HABILITAR TESTS CRIPTOGRÁFICOS

49. 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.

50. 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*.

6.1.9 SOFTWARE ANTIVIRUS

51. 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.

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

    a) Accedemos al editor de políticas de grupo de Windows mediante el comando gpedit.msc y deshabilitamos la política Configuración de Equipo → Plantillas administrativas → Componentes de Windows → Antivirus de Microsoft Defender → Protección en tiempo real → Desactivar protección en tiempo real

    b) Accedemos al editor de políticas de grupo de Windows mediante el comando gpedit.msc y deshabilitamos la política Configuración de Equipo → Plantillas administrativas → Componentes de Windows → Antivirus de Windows Defender → Desactivar Antivirus de Windows Defender

    c) Desde la configuración de Windows accedemos a la sección *de Privacidad y Seguridad*, una vez dentro abrimos la sección de *Seguridad de Windows*.

Figura 34: Seguridad de Windows

d) Hacemos clic en el área de Protección de virus y amenazas. Una vez se haya abierto la ventana activamos las Amenazas actuales y la Configuración de antivirus y protección contra amenazas.

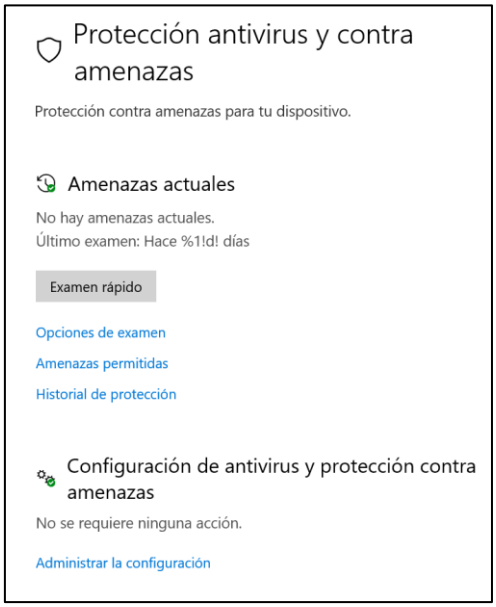

Figura 41: Estado final 1/2

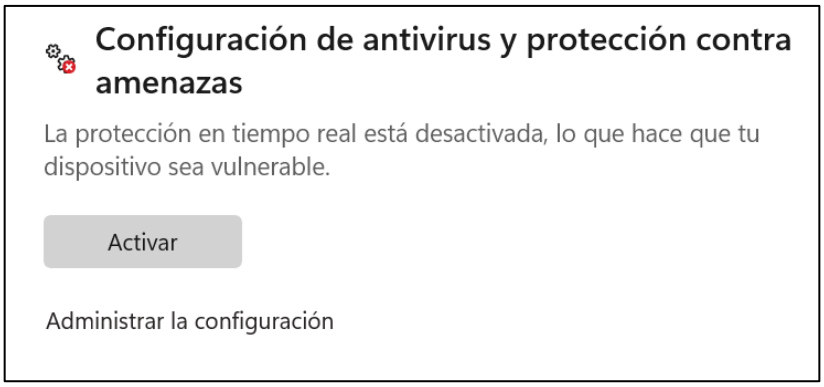

Figura 42: Estado final 2/2

53. Podemos observar que la sección de *Actualizaciones de protección contra virus y amenazas* esta desactivada, esto es porque no tenemos acceso a Internet y no se pueden buscar actualizaciones online.

6.1.10 PEGATINAS DE DETECCIÓN DE MANIPULACIÓN FÍSICA

54. 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**].

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

Figura 43: Pegatina anti-tamper - 1.

Figura 44: Pegatina anti-tamper - 2.

6.1.11 HABILITAR ARCHIVO DE REGISTROS DE AUDITORÍA

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

57. Para ello, accedemos al *Visor de eventos* mediante el comando *eventvwr.msc* y configuramos las propiedades de los registros 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.

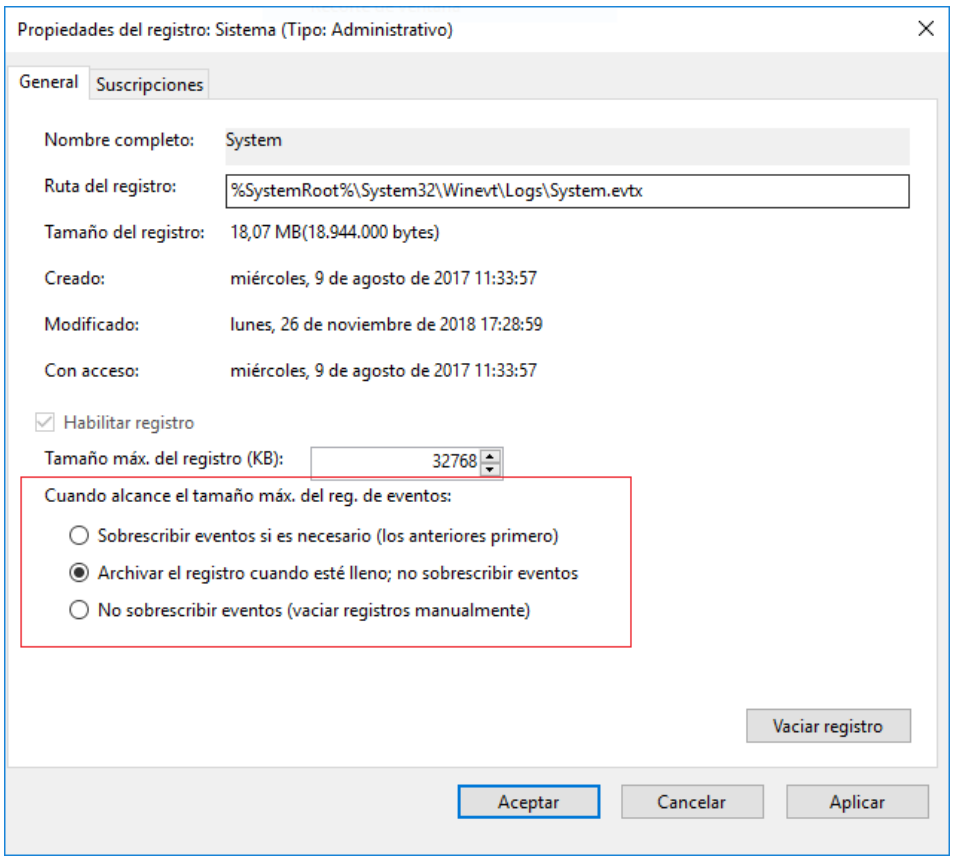

Figura 45: Propiedades de registro de eventos.

6.1.12 COMPROBACIÓN DE DIRECTORIOS DE APPLOCKER

58. 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.

59. 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 "6.4.3 Añadir excepciones en reglas" de este documento

60. 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.

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

    a) Se abrirá una consola PowerShell **sin privilegios de administrador**.

    b) 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. La herramienta AppLocker enseñara por pantalla los subdirectorios dentro del [directorio] a los cuales el grupo Usuarios no tiene acceso.

6.1.13 SOFTWARE DE BORRADO SEGURO

62. Para asegurar la protección de los datos de los usuarios de la tableta se debe hacer uso del software OLVIDO Windows **[OLVIDO]** para realizar el borrado seguro de ficheros. Esta herramienta pertenece al catálogo de productos aprobados por CPSTIC y se debe instalar y configurar de acuerdo con la guía **[CCN-STIC-1508]**.

6.2 AUTENTICACIÓN

63. 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 que se escribirá la frase de paso que se ha configurada previamente en el apartado "6.1.4 Cifrado del almacenamiento interno". 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 **P2**, 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 avanzada – 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.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 GESTIÓN DE USUARIOS

64. 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.

6.3.1.1 CREACIÓN Y BORRADO DE UN USUARIO

65. Para crear un usuario se seguirán los siguientes pasos:

    a) Abrimos la herramienta *Administración de equipos* mediante el comando compmgmt.msc.

    b) Hacemos clic derecho sobre el apartado *Usuarios y grupos locales* → *Usuarios* y seleccionamos *Usuario nuevo…*.

    c) Rellenamos los campos Nombre de usuario, Contraseña y Confirmar contraseña y hacemos clic en Crear.

    d) Hacemos clic en *Cerrar*.

66. Para eliminar un usuario se seguirán los siguientes pasos:

    a) Abrimos la herramienta *Administración de equipos* mediante el comando compmgmt.msc.

    b) Nos dirigimos al apartado *Usuarios y grupos locales* → *Usuarios,* hacemos clic derecho sobre el usuario y seleccionamos la opción *Eliminar.*

6.3.1.2 AÑADIR O RETIRAR UN USUARIO DE UN GRUPO

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

    a) Abrimos la herramienta *Administración de equipos* mediante el comando compmgmt.msc.

    b) Nos dirigimos al apartado *Usuarios y grupos locales* → *Usuarios* y hacemos doble clic sobre el usuario a gestionar.

    c) Seleccionamos la pestaña *Miembro de* y…:

i. Para añadirlo a un grupo, hacemos clic en *Agregar*, escribimos el nombre del grupo y seleccionamos *Aceptar*.

ii. Para retirar el usuario de un grupo, seleccionamos el grupo del cual se desee retirar la pertenencia del usuario y hacemos clic en *Quitar*.

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

6.3.2 CONTROL DE ACCESO

68. 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.

69. Existen dos roles de usuario en el dispositivo:

    a) Administrador: las funciones de este rol son la configuración del dispositivo y todas las funciones descritas en 7.1 USUARIO ADMINISTRADOR.

    b) Usuario estándar: las funciones de este rol se limitan al modo de operación sin privilegios de administrador, y las funciones descritas en 7.2 USUARIO ESTÁNDAR

6.4 ADMINISTRACIÓN DE APPLOCKER

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

71. Antes de comenzar, hay que 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.

6.4.1 PERMITIR O DENEGAR UNA APLICACIÓN

72. Para permitir o denegar una aplicación adicional a lo establecido durante la configuración segura en AppLocker, sección “6.1.7 Configuración de AppLocker” de este documento, seguiremos los siguientes pasos:

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

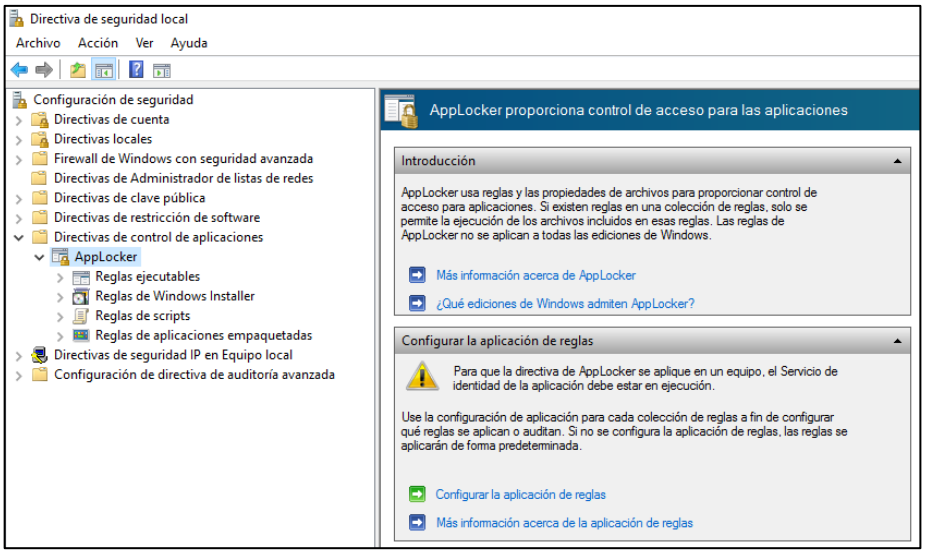

Figura 46: Directiva de seguridad local - AppLocker.

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

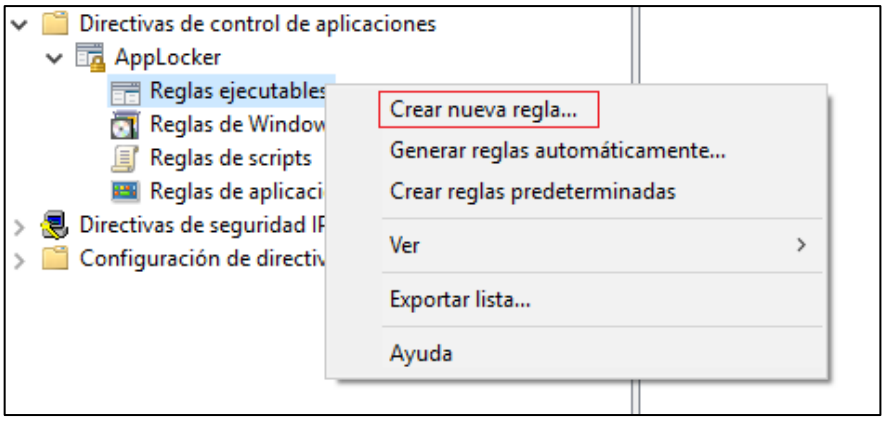

Figura 47: Permitir aplicación en AppLocker - 1.

c) 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.

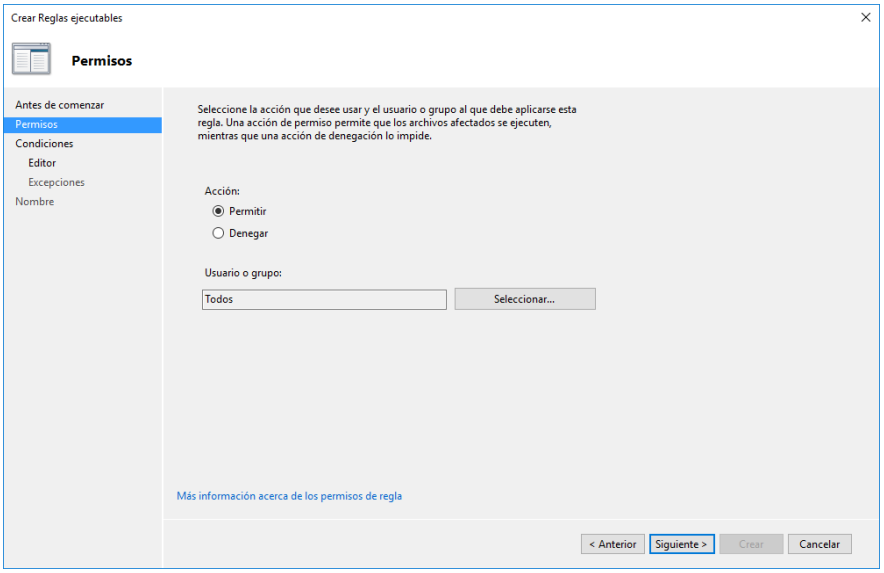

Figura 48: Permitir aplicación en AppLocker - 2.

d) Seleccionamos la opción *Ruta de acceso* como condición de la regla.

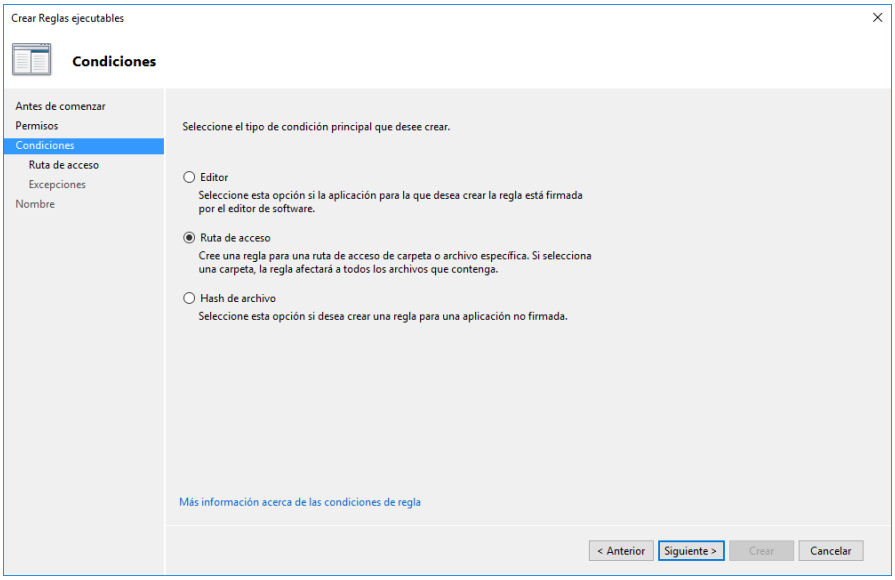

Figura 49: Permitir aplicación en AppLocker - 3.

e) 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 50, o bien a un fichero ejecutable específico, Figura 51.

f) 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...*

g) 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.

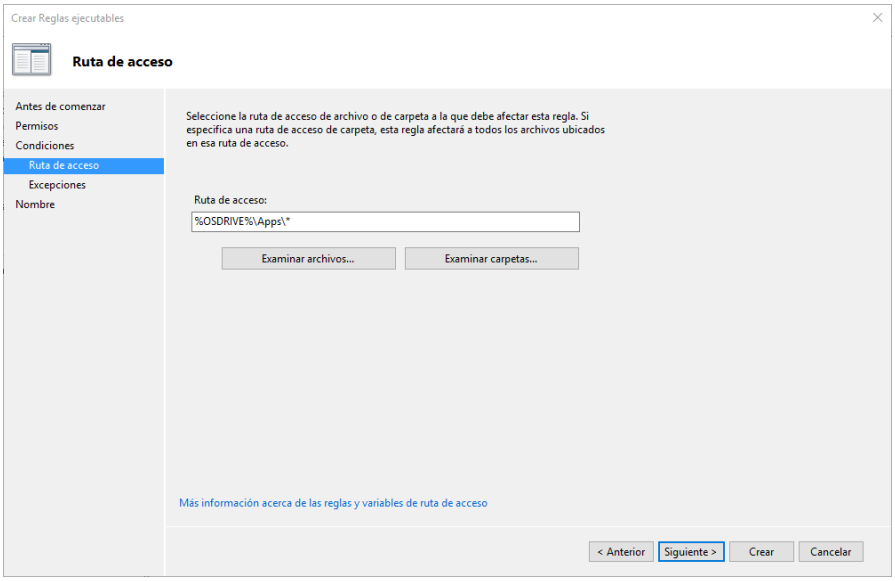

Figura 50: Permitir aplicación mediante ruta de acceso a un directorio en AppLocker - 4.

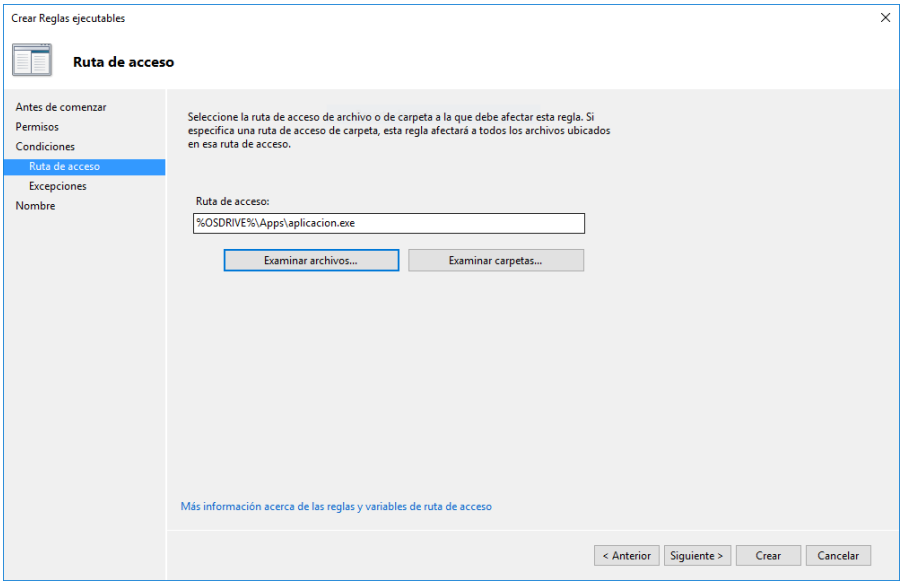

Figura 51: Permitir aplicación mediante ruta de acceso a un fichero ejecutable en AppLocker – 5.

6.4.2 EXPORTAR/IMPORTAR REGLAS

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

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

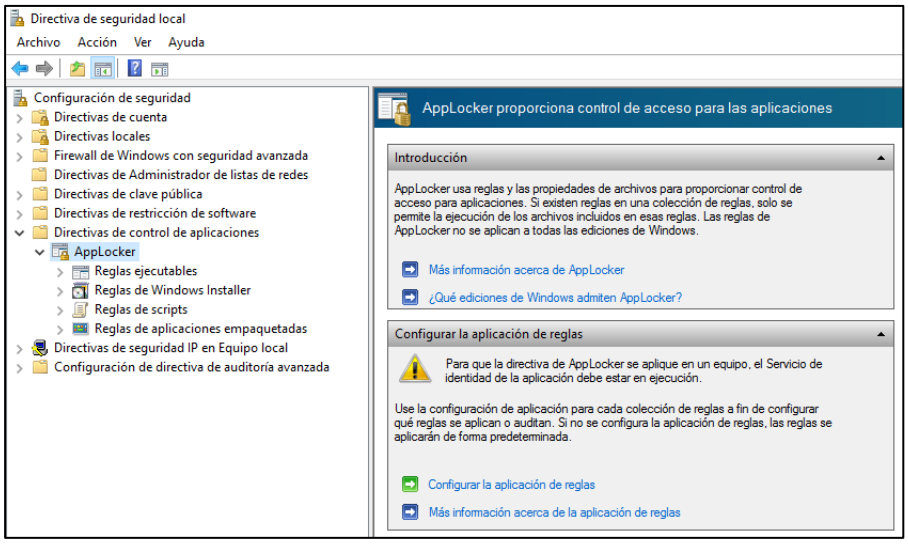

Figura 52: Directiva de seguridad local - AppLocker.

b) 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.

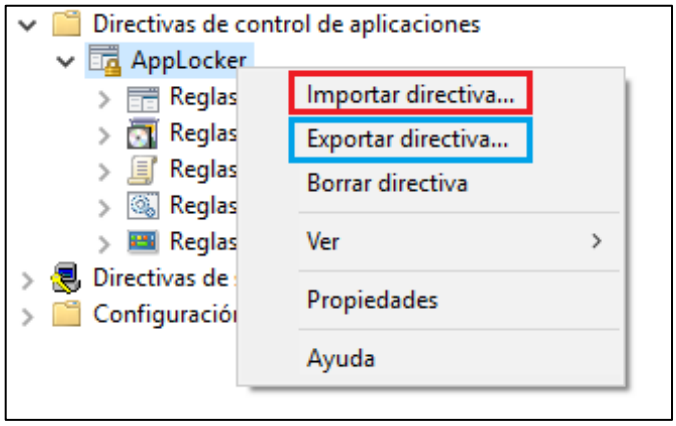

Figura 53: Importando/Exportando reglas de AppLocker - 1.

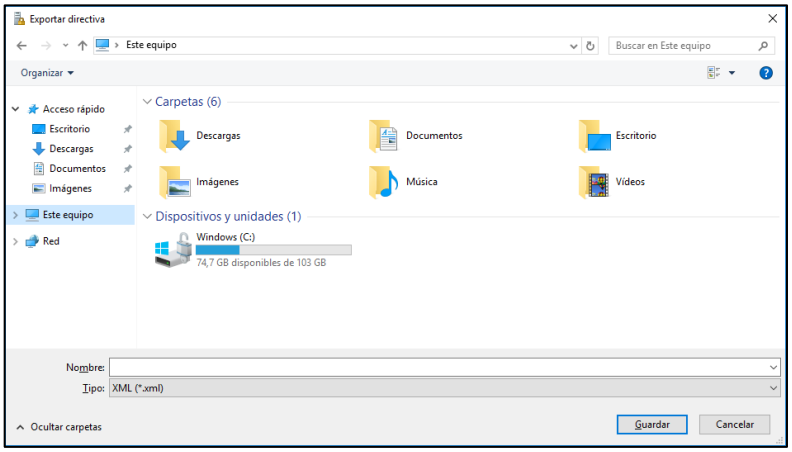

Figura 54: Importando/Exportando reglas de AppLocker – 2

6.4.3 AÑADIR EXCEPCIONES EN REGLAS

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

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

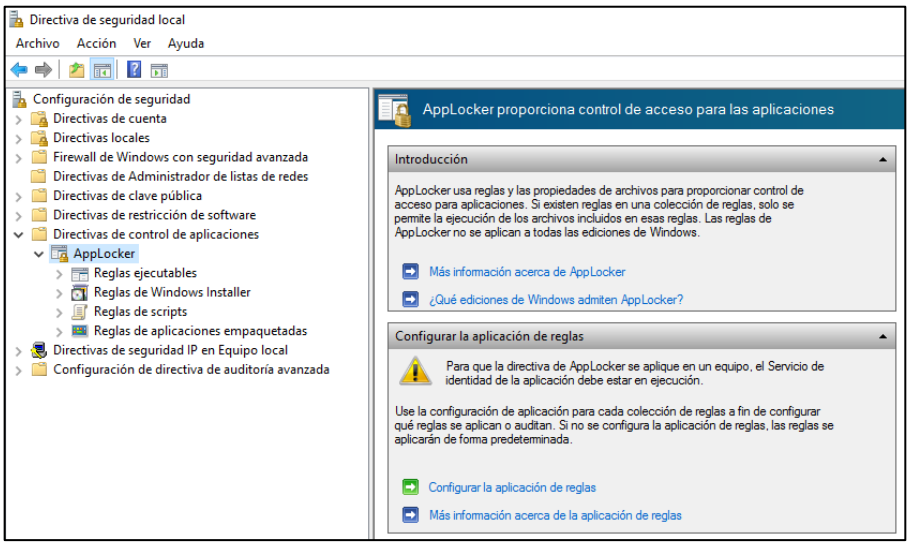

Figura 55: Directiva de seguridad local - AppLocker.

b) 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*.

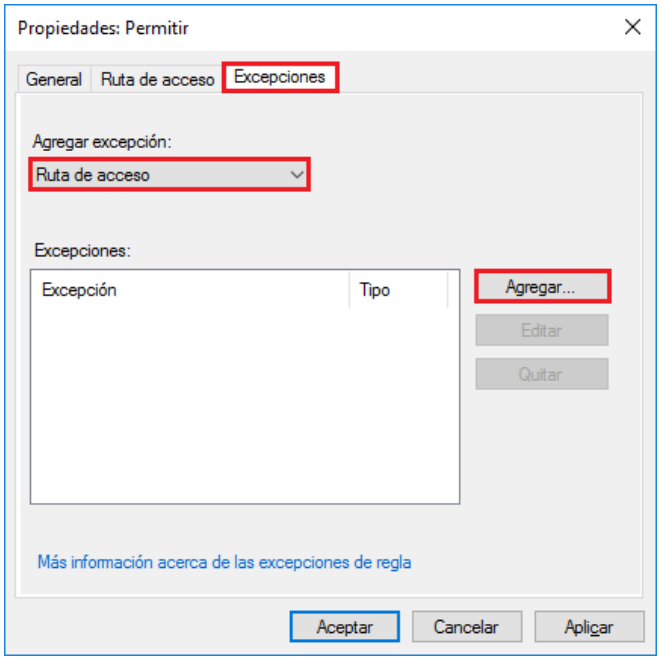

Figura 56: Agregando excepción - 1.

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

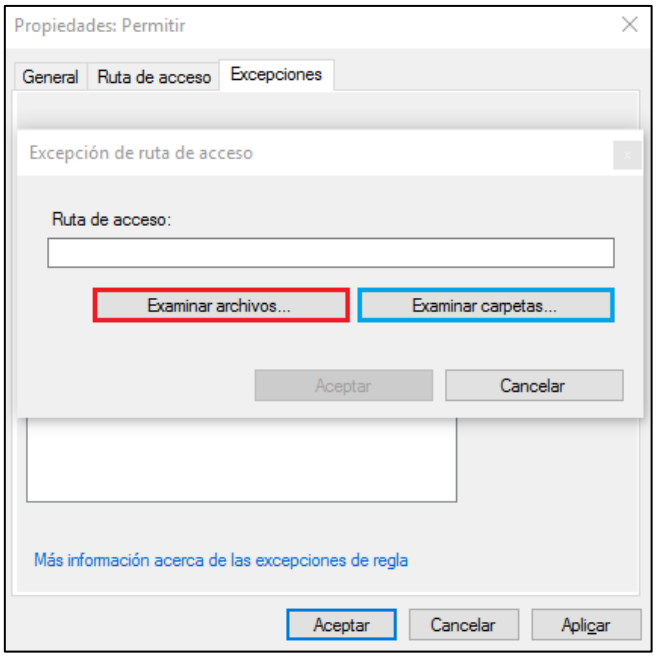

Figura 57: Agregando excepción - 2.

d) Seleccionamos el fichero o directorio deseado.

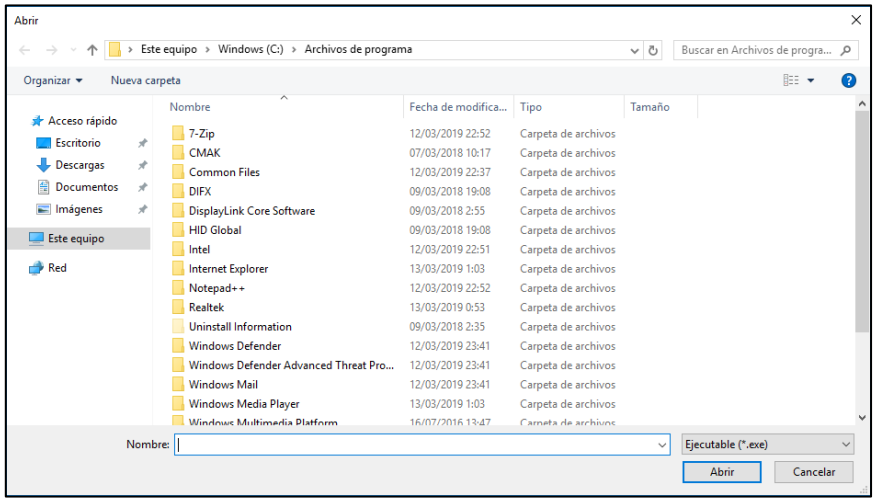

Figura 58: Agregando excepción - 3.

e) Hacemos clic en Aceptar.

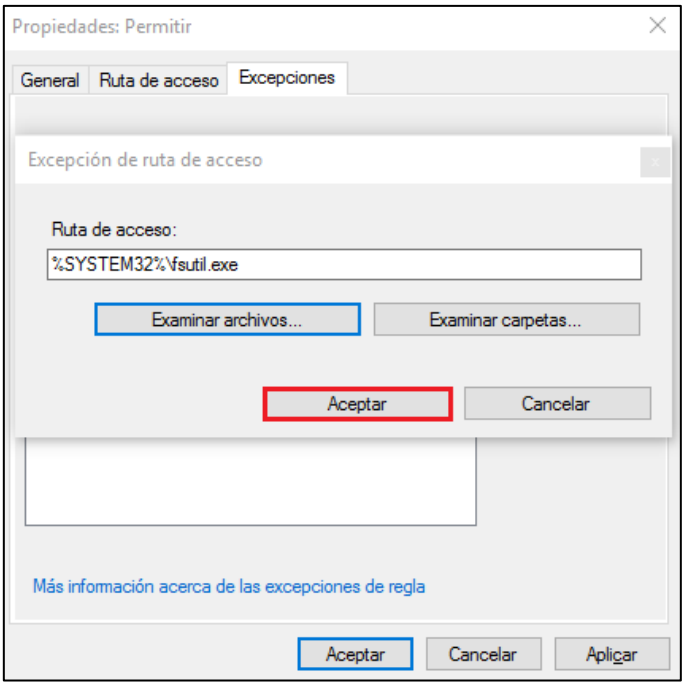

Figura 59: Agregando excepción - 4.

f) Hacemos clic en *Aplicar* y seguidamente en *Aceptar*.

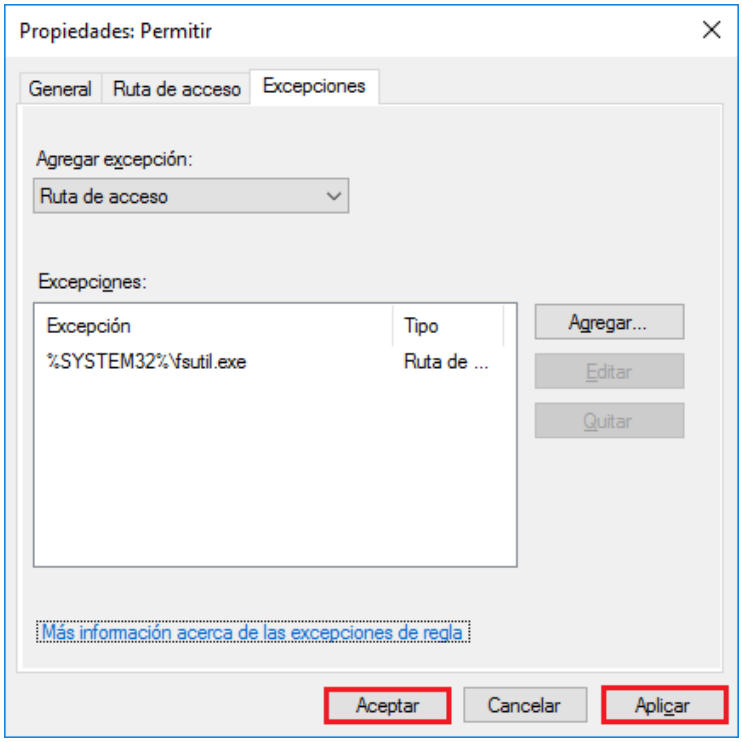

Figura 60: Agregando excepción – 5

7 FASE DE EMPLEO SEGURO

7.1 USUARIO ADMINISTRADOR

7.1.1 BLOQUEO Y DESBLOQUEO DE SESIÓN

75. 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*, o bien mantener pulsado el botón **P2** y seleccionar **bloquear**.

76. Por otro lado, para desbloquear la sesión, se mantendrá pulsado el botón con la etiqueta **P2**, colocado a la derecha de la pantalla de la tableta, para acceder a la pantalla de autenticación, en la que se ingresarán las credenciales.

7.1.1.1 TIEMPO DE INACTIVIDAD PARA EL BLOQUEO DE SESIÓN

77. La configuración aplicada en la sección "6.1.3 Aplicación de la guía [**CCN-STIC-599AB23**]" establece el tiempo de inactividad en 900 segundos de forma predeterminada. Si se desea modificar este tiempo de inactividad se realizarán los siguientes pasos:

    a) Accedemos al editor de políticas de grupo mediante el comando *gpedit.msc.*

    b) 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.

7.1.2 HABILITAR LA INSTALACIÓN DE UN DISPOSITIVO

78. La guía **[CCN-STIC-599AB23]** aplicada en la sección "6.1.3 Aplicación de la guía [CCN-STIC-599AB23]" establece el bloqueo de instalación de dispositivos hardware mediante controladores administrados por usuarios con privilegios elevados.

79. Para permitir la instalación de un dispositivo en concreto, se deberá seguir los pasos del **Anexo B.2.7.1.**

7.1.3 INSTALACIÓN DE APLICACIONES

80. Cuando se realice la instalación de una aplicación se tendrá en cuenta lo descrito en la sección "6.1.12 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.

7.1.4 BORRADO SEGURO DE FICHEROS

81. Cuando se eliminen ficheros que contengan datos confidenciales, debe utilizarse la herramienta de borrado seguro Olvido Windows, que se instaló en la sección "6.1.13 Software de borrado seguro", de acuerdo con la guía **[CCN-STIC-1508].**

7.1.5 SINCRONIZACIÓN

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

    a) **Set-Date.** Permite cambiar la fecha y hora del sistema en la tableta. Para realizar esto, se hará uso de los siguientes comandos:

        i. 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:

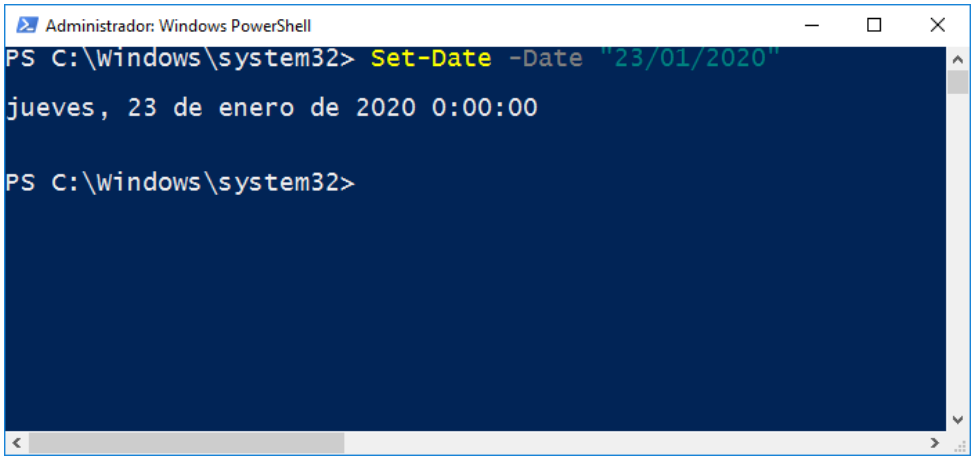

Figura 61: Cambio de fecha del sistema.

        ii. 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:

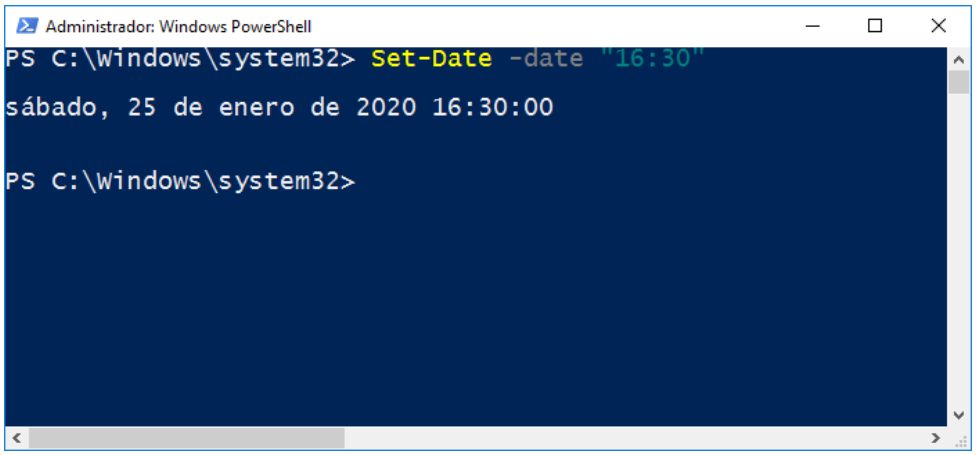

Figura 62: Cambio de hora del sistema.

        iii. 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:

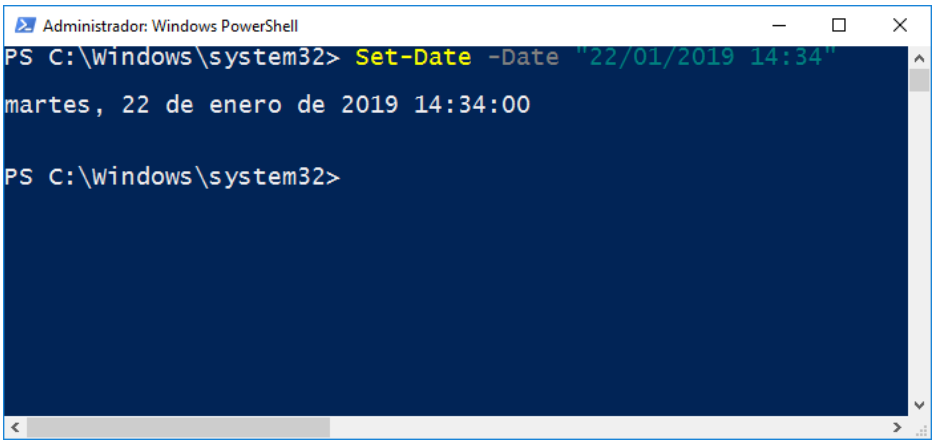

Figura 63: Cambio de fecha y hora del sistema.

83. **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.
```

7.1.6 ACTUALIZACIONES DEL SISTEMA OPERATIVO

84. Para escoger el método de distribución y entrada de actualizaciones se tendrá en cuenta la guía [**CCN-STIC-512**]. El administrador debe instalar las actualizaciones del Sistema Operativo de forma periódica debido a que el dispositivo no dispone de conexión a internet y no puede realizar actualizaciones automáticas.

85. 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:

    a) Abrimos la herramienta *Servicios* mediante el comando *services.msc*.

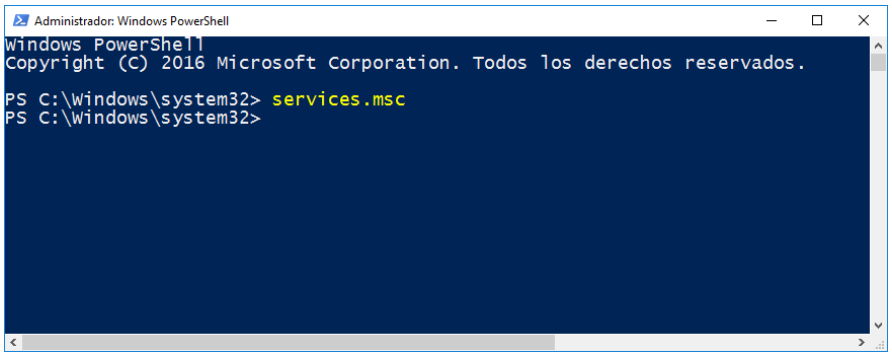

Figura 64: Actualizaciones, activando servicios necesarios - 1.

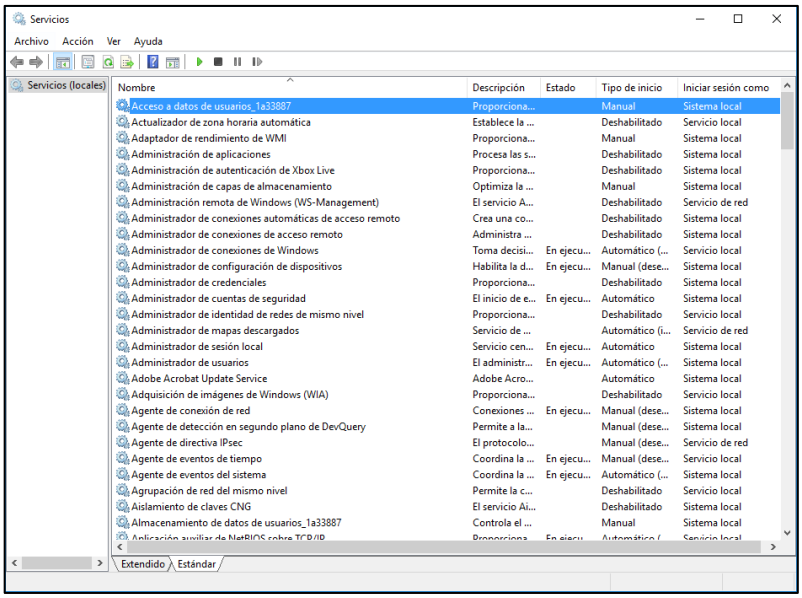

Figura 65: Actualizaciones, activando servicios necesarios – 2.

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

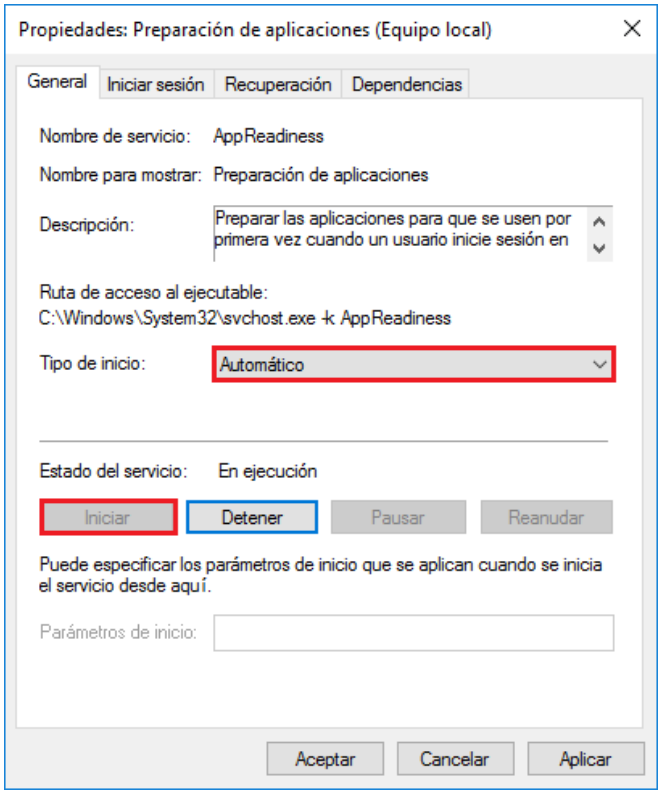

Figura 66: Actualizaciones, activando servicios necesarios – 3.

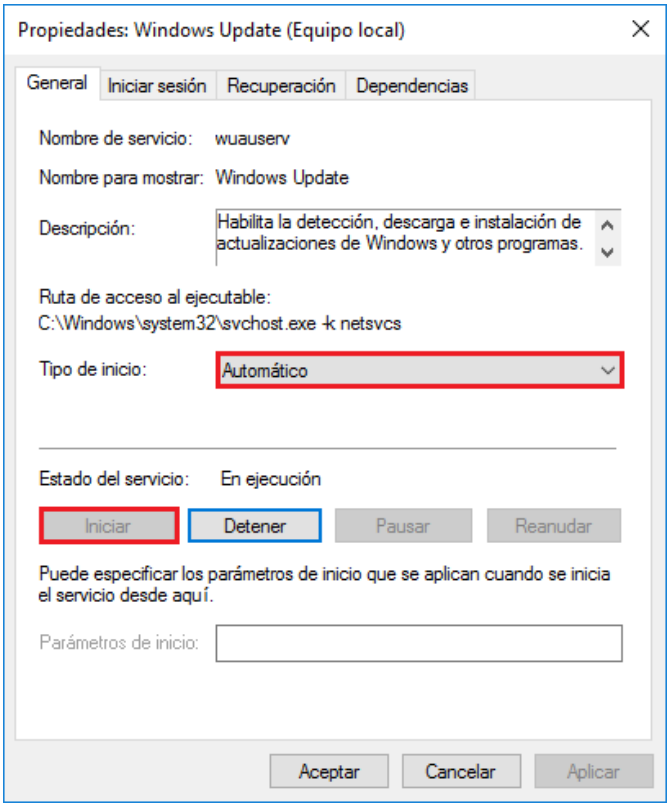

Figura 67: Actualizaciones, activando servicios necesarios – 4.

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

86. Para finalizar, cuando se realice la actualización se tendrá en cuenta lo descrito en la sección *"6.1.12* 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.

7.1.7 DIAGNÓSTICO

7.1.7.1 DIAGNÓSTICO DEL MÓDULO DE PLATAFORMA SEGURA (TPM)

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

a) **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.

b) **Get-TpmEndorsementKeyInfo.** Muestra información básica sobre las claves contenidas en el TPM.

c) **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

7.1.7.2 DIAGNÓSTICO DEL CIFRADO DE DISCO

88. Para diagnosticar y comprobar el estado del cifrado de disco se hará uso del comando de PowerShell:

```
Get-BitlockerVolume.
```

7.1.7.3 DIAGNÓSTICO DEL ARRANQUE SEGURO

89. Para comprobar el estado del arranque seguro se hará uso del comando de PowerShell:

```
Confirm-SecureBootUEFI.
```

7.1.7.4 DIAGNÓSTICO DE PRUEBAS CRIPTOGRÁFICAS

90. Para comprobar si los self-tests criptográficos FIPS realizados 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.

7.1.8 AUDITORÍA

7.1.8.1 REGISTRO DE EVENTOS

91. Para acceder a los registros de auditoría se hará uso de la herramienta *Visor de eventos*. Para ejecutarla se hará uso del comando *eventvwr.msc*.
92. 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.

7.1.9 BACKUP

93. Se recomienda implementar mecanismos de respaldo que permitan recuperar el equipo en caso de fallos o incidencias. Para ello, se aconseja la creación periódica de **puntos de restauración** mediante las herramientas integradas en **Microsoft Windows**, los cuales permiten revertir el sistema a un estado anterior ante problemas derivados de cambios en la configuración o instalación de software. Para evitar un uso excesivo del almacenamiento, se recomienda realizarlos **de forma mensual o antes de efectuar modificaciones relevantes en el sistema**. Se seguirá la documentación oficial de Microsoft para Crear un Punto de Restauración.
94. Asimismo, se recomienda complementar esta medida con **copias de seguridad completas del sistema y de los datos** en dispositivos de almacenamiento externos, permitiendo la recuperación de la información en caso de fallo del dispositivo o pérdida de datos. Ambos mecanismos deben considerarse complementarios dentro de la estrategia de recuperación del sistema. Se seguirá la documentación oficial de Microsoft para crear una Copia de Seguridad, restauración y recuperación en Windows.

7.1.10 MANIPULACIÓN FÍSICA

95. 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.

7.2 USUARIO ESTÁNDAR

7.2.1 AUTENTICACIÓN

96. 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

7.2.2 REGISTROS DE AUDITORÍA

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

98. 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.

7.2.3 BLOQUEO Y DESBLOQUEO DE SESIÓN

99. 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, o bien mantener pulsado el botón **P2** y seleccionar bloquear.

100. Por otro lado, para desbloquear la sesión, se mantendrá pulsado el botón con la etiqueta **P2**, colocado a la derecha de la pantalla de la tableta, para acceder a la pantalla de autenticación, en la que se ingresarán las credenciales

7.2.4 BORRADO SEGURO DE FICHEROS

101. Cuando se eliminen ficheros que contengan datos confidenciales, debe utilizarse la herramienta de borrado seguro Olvido Windows, que se instaló en la sección “6.1.13 Software de borrado seguro”, de acuerdo con la guía [**CCN-STIC-1508**]

8 REFERENCIAS

[CCN-STIC-409A] Colocación de etiquetas de seguridad
https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/400-guias-generales/76-ccn-stic-409a-colocacion-de-etiquetas-de-seguridad-dl/file.html

[CCN-STIC-512] Gestión de Actualizaciones de Seguridad
https://www.ccn-cert.cni.es/es/500-guias-de-entornos-windows/302-ccn-stic-512-gestion-de-actualizaciones-de-seguridad-en-sistemas-windows/file.html

[CCN-STIC-599AB23] Perfilado de Seguridad para Windows Cliente
https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/7242-ccn-stic-599ab23-perfilado-de-seguridad-para-windows-cliente-cliente-miembro-o-cliente-independiente/file.html

[CCN-STIC-1508] Procedimiento de empleo seguro OLVIDO Windows
https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/6720-ccn-stic-1508-procedimiento-de-empleo-seguro-olvido-windows/file.html

[CPSTIC] Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

[OLVIDO] Software OLVIDO Windows
https://www.ccn.cni.es/es/soluciones-ccn/olvido

[ACCESSCHK] Herramienta *AccessChk* de SysInternals
https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

9 ABREVIATURAS

CCN	Centro Criptológico Nacional
FIPS	Federal Information Processing Standard
HDMI	High-Definition Multimedia Interface
LINCE	Certificación Nacional Esencial de Seguridad (LINCE)
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

ANEXO A: DIRECTORIOS Y FICHEROS PARA BLOQUEAR EN APPLOCKER

En siguiente tabla 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\extrac32.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 3: Directorios y ficheros para bloquear en AppLocker.