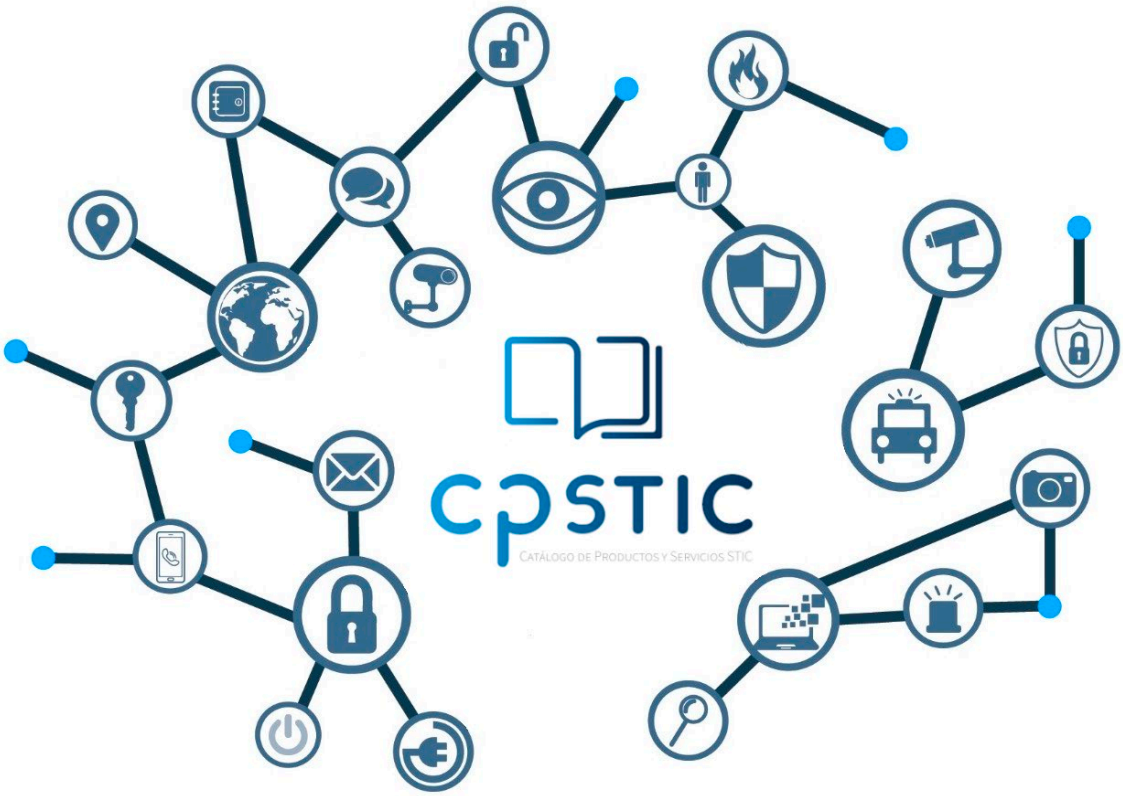
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1618

Procedimiento de Empleo Seguro
DELL PRECISION 3570



Septiembre 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-244-8.

Fecha de Edición: septiembre de 2022

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.28 14:06:34 +02'00'

ÍNDICE

1. INTRODUCCIÓN

1. El producto para el que se desarrolla esta guía consiste en un **equipo portátil DELL PRECISION 3570 con sistema operativo Windows 10 Enterprise N LTSC**, Versión 21H2, Compilación 19044.1288 securizable mediante la aplicación de las guías STIC [6].
2. De acuerdo con sus funcionalidades principales, el producto es conforme a la familia de productos denominada como Plataformas de Confianza ya que consiste en un producto que sirve como base o soporte para la ejecución de determinados módulos software con los que es compatible. **El equipo ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional.**
3. A lo largo de los diferentes capítulos, se ofrecen consejos y recomendaciones para la activación o desactivación de servicios, políticas y funcionalidades con el fin de establecer una configuración lo más segura posible.

2. OBJETO Y ALCANCE

2.1 REQUISITOS *HARDWARE*

4. El *hardware* sobre el que se despliega el sistema operativo es el siguiente:
    a) Portátil DELL PRECISION 3570
    b) Procesador 12th Gen Intel® Core™ Intel i7-1265U 1.8GHz con VPro habilitado.
    c) Procesador 12th Gen Intel® Core™ Intel i7-1255U 1.7GHz.
    d) TPM 2.0 ver 1.258.0.0
5. Aunque la configuración y empleo seguro del producto se centra en el *software* utilizado, el procesador deberá tener soporte para el módulo TPM (*Trusted Platform Module*), para el correcto funcionamiento de módulos de protección criptográficos.

2.2 REQUISITOS *SOFTWARE*

6. En cuanto a los requisitos *software*, el sistema operativo requerido para la aplicación de esta guía es Windows 10 Enterprise N LTSC compilación 19044.1288.
7. No se establece una restricción estricta a nivel *software*. Sin embargo, es necesario que la versión del sistema operativo sea compatible con la herramienta de cifrado en reposo "*BitLocker*", la cual es un requisito para el cumplimiento de funcionalidades de seguridad.
8. Para mantener la configuración evaluada, deben tenerse en cuenta las siguientes reglas:
    a) Todas las configuraciones indicadas en este documento deben seguirse estrictamente
    b) Para configurar el equipo, será necesaria una cuenta de administrador local.

3. ORGANIZACIÓN DEL DOCUMENTO

9. Indicar la estructura de capítulos del documento:

   a) Apartado **4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

   b) Apartado **5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura, así como los métodos de autenticación presentes en el producto.

   c) Apartado **6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   d) Apartado **7**. Lista de comprobación de los pasos de configuración del producto.

   e) Apartado **8**. Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

   f) Apartado **9**. Incluye un listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Aunque el dispositivo Dell requiere una configuración inicial antes de añadirse a una organización, es fundamental asegurarse de que el dispositivo ha sido transportado y configurado sin ninguna manipulación o modificación.
11. Es muy importante que estos productos se adquieran a través de proveedores de confianza para mitigar riesgos relacionados con la cadena de suministro.
12. Al recibir el equipo deben verificarse los siguientes aspectos:
    a) **El embalaje es original y no ha sido manipulado su sellado**.
    b) **El equipo no presenta señales de haber sido manipulado o abierto**. Para ello, el producto estará provisto de etiquetas *tamper-evident* que validan este punto.

    c) El sistema operativo instalado debe ser Windows 10 Enterprise N.

4.2 REGISTRO Y LICENCIAS

13. En caso de que el *appliance* se reciba sin el *software* instalado, o la versión no corresponda con Windows 10 Enterprise LTSC, se deberá descargar e instalar el sistema operativo.
14. Para ello, se deberán seguir los siguientes pasos:
    a) Acceder a la página oficial de Windows para descargar el *software*. En el centro de descarga se indican directrices y consideraciones de instalación.
    b) Localizar la versión LTSC de Windows 10 Enterprise del idioma que corresponda.
    c) El *software* se descargará en formato .iso.
    d) Una vez descargado, utilizar un dispositivo de almacenamiento USB que servirá de dispositivo de arranque para la instalación en el *appliance*.
    e) Introducir el dispositivo USB en el equipo y seguir los pasos de instalación. **Es recomendable seguir las indicaciones descritas en la guía de configuración segura sobre Microsoft Windows 10 (cliente independiente) [CCN-STIC-599B19].**

f) Se deberá utilizar una licencia correspondiente a la versión de Windows que se va a instalar.

4.3 CONSIDERACIONES PREVIAS

15. Para la configuración de los equipos es necesario crear una cuenta de administrador local. Además, aunque no es un requisito, **es recomendable realizar dicha configuración en un entorno seguro y aislado de una red, ya que no es necesaria la conexión a internet para ello.**
16. La configuración del sistema operativo hace referencia a la **Guía de Seguridad Implementación de Seguridad sobre Microsoft Windows 10 para Cliente Independiente [CCN-STIC-599B19].**
17. Para la configuración de la utilidad BitLocker, será necesario una unidad de almacenamiento distinta de la que se cifrará para almacenar la clave de recuperación en caso de pérdida de la contraseña de autenticación de BitLocker. Por ejemplo, se podrá utilizar una unidad USB que deberá guardarse en un lugar seguro.

5. FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

5.1.1 AUTENTICACIÓN DEL SISTEMA OPERATIVO

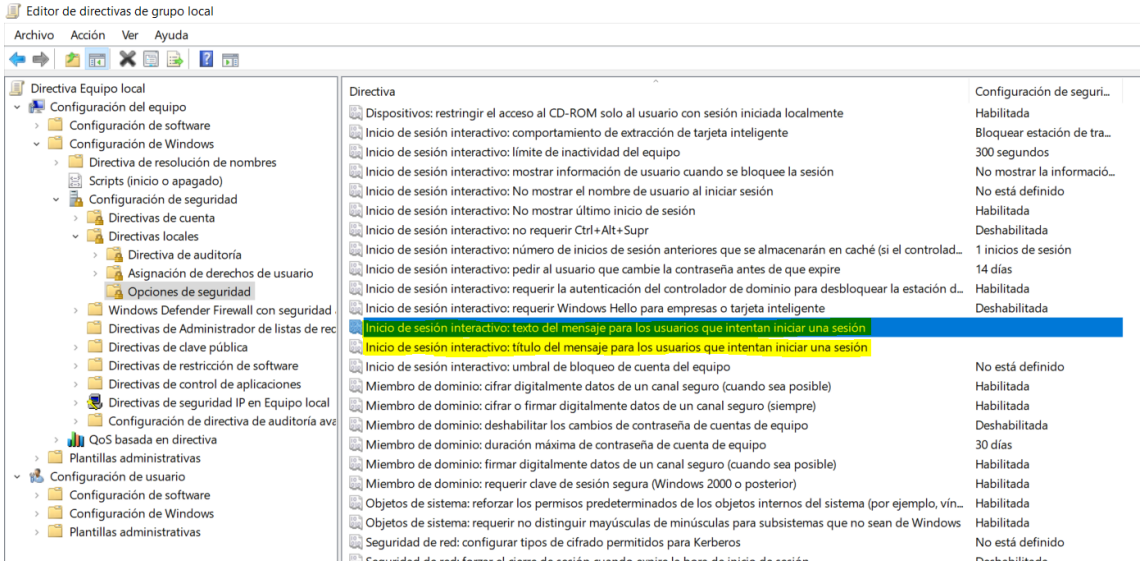
18. En los equipos Dell configurados, la autenticación de usuarios será local. Las credenciales de acceso se definen localmente en cada equipo, siguiendo la política de contraseñas robustas definidas en las políticas de control de acceso de las que dispone el sistema operativo (GPO – *Group Policy Object*). La configuración de las directivas de contraseñas se detalla en 5.2.2.1.

19. El producto permite crear nuevos usuarios para acceder al sistema operativo desde: *Inicio > Configuración > Cuentas > Familia y otros usuarios*.

20. Una vez el usuario accede a la pantalla de inicio del sistema operativo, para ingresar las credenciales se deberán presionar las teclas *Ctrl + Alt + Supr*.

21. Una vez el usuario haya ingresado sus credenciales de acceso al sistema operativo, será informado de los últimos intentos de inicio de sesión.

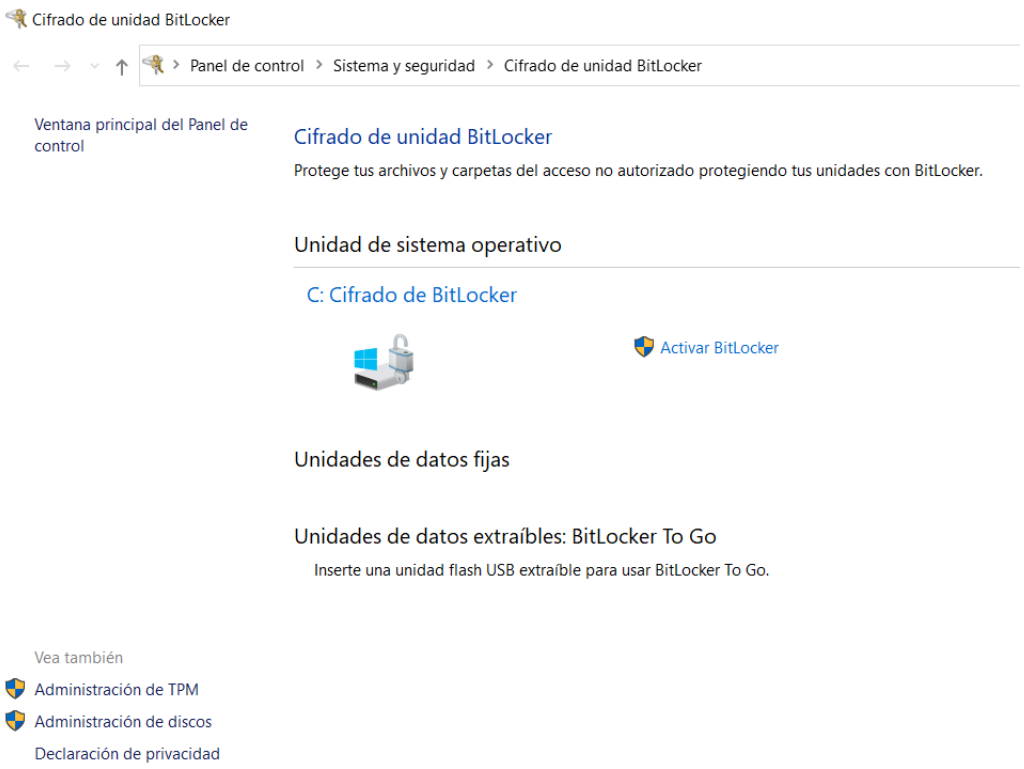
22. En el caso de incluir un banner de inicio de sesión, por ejemplo, para dar consentimiento de acceso y avisar del mismo, el administrador podrá modificar la configuración de las opciones de seguridad en el *Editor de directivas de grupo local, Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales.*



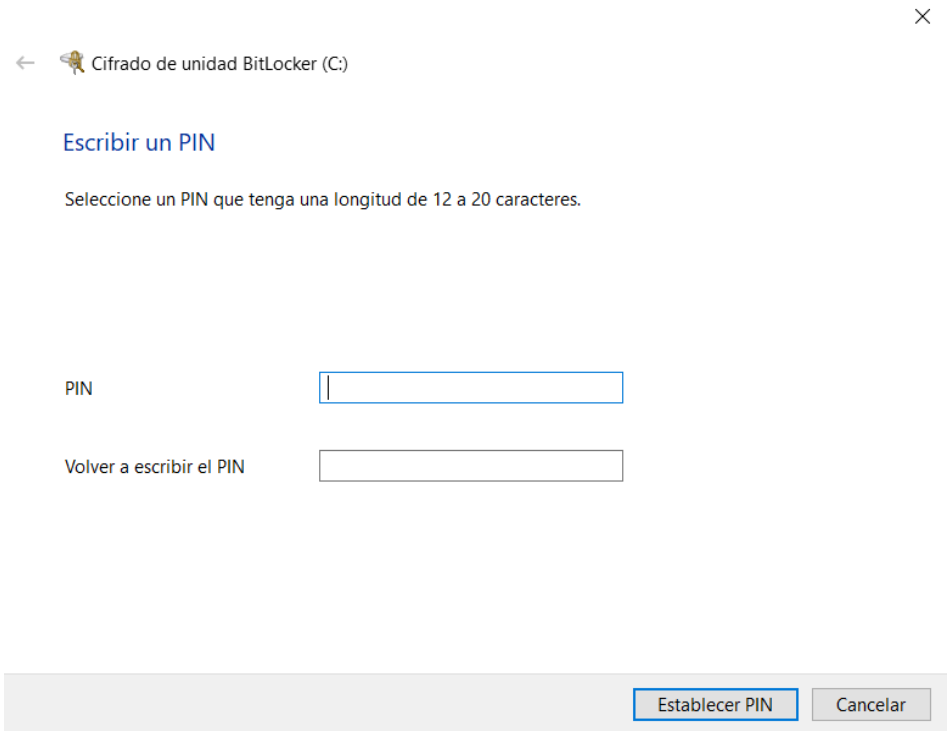
5.1.2 AUTENTICACIÓN DE *BITLOCKER*

23. **El equipo se deberá configurar con la herramienta *BitLocker*, la cual permite el cifrado del disco**. Como protección adicional al acceso del sistema, el usuario deberá introducir una clave definida previamente para el descifrado de los datos protegidos por la utilidad.

24. Para cumplir con los requisitos de seguridad para plataformas de confianza, es necesario **definir las políticas de cifrado de *BitLocker***. Para ello:
    a) Acceder a la herramienta *gpedit.msc* desde el comando "*Ejecutar*" (Tecla de Windows + R).
    b) Las políticas para la herramienta se encuentran en: *Configuración del equipo > Plantillas administrativas > Cifrado de unidad BitLocker.*
    c) Definir al menos las siguientes políticas:
        i. **Permitir arranque seguro** para comprobación de integridad: Habilitada
        ii. **Requerir autenticación adicional**: Habilitada, con las siguientes opciones:
            1. Configurar inicio del TPM: Permitir TPM
            2. Configurar PIN de inicio del TPM: Requerir PIN de inicio con TPM
            3. Configurar clave de inicio del TPM: No permitir clave de inicio con TPM
            4. Configurar la clave de inicio y el PIN del TPM: No permitir clave y PIN de inicio con TPM
            5. Permitir los PIN mejorados para el inicio: Habilitada
            6. Configurar longitud mínima de PIN para el inicio: Habilitada, 8 caracteres.
        iii. **Configurar el perfil de validación de plataforma del TPM** para configuraciones de *firmware* basado en BIOS: Habilitada, definiendo los siguientes grupos: 0, 2, 4, 5, 7, 8, 9, 10, 11.
25. Para configurar esta herramienta, se deberá proceder de la siguiente manera:
    a) Abrir la Administración de *BitLocker* desde la barra de búsqueda de Windows.

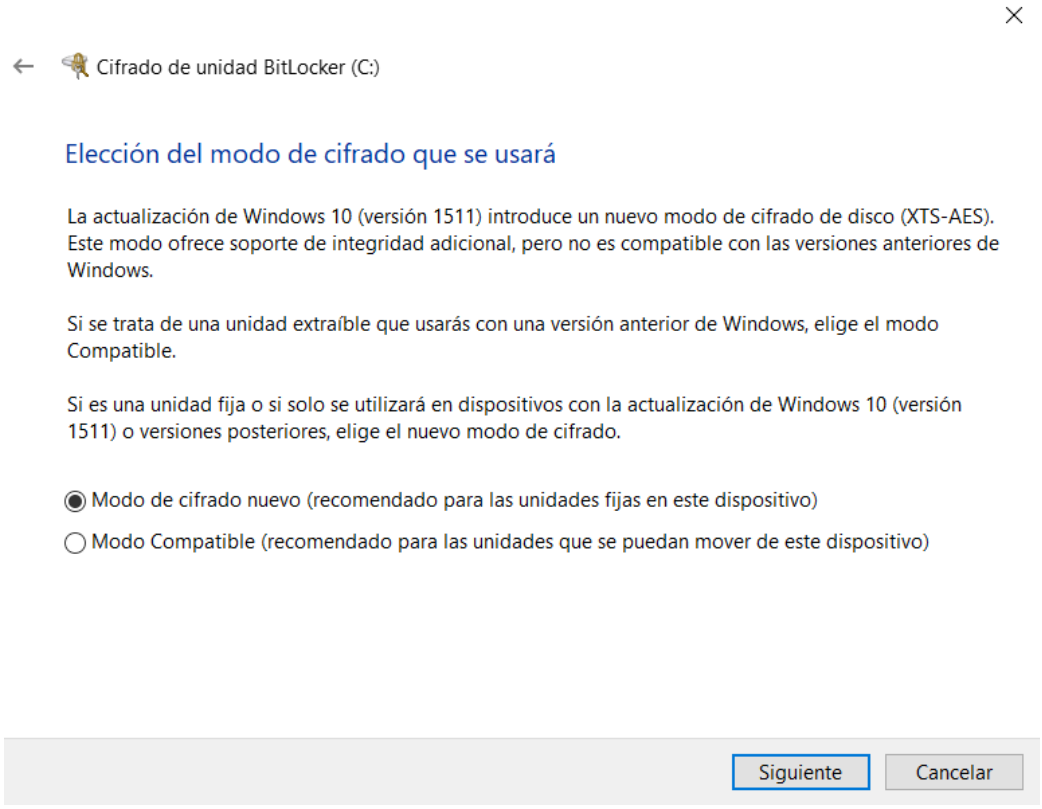


b) Activar *BitLocker*. A partir de aquí, se solicitará un PIN que cumpla con las políticas definidas anteriormente.



c) La herramienta, antes de cifrar el disco solicitará almacenar una clave de recuperación en un dispositivo de almacenamiento distinto al que se va a proteger. **Se debe almacenar la clave en un lugar seguro.** En el caso de que el PIN de autenticación se pierda, será necesario hacer uso de esta clave.

d) **Elegir la opción de cifrado nuevo, que utilizará el modo de cifrado XTS-AES de 128 bits**.



5.1.3 AUTENTICACIÓN DE BIOS UEFI

26. La configuración de la BIOS del producto podrá ser protegida con una contraseña de administrador para evitar modificaciones no deseadas.
27. Para acceder a la BIOS del equipo, es necesario presionar F2 en el momento de arranque. Una vez dentro, acceder a la categoría *Passwords*.
28. Esta contraseña se establece en el apartado *Admin Password*, cumpliendo con la política de contraseñas establecida en el apartado *Password Configuration*, encontrado en una sección posterior dentro de la categoría *Passwords*.
29. El administrador deberá establecer una contraseña que debe cumplir con las siguientes características para proteger el acceso a la UEFI de ataques de fuerza bruta:
    a) Longitud mínima de 12 caracteres.
    b) Utilización de una combinación de mayúsculas, minúsculas, símbolos y números.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

30. El producto será administrado por una cuenta de administrador local. Esta cuenta puede ser creada durante la instalación del sistema operativo, o en el menú de creación de cuentas de usuarios (*Inicio > Configuración > Cuentas > Familia y otros usuarios*), teniendo como requisito previo la existencia de otra cuenta de administrador.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

5.2.2.1 CONFIGURACIÓN DE LA DIRECTIVA DE CONTRASEÑAS

31. Para definir las políticas de control de acceso, con una cuenta de administrador, se deberá utilizar el editor de directivas de grupo local del sistema operativo. Para ello:
    a) Acceder a la herramienta *gpedit.msc* desde el comando "*Ejecutar*" (Tecla de Windows + R).
    b) La configuración para las directivas de contraseña se encuentra en: *Configuración de equipo -> Configuración de Windows > Directivas de cuenta > Directiva de contraseñas*.
32. Para cumplir con los requisitos establecidos en la guía de seguridad para plataformas de confianza [TAXF6], la política de contraseñas deberá contener, al menos, la siguiente configuración:
    a) **Vigencia máxima de contraseña: 180 días**
    b) **Vigencia mínima de contraseña: 4 días**
    c) **Historial de contraseñas: 5 contraseñas**
    d) **Longitud mínima: 9 caracteres**
    e) **Requisitos de complejidad: Habilitado**
33. El *timeout* de inactividad será de 300 segundos (5 minutos), definido en el *Editor de directivas de grupo local, Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales.*
34. El número máximo de intentos fallidos de autenticación es de 8, bloqueando el acceso durante 30 minutos.

5.2.2.2 CONFIGURACIÓN DEL ACCESO AL EDITOR DE REGISTRO

35. Para evitar que los usuarios puedan realizar modificaciones del registro de Windows, y así proteger de potenciales vulnerabilidades que requieran de este acceso, **se debe deshabilitar el acceso a esta herramienta**. En el *Editor de directivas de grupo local, Configuración de usuario > Plantillas administrativas >*

Sistema > Impedir el acceso a herramientas de edición del Registro, será necesario habilitar esta política.

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

36. La configuración segura de servicios deberá establecerse siguiendo la guía de configuración segura para Windows 10 para cliente independiente [CCN-STIC-599B19], a partir del apartado 36, donde se determina el estado que deberán tener los servicios.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

37. El sistema operativo permite la configuración de la directiva *Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash*, la cual habilita al sistema para utilizar algoritmos criptográficos FIPS 140 apropiados: 3DES y AES para cifrado, criptografía de clave pública RSA o ECC para el intercambio y la autenticación de claves TLS, y el algoritmo de hash seguro (SHA1, SHA256, SHA384 y SHA512) para los requisitos de hash TLS.
38. **Se debe habilitar la configuración FIPS**. Para ello, acceder al *Editor de directivas de grupo local, Configuración de Windows > Configuración de seguridad > Opciones de seguridad*, y seleccionar *Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash.*
39. La configuración de BitLocker está establecida para utilizar un método de cifrado XTS-AES de 128 bits, cumpliendo así con guía CCN-STIC-807 [CCN-STIC-807].
40. Este método de cifrado se define accediendo al *Editor de directivas de grupo local, Configuración del equipo > Plantillas administrativas > Componentes de Windows > Cifrado de unidad BitLocker.*

5.5 CONFIGURACIÓN DE APPLOCKER

41. El administrador será el encargado de configurar las aplicaciones según las necesidades de la organización. **Se deberán configurar reglas en la herramienta que permitirán evitar el uso de aplicaciones no deseadas o la instalación de paquetes definidos como no seguros**.
42. **AppLocker** es una característica de Windows que permite la administración y control del acceso a los archivos por parte de los usuarios.
43. Esta característica permite realizar las siguientes acciones:
    a) En base a las firmas de archivo puede definir reglas específicas para una versión de archivo determinada.
    b) Asignar una regla a un grupo de seguridad o a un usuario individual.
    c) Crear reglas de excepción para impedir el uso de un proceso determinado.
    d) Crear y administrar reglas para *AppLocker* a través del uso de *PowerShell*.

e) Auditar al implantar la directiva con la finalidad de medir su alcance.

f) Importar directivas para sobrescribir las actuales y exportar las existentes.

44. De esta forma, es posible controlar los permisos que tienen los usuarios para instalar o ejecutar paquetes en el sistema operativo. Por ejemplo, es posible configurar *AppLocker* para que únicamente permita instalar paquetes que estén firmados y validados por Windows.

45. Para configurar *AppLocker* hay que acceder al *Editor de directivas de grupo local, Configuración del equipo > Configuración Windows > Configuración de seguridad > Directivas de control de aplicaciones > AppLocker*.

46. AppLocker permite aplicar reglas en diferentes categorías:

    a) Reglas ejecutables.

    b) Reglas de Windows Installer.

    c) Reglas de scripts.

    d) Reglas de aplicaciones empaquetadas.

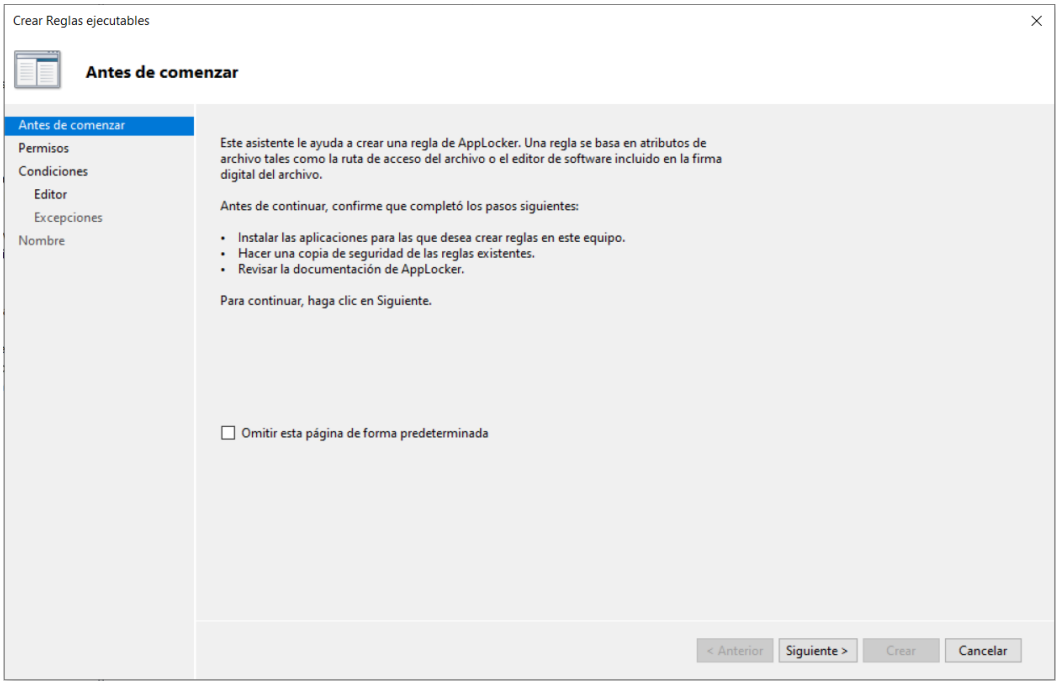
47. En esta guía se explica la configuración de reglas para las dos primeras categorías: ejecutables y *Windows Installer*. Sin embargo, el administrador podrá configurar tantas como sean necesarias. Para más información sobre la configuración de AppLocker, Documentación AppLocker.

5.5.1 REGLAS EJECUTABLES

48. **El administrador deberá configurar las reglas ejecutables según las necesidades de la organización**. Aquellos ejecutables con un editor considerado como seguro podrá incluirse en la definición de la regla. Del mismo modo, se podrán definir rutas de archivo desde las cuales se podrán o no ejecutar las aplicaciones que se encuentren en ellas.

49. Estas reglas permiten al administrador bloquear o permitir la ejecución de archivos.

50. Para definir una regla, es necesario acceder a la categoría *Reglas ejecutables*, pulsar *click* derecho y *crear nueva regla*.



51. En la pestaña *Permisos* se puede determinar la acción (Permitir o Denegar) y el usuario o grupo de usuarios a los que aplicará la regla.

52. En la pestaña *Condiciones*, se determina el tipo de condición para crear la regla:

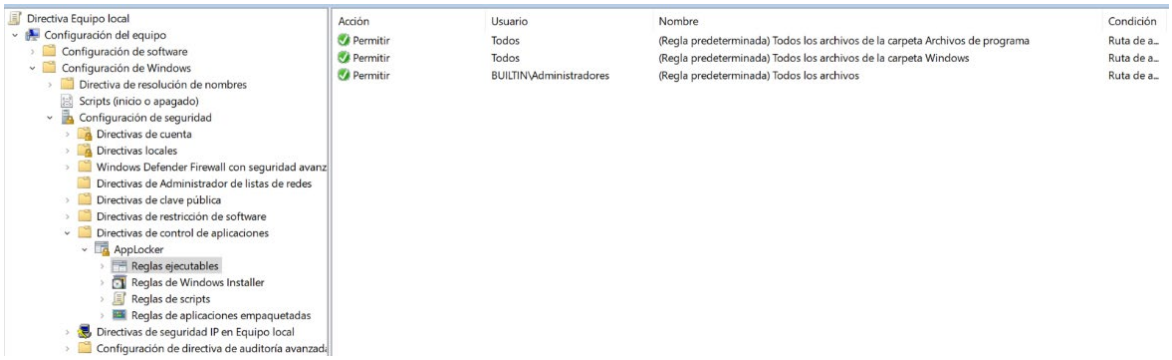
    a) Editor. La aplicación deberá estar firmada por el editor de software seleccionado.

    b) Ruta de acceso. La regla se aplicará para aquellos archivos o carpeta especificada.

    c) Hash de archivo. La regla se aplicará sobre un archivo no firmado.

53. En cada una de las condiciones, se deberá seleccionar el valor por el que se aplicará la regla, como por ejemplo la ruta de acceso, y las posibles excepciones. Por último, se deberá establecer el nombre de la regla.

54. Una vez creada las reglas, la ventana de *Reglas ejecutables* se mostrará como la siguiente imagen:

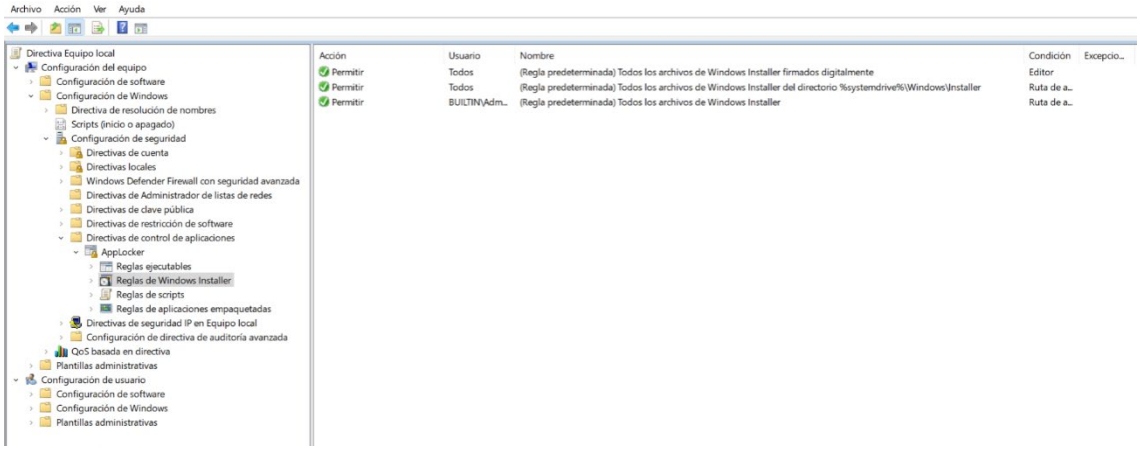


5.5.2 REGLAS DE *WINDOWS INSTALLER*

55. **El administrador deberá configurar las reglas de Windows Installer según las necesidades de la organización**. Se podrán definir reglas que establezcan la posibilidad de ejecutar archivos de Windows Installer que se encuentren firmados digitalmente o en una ruta especificada por el administrador.

56. Estas reglas se configuran de manera similar a las reglas ejecutables. Sin embargo, está orientado a archivos de *Windows Installer*.

57. En el caso de la configuración mostrada en la siguiente imagen, se han definido reglas que permiten a los usuarios ejecutar archivos de *Windows Installer* que se encuentren firmados digitalmente, y aquellos que se encuentren en el directorio *C:\Windows\Installer* (asumiendo que el disco principal del sistema es C:\, en otro caso, modificar por el disco principal del sistema operativo).



5.6 SINCRONIZACIÓN HORARIA

58. Windows 10 utiliza el servicio W32Time para la sincronización horaria. Este servicio sigue la especificación NTP. Para modificar su configuración, se deberá acceder a *services.msc,* y acceder al servicio *Hora de Windows*. **La configuración segura para el producto será "Manual".**

5.7 ACTUALIZACIONES

59. La gestión de las actualizaciones del sistema podrá ser realizada a través de la herramienta de actualización de Windows 10. El administrador podrá gestionar y limitar estas actualizaciones automáticas accediendo al *Editor de directivas de grupo local, gpedit.msc, Plantillas administrativas > Componentes de Windows > Windows Update*. Se pueden establecer, programar días de instalación o restringir el acceso a las actualizaciones de Windows, entre otras opciones.

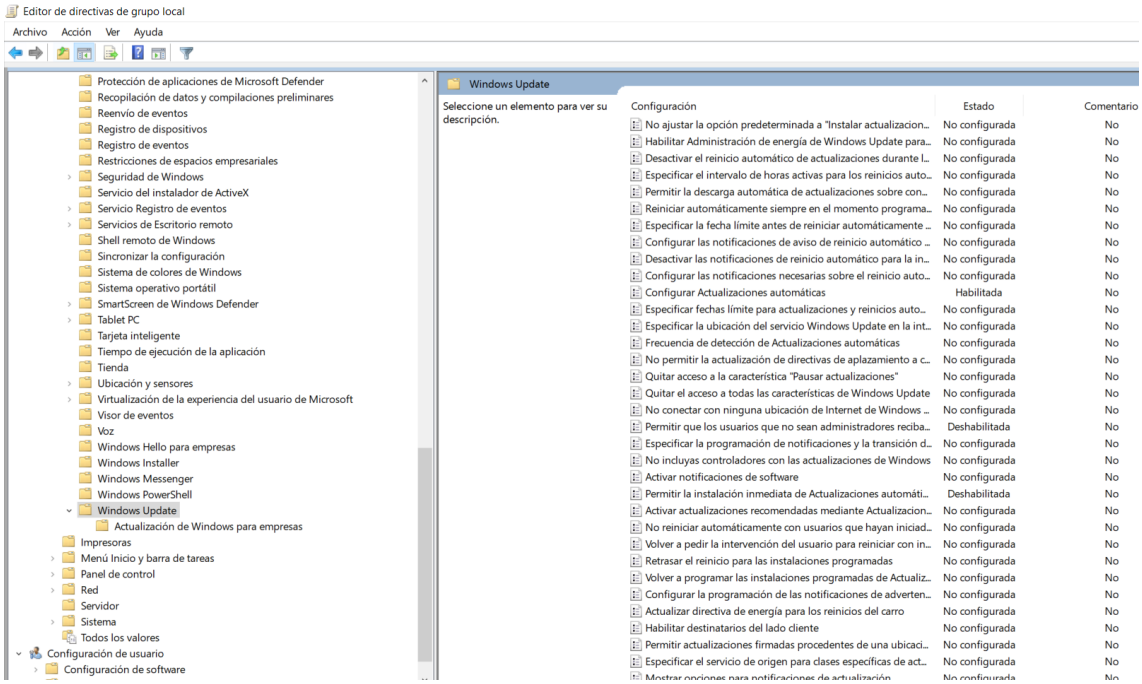
60. En la página oficial del producto Dell se encuentran las actualizaciones para la BIOS y controladores específicos del *hardware* del equipo. El procedimiento consiste en descargar el archivo instalador del controlador a actualizar de la web Controladores y descargas, y ejecutarlo como administrador del sistema.

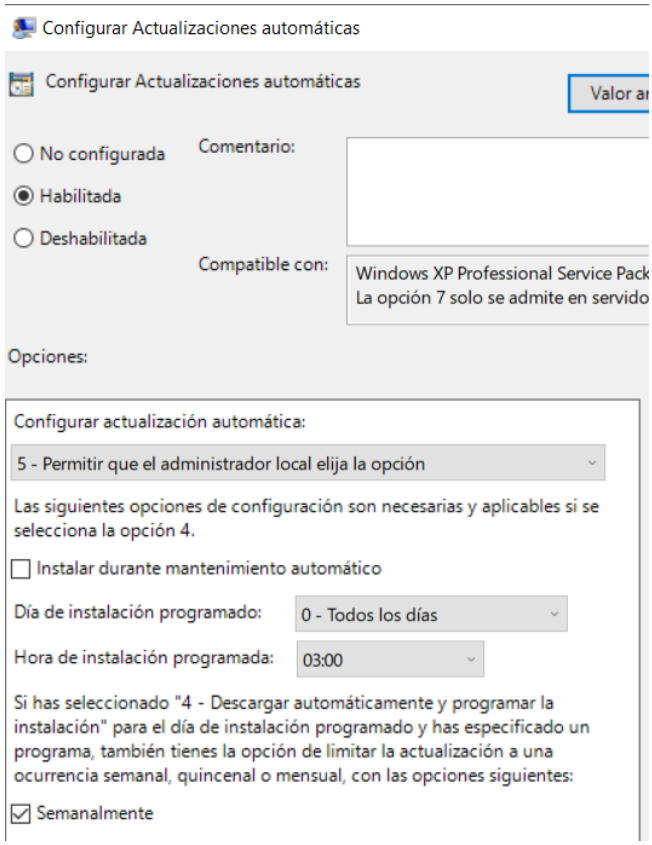
Nota: en algunos componentes, puede ser necesario seguir algunas indicaciones para actualizarlos. El sitio web ofrece comentarios para ello.

61. Windows 10 sigue un ciclo de actualizaciones en el que libera parches de seguridad el segundo martes de cada mes. Sin embargo, si las actualizaciones automáticas están habilitadas, el sistema operativo realiza un escaneo en busca de nuevas actualizaciones cada día.

62. **Se debe Mantener el sistema actualizado haciendo uso de la herramienta de *Windows Update*.**

63. Además, el administrador **deberá definir la configuración de las actualizaciones automáticas** en la siguiente ubicación del editor de directivas de grupo local, *Configuración del equipo > Plantillas administrativas > Componentes de Windows > Windows Update*, y configurar las siguientes políticas: *Configurar Actualizaciones automáticas > Habilitada* y configurada en *Permitir que el administrador local elija la opción; Permitir que los usuarios que no sean administradores reciban notificaciones de actualización > Deshabilitada; Permitir la instalación inmediata de Actualizaciones automáticas > Deshabilitada.*





5.8 MITIGACIÓN *SPECTRE* Y *MELTDOWN*

64. El producto, con la configuración ofrecida en esta guía, debería mitigar la mayoría de CVEs asociados a *Meltdown* y *Spectre*. Para proteger el equipo de estas dos vulnerabilidades, es necesario realizar un cambio en el registro de Windows, ya que existe un CVE que, tras la configuración actual, no se encuentra mitigado, el CVE-2018-3639.

65. **Para habilitar la protección del producto, es necesario abrir una consola de *PowerShell* como administrador, e ingresar los siguientes comandos**:

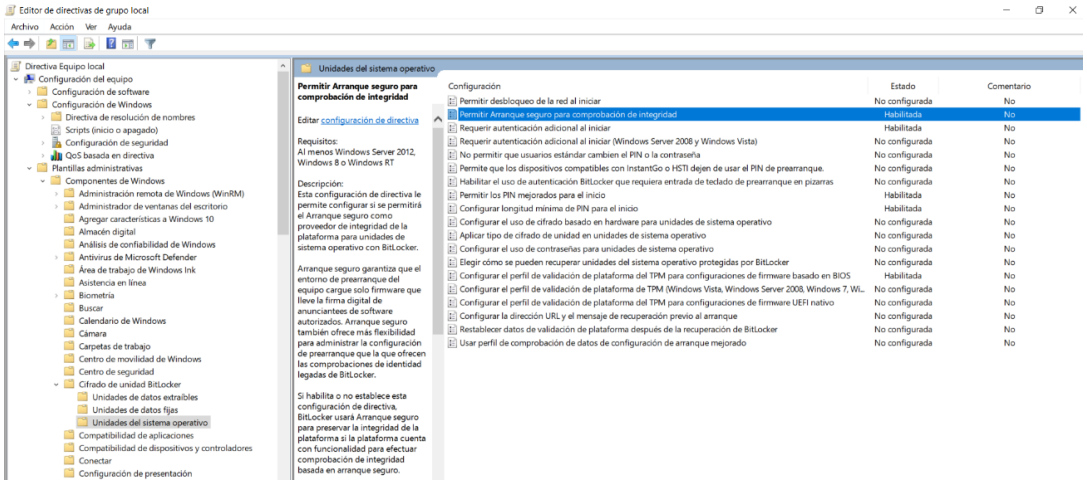
    - reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 8 /f
    - reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f

66. Tras aplicar estos comandos, es necesario **reiniciar el equipo** para que surtan efecto.

5.9 AUTO-CHEQUEOS

67. **Se debe hacer uso de la funcionalidad de auto-chequeo de integridad con la herramienta BitLocker**. Esta configuración permite comprobar la integridad de los componentes básicos del sistema durante el arranque.

68. Esta configuración se habilita desde el *Editor de directivas de grupo local, Plantillas administrativas > Cifrado de unidad BitLocker > Unidades del sistema operativo, junto a otras directivas de configuración de BitLocker*.



69. Además, también **se debe configurar la comprobación de integridad al arranque del sistema operativo con la utilidad *Secure Boot***. Esta utilidad impide el arranque del producto si no se validan la autenticidad e integridad de los ficheros utilizados en el arranque.

70. También **se deben realizar comprobaciones de los archivos del sistema con la herramienta *Windows System File Checker (SFC)*.** Esta herramienta se ejecuta desde la línea de comandos, o desde medios de recuperación de Windows.

71. Desde una línea de comandos o *Powershell* ejecutado como administrador, presionando el botón de inicio con el *click* derecho del ratón y seleccionando *Windows Powershell* (administrador) o Línea de comandos (administrador).

72. Una vez dentro, ejecutar *sfc /scannow* y presionar la tecla *Intro*. La herramienta comprobará la integridad de los archivos del sistema y los repara si es necesario.

73. **El equipo deberá ser reiniciado** al finalizar el proceso.

5.10 AUDITORÍA

5.10.1 REGISTRO DE EVENTOS

74. **El producto deberá configurarse para auditar distintos eventos**. Para ello, se deberá acceder al *Editor de directivas de grupo local, Configuración de Windows > Configuración de seguridad > Directivas locales > Directiva de auditoría* y configurar la auditoría de los siguientes eventos:

    a) Acceso a objetos. Esta configuración de seguridad determina si el sistema operativo audita los intentos de usuario de obtener acceso a objetos que no son de *Active Directory*. Solo se generan eventos de auditoría para objetos que tienen listas de control de acceso del sistema (SACL) especificadas.

b) Acceso al servicio de directorio. Esta configuración de seguridad determina si el sistema operativo audita los intentos de usuario de obtener acceso a objetos de *Active Directory*. Solo se generan eventos de auditoría para objetos que tienen listas de control de acceso del sistema (SACL) especificadas.

c) Cambio de directivas. Esta configuración de seguridad determina si el sistema operativo audita cada instancia de intentos de cambiar la directiva de asignación de derechos de usuario, la directiva de auditoría, la directiva de cuentas o la directiva de confianza.

d) Seguimiento de procesos. Esta configuración de seguridad determina si el sistema operativo audita eventos relacionados con procesos como la creación de un proceso, la finalización de un proceso, identificadores duplicados y acceso indirecto a objetos.

e) Uso de privilegios. Esta configuración de seguridad determina si debe auditarse cada instancia de un usuario que ejerce un derecho de usuario.

f) Eventos de inicio de sesión. Esta configuración de seguridad determina si el sistema operativo audita cada instancia de un intento de usuario de iniciar o cerrar sesión en este equipo.

g) Eventos de inicio de sesión de cuenta. Esta configuración de seguridad determina si el sistema operativo audita cada vez que el equipo valida las credenciales de una cuenta.

h) Auditar eventos del sistema. Esta configuración de seguridad determina si el sistema operativo audita los siguientes eventos:

- Intento de cambio de hora del sistema
- Intento de inicio o cierre del sistema de seguridad
- Intento de carga de componentes de autenticación extensible
- Pérdida de eventos auditados debido a errores del sistema de auditoría
- Tamaño del registro de seguridad que excede un umbral de advertencia configurable.

i) Administración de cuentas. Esta configuración de seguridad determina si debe auditarse cada evento de administración de cuentas en un equipo.

75. Estos eventos se pueden consultar en la herramienta *Visor de eventos*.

5.10.2 ALMACENAMIENTO LOCAL

76. El producto realiza un almacenamiento local de los registros de auditoría, en distintos directorios y con un tamaño máximo del registro. Se sobreescriben los más antiguos. Según el tipo de evento, la configuración es la siguiente:

- Aplicación:

- Ruta: *%SystemRoot%\System32\Winevt\Logs\Application.evtx*
- Tamaño máximo de registro: 32768 KB

- Seguridad:
  - Ruta: *%SystemRoot%\System32\Winevt\Logs\Security.evtx*
  - Tamaño máximo de registro: 163840 KB
- Sistema:
  - Ruta: *%SystemRoot%\System32\Winevt\Logs\System.evtx*
  - Tamaño máximo de registro: 32768 KB

77. Para consultar o modificar la configuración de los registros de eventos, se deberá acceder al *Visor de eventos, Registros de Windows* y seleccionar el tipo de evento que corresponda.

5.11 *BACKUP*

78. La configuración de seguridad determina que **únicamente los usuarios pertenecientes al grupo Administradores pueden realizar copias de seguridad de archivos y directorios.**
79. Para realizar una copia de seguridad, acceder a *Configuración > Actualización y seguridad > Copia de seguridad.* Se solicitará una unidad sobre la que se almacenará la copia de seguridad.
80. Es posible configurar la periodicidad a la que se realizan las copias de seguridad, así como las carpetas a copiar.
81. Es importante tener en cuenta que esta copia de seguridad no se encuentra cifrada, por lo que **será necesario aplicar una protección adicional a esta unidad de almacenamiento.**

5.12 SERVICIOS DE SEGURIDAD

5.12.1 CONFIGURACIÓN DEL ANTIVIRUS

82. **Se debe asegurar que el servicio de Windows Defender como Antivirus está activo**. Para ello, es necesario desactivar la directiva de seguridad que desactiva el antivirus de Windows Defender:

    a) Acceder a Editor de directivas de grupo local, *Plantillas administrativas > Antivirus de Windows Defender > Desactivar Antivirus de Microsoft Defender*, y deshabilitar la opción.

    b) Una vez deshabilitada esta directiva, activar *Windows Defender* en *Inicio > Configuración > Actualización y seguridad > Seguridad de Windows > Abrir Seguridad de Windows*, y habilitar la protección contra virus y amenazas.

83. Es recomendable revisar la configuración del antivirus de Windows Defender en el caso de instalar otro antivirus en el sistema según las directrices de la organización, deshabilitándolo si es necesario.

5.12.2 CONFIGURACIÓN DEL CORTAFUEGOS

84. **El cortafuegos de Windows Defender se configurará de la siguiente manera**:

- Perfil de dominio
  - *Firewall*: **activo**
  - Conexiones entrantes: **bloquear**
  - Conexiones salientes: **permitir**
- Perfil privado
  - *Firewall*: **activo**
  - Conexiones entrantes: **bloquear**
  - Conexiones salientes: **permitir**
- Perfil público
  - *Firewall*: **activo**
  - Conexiones entrantes: **bloquear**
  - Conexiones salientes: **permitir**

85. **Se debe hacer uso de la funcionalidad del sistema operativo de protección de aplicaciones basada en reputación**, llamada *SmartScreen*. La configuración del producto mantiene este filtro activado y no es posible desactivarse. Esta configuración se habilita en la herramienta *gpedit.msc*, *Directivas de Equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Explorador de archivos*, y marcar *Habilitado (Advertir e impedir la omisión)* en *Configurar SmartScreen de Windows Defender.*

5.12.3 HERRAMIENTAS DE DIAGNÓSTICO

86. Windows 10 posee herramientas de línea de comandos que permiten realizar comprobaciones sobre el estado del módulo de plataforma segura (TPM), del cifrado del disco con BitLocker y del arranque seguro con SecureBoot.

87. **Dichas comprobaciones deben ser realizadas** y, para ello, se deberá abrir una línea de comandos como administrador y ejecutar:

a) Para el diagnóstico del módulo TPM: *tpmtool getdeviceinformation.*

b) Para el diagnóstico del cifrado en disco con BitLocker: *manage-bde -status*.

c) Para el diagnóstico de arranque seguro, o *SecureBoot* (desde *Powershell*): *Confirm-SecureBootUEFI*.

6. FASE DE OPERACIÓN

88. En la operativa habitual de Windows 10 se debe:

- **Realizar chequeos** con Windows Defender para comprobar archivos maliciosos.
- **Revisar los registros de auditoría**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas.
- **Verificar** que los **componentes** de Windows se encuentran **actualizados**.
- **Comprobar actualizaciones de seguridad para BIOS o controladores** que no se actualicen desde *Windows Update* en la página oficial del producto.
- En las operaciones de mantenimiento del equipo, **realizar rutinas de comprobación de integridad de archivos y configuración de BitLocker y TPM.**

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Registro de las licencias	☐	☐	
CONFIGURACIÓN			
Autenticación. Creación de usuarios	☐	☐	
Autenticación. Configuración de *BitLocker*	☐	☐	
Autenticación. Configuración de contraseña BIOS UEFI	☐	☐	
Administración. Configuración de directivas de contraseñas	☐	☐	
Administración Configuración de acceso al editor de registro	☐	☐	
Configuración de interfaces	☐	☐	
Configuración de protocolos seguros	☐	☐	
Configuración de *AppLocker*	☐	☐	
Sincronización horaria	☐	☐	
Actualizaciones	☐	☐	
Configuración de mitigación *Spectre* y *Meltdown*	☐	☐	
Realización de auto-chequeos	☐	☐	
Configuración de la auditoría	☐	☐	
Activación de servicios de seguridad	☐	☐	
OPERACIÓN			
Realización de chequeos para detectar archivos maliciosos	☐	☐	
Autenticación. Log in a través de Windows	☐	☐	
Autenticación. Log in a través de *BitLocker*	☐	☐	
Autenticación. Log in a través de BIOS UEFI	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Revisión de los registros de auditoría	☐	☐	
Actualización de componentes de Windows	☐	☐	
Actualización de BIOS y controladores	☐	☐	
Realización de comprobaciones de integridad de archivos, *Bitlocker* y TPM	☐	☐	

8. REFERENCIAS

[CCN-STIC-599B19] CCN-STIC-599B19. Implementación de seguridad sobre Microsoft Windows 10 (Cliente independiente), septiembre 2019

[CCN-STIC-807] CCN-STIC-807. Criptología de empleo en el Esquema Nacional de Seguridad, mayo 2022

[TAXF6] Taxonomía de referencia para productos de Seguridad TIC. Febrero 2019. Anexo F6: Plataformas de Confianza.

9. ABREVIATURAS

GPO *Group Policy Object*

LTSC *Long-Term Servicing Channel* (Canal de mantenimiento a largo plazo).

PIN *Personal Identification Number* (Número de identificación personal).

SFC *System File Check*er (Herramienta de comprobación de archivos).

TPM *Trusted Platform Module* (Módulo de Plataforma Segura).

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL