



SIN CLASIFICAR



Informe de Amenazas CCN-CERT IA-06/16

Privacidad en Microsoft Windows 10

(Puestos de Trabajo en las
Administraciones Públicas)

Marzo 2016

SIN CLASIFICAR

**LIMITACIÓN DE RESPONSABILIDAD**

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE EL CCN-CERT	4
2. PRÓLOGO	4
3. SOBRE EL PRESENTE INFORME.....	5
4. ESCENARIOS	6
5. PRUEBAS EFECTUADAS Y COMPONENTES AFECTADOS	9
5.1. Componentes y servicios afectados.....	9
6. COMUNICACIONES	10
7. APLICACIÓN DE SEGURIDAD	11
7.1. Opciones de privacidad	11
7.2. Configuración de seguridad y aplicación de directivas a través de plantillas de seguridad.....	19
7.2.1. Configuración de servicios.....	19
7.2.2. Plantillas administrativas configuradas	22
7.2.3. Componentes de Windows	23
7.2.4. Sistema	23
8. COMPONENTES DE TELEMETRÍA.....	24
9. CONCLUSIONES.....	26
10.CONTACTO	29
ANEXO A. SERVIDORES DE TELEMETRÍA.....	30
ANEXO B. LISTADO DE CONEXIONES ESTABLECIDAS.....	32

1. SOBRE EL CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el CERT Gubernamental/Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas clasificados, de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. PRÓLOGO

En los últimos años, se ha producido una significativa tendencia al intercambio de información con Internet de forma más habitual que el que hasta la fecha soportaban los sistemas operativos especialmente con la aparición de *Ms Windows 8* y el avance en el empleo de sistemas operativos, la tecnología *Cloud Computing* y el uso de aplicaciones orientadas a dispositivos móviles.

Los entornos de *Big Data*, tan ampliamente extendidos, presentan entre otros, como objetivos obtener información de navegación en Internet, uso de los sistemas, telemetría, etc. Se busca con ello la mejora posterior de los propios sistemas. Este hecho por ejemplo redundaría en una mejora en la experiencia del usuario, pero todo ello a costa de posibles repercusiones negativas en cuanto a la privacidad.

Lógicamente, en este sentido Microsoft no es una excepción, habiendo dotado a sus nuevos sistemas operativos cliente de características destinadas a ese fin. La *Tienda de Microsoft* y la incorporación de las aplicaciones tipo *METRO*, ahora denominadas *Modern Apps*, operan por debajo de los sistemas, siendo complejo en ocasiones conocer realmente cuál es su operativa, qué información recolectan de los equipos en los que están instaladas y a quién envían esa información.

Esto unido a los actuales sistemas de telemetría y otros componentes, que como *Cortana* aparecen en *Ms Windows 10*, generan una alta incertidumbre en lo que respecta a la información recopilada.

En este punto, debe tenerse en cuenta que un sistema operativo como *Ms Windows 10* recién instalado y sin aplicar medidas de seguridad y privacidad, realiza sistemática y continuamente envíos de información a Microsoft. La finalidad que se persigue es la mejora de la experiencia del usuario mediante el estudio de sus costumbres, modos de escritura, tipos de aplicaciones, ficheros que utiliza, junto a otros aspectos de índole similar.

Microsoft, en respuesta a las dudas generadas por los contratos de licencia del sistema operativo, ha especificado ciertas condiciones relativas a la información que le otorgan el derecho a acceder, revelar y preservar la información de sus clientes. Esto incluye comunicaciones privadas o información almacenada en los dispositivos, atendiendo a que el acceso a dicha información se realiza con una clara intención de buena fe y sólo en casos necesarios para proteger y preservar los derechos de sus clientes, así como evitar el uso incorrecto de sus sistemas (fines maliciosos), proteger los derechos de propiedad de Microsoft o colaborar en el cumplimiento de las leyes internacionales.

Sin embargo, es totalmente legítimo mantener la privacidad en los casos que se requiera. El mismo Microsoft proporciona medidas que permiten conservar dicha privacidad, mediante políticas de grupo así como el establecimiento de configuraciones directamente relacionadas con la seguridad y la privacidad de los usuarios. En este sentido, Microsoft se encuentra trabajando en la emisión de informes y mecanismos que despejen reticencias y arrojen transparencia en la funcionalidad de nuevos componentes.

3. SOBRE EL PRESENTE INFORME

El presente informe se destina a la evaluación específica de la seguridad y privacidad del sistema operativo *MS Windows 10*. De igual modo, con el mismo se pretende emitir conclusiones de valor para la implementación de puestos de trabajo con el citado sistema y en el marco de operación de las diferentes Administraciones Públicas.

Se excluye del alcance del presente informe la configuración de aquellos sistemas incluidos en las siguientes categorías:

- Puestos de trabajo vinculados a redes clasificadas.
- Sistemas aislados, altamente críticos como los correspondientes a sistemas de control tipo SCADA o de control hospitalario entre otros.

Para dichos sistemas se recomienda la lectura del Informe CCN-CERT IA-08-16 "Privacidad en Microsoft Windows 10 (Equipos Críticos Aislados y Redes Clasificadas)".

Los análisis, valoraciones y conclusiones del presente documento tienen en consideración la heterogeneidad de las diferentes Administraciones Públicas. En este sentido, es una realidad la existencia de diferentes acuerdos establecidos con Microsoft por parte de los múltiples organismos, tanto en el mantenimiento de soporte como en la implementación de las distintas versiones del sistema operativo.

En el caso del soporte ofrecido por el fabricante influyen significativamente algunos de los componentes que incorpora *MS Windows 10*, tales como los de telemetría. Estos componentes presentan como objetivo la mejora del servicio ofrecido en virtud de los acuerdos a los que se hubiera llegado con el fabricante.

No obstante, debe tenerse también en consideración que estas funcionalidades podrían no ser requeridas por la totalidad de los sistemas afectados. Es por ello que se

evalúa la posibilidad de controlar o limitar aquellos componentes que no fueran de necesidad en un determinado escenario.

De igual modo, el informe tiene en consideración la evolución en la forma de entender y usar los sistemas operativos modernos. En este sentido, elementos tales como las *Modern App* deben observarse desde la panorámica de que su uso se ha extendido a dispositivos móviles y tabletas. Este aspecto es ya una realidad para los sistemas más convencionales.

Los distintos análisis realizados se llevan a efecto por lo tanto desde el punto de vista de los nuevos sistemas operativos y el control que las organizaciones deberían tener de ellos, tanto en lo que respecta a la privacidad como a su implantación en un entorno corporativo.

El presente informe recoge el resultado de una serie de análisis cuyo objetivo no es otro que definir y conocer las condiciones de seguridad relacionadas con el envío de información hacia el exterior que realiza el sistema operativo cliente *MS Windows 10*. El informe recogerá también aquellas medidas de seguridad de posible aplicación que permiten incrementar de forma significativa el grado de confianza en el sistema. También determinará la versión del sistema más óptima para la tipología de equipo a la que se orienta el presente informe.

4. ESCENARIOS

Las pruebas y análisis se han realizado en diferentes entornos, expresamente implementados al efecto, y que de una u otra forma emulan entornos corporativos habituales. Estos escenarios son:

- Escenario en un entorno de dominio compuesto por los siguientes elementos:
 - Un equipo controlador de dominio con *MS Windows Server 2012 R2* con las actualizaciones de *Windows Update* aplicadas hasta el 10 de noviembre 2015.
 - Un equipo cliente *MS Windows 10 Enterprise LTSB 64 bits* con las actualizaciones de *Windows Update* aplicadas hasta el 10 de noviembre 2015.
- Escenario en un entorno de dominio compuesto por los siguientes elementos:
 - Un equipo controlador de dominio con *MS Windows Server 2012 R2* con las actualizaciones de *Windows Update* aplicadas hasta el 10 de noviembre de 2015.
 - Un equipo cliente *MS Windows 10 Enterprise CBB 64 bits* con las actualizaciones de *Windows Update* aplicadas hasta el 10 de noviembre 2015.
 - Equipo independiente con un cliente *MS Windows 10 Enterprise CBB 32 bits* con las actualizaciones de *Windows Update* aplicadas hasta el 10 de noviembre 2015.

- Un equipo cliente *MS Windows 10 Enterprise LTSB 64 bits* con las actualizaciones de *Windows Update* aplicadas hasta el 10 de noviembre 2015.

Durante los meses de enero y febrero de 2016, se han realizado las pruebas adicionales de comportamiento y funcionalidad de los componentes de telemetría y *Tienda de Microsoft*.

Para definir con mayor claridad el alcance de las pruebas realizadas, se hace necesario conocer las diferencias existentes entre las versiones disponibles del sistema operativo *MS Windows 10*, así como la nueva categorización de opciones de mantenimiento del sistema.

Los profesionales técnicos están familiarizados con las distintas tipologías de versiones del producto: domésticas, profesionales y de negocio. La nomenclatura en inglés de dichas versiones es *Home*, *Professional* (también denominada *Pro*) y *Business*. Adicionalmente existe una versión específica para educación. Cada una de ellas aporta diferentes funcionalidades en función del entorno de implementación, así el usuario doméstico tiene a su disposición una solución que se adaptaba a sus necesidades, la versión *home*.

Para entornos de tipo corporativo, Microsoft ha proporcionado dos líneas de productos diferenciadas, las versiones *Profesional* y *Business*. La diferencia fundamental radica en que esta última aporta una serie de características que posibilitan un mayor control corporativo, incorporando por ejemplo soluciones de seguridad tales como *Microsoft Bitlocker Administration and Monitoring*, que no se encontrarían disponibles para la primera. Este hecho redunda, como es lógico, en el coste de la versión.

Adicionalmente a esta modalidad de versiones que se mantiene en *MS Windows 10*, aparece una nueva categorización diferenciada fundamentalmente en las opciones de mantenimiento. El objetivo principal es asegurarse que los sistemas no se encuentran desactualizados, con el consiguiente riesgo que ello supone. De este modo, cuando ha transcurrido un determinado tiempo de "no actualización" el sistema perderá funcionalidades.

Dentro de las opciones de mantenimiento de *MS Windows 10*, se encuentran disponibles tres (3) opciones:

- **CB** (Rama actual o *Current Branch*).
- **CBB** (Rama actual para empresas o *Current Branch for Business*).
- **LTSB** (Rama de mantenimiento a largo plazo para empresas o *Long Term Servicing Branch*)

Entre las diferentes opciones CB, CBB y LTSB que proporciona Microsoft para *MS Windows 10*, es interesante mencionar para cada caso la disponibilidad de actualizaciones y el ciclo de vida de mantenimiento de cada opción:

- Para la opción CB, la duración mínima del ciclo de vida de mantenimiento es de cuatro (4) meses aproximadamente.

- Para la opción *CBB*, la duración mínima del ciclo de vida de mantenimiento es de ocho (8) meses aproximadamente.
- Para la opción *LTSB*, la duración mínima del ciclo de vida de mantenimiento es de diez (10) años.

Debe entenderse lo anterior como el plazo máximo que un sistema podrá mantenerse operacional sin haberse realizado la debida actualización del mismo. Esto en ningún caso quiere indicar que los periodos máximos de desactualización deban ser observados como referencia en lo que a aplicación de actualizaciones se refiere. Las buenas prácticas de seguridad, de absoluta validez para *MS Windows 10*, establecen la necesidad de mantener los sistemas actualizados en todo momento, habiendo aplicado las últimas actualizaciones disponibles en materia de seguridad.

Adicionalmente a lo expuesto en los párrafos anteriores, es interesante también reseñar que la opción *LTSB*, con respecto a las otras, presenta también diferencias en cuanto a las propias funcionalidades del producto. De este modo la mencionada opción no presenta entre otros, elementos como *Cortana*, *Microsoft Edge* o la *Tienda Microsoft*. En definitiva, la opción *LTSB* de *MS Windows 10* no aporta todas las características del sistema disponibles para las opciones *CB* y *CBB*.

Por tanto, la opción *LTSB* no presenta el mismo mantenimiento de funcionalidad que las otras dos opciones existentes. Así resultaría factible que mientras las opciones *CB* y *CBB* incorporarán mejoras funcionales de producto, éstas no se encontrarán disponibles necesariamente para la versión *LTSB* aunque sí se mantendría en su ciclo de vida las actualizaciones de seguridad, pero no de aquellas otras correspondientes a mejoras funcionales.

Por último, es necesario tener en consideración la disponibilidad de las opciones descritas para las diferentes versiones que el sistema operativo *MS Windows 10* presenta. De este modo:

- Opción *CB*. Disponible para versiones *Home*, *Education*, *Pro* y *Enterprise*.
- Opción *CBB*. Disponible para las versiones *Education*, *Pro* y *Enterprise*
- Opción *LTSB*. Disponible *Enterprise*.

Para más información sobre las diferentes opciones de mantenimiento es posible dirigirse a la siguiente dirección URL:

[https://technet.microsoft.com/es-es/library/mt598226\(v=vs.85\).aspx](https://technet.microsoft.com/es-es/library/mt598226(v=vs.85).aspx)

Los escenarios de pruebas contemplados asumen versiones de tipo *Enterprise* con las opciones de ámbito corporativo, *CBB* y *LTSB*. En las opciones *CB* y *CBB*, los resultados para versiones *Pro* y *Enterprise* ofrecerían similares resultados. Se llevan a efecto los análisis con las versiones *Enterprise* debido a la orientación más operacional desde el punto de vista corporativo con dicha versión del producto.

Para los mencionados escenarios de prueba y en lo referente a opciones, se ha optado por emplear *CBB* y *LTSB* ya que las mismas se encuentran principalmente destinadas a uso empresarial.

5. PRUEBAS EFECTUADAS Y COMPONENTES AFECTADOS

Las pruebas efectuadas se han llevado a cabo en tres líneas. En la primera de ellas se han realizado análisis de conectividad con los sistemas operativos en las condiciones predeterminadas de instalación. Este hecho contempla que el sistema mantiene múltiples mecanismos de comunicación con Internet y no se han deshabilitado ninguna de las opciones que implementa.

La segunda de las pruebas ha sido llevada a efecto mediante la aplicación de los controles de privacidad que facilita el propio sistema operativo y que de una u otra forma son visibles para un usuario convencional. Lo cual va orientado fundamentalmente al control de determinada información que será remitida a Microsoft.

Las últimas pruebas corresponden al bastionado de los sistemas, aplicando condiciones de seguridad haciendo uso para ello de políticas de seguridad, plantillas administrativas y el control de determinados servicios, tal y como se plantean en las guías CCN-STIC tanto de la serie 500 para redes clasificadas, como de la serie 800 para el cumplimiento del Esquema Nacional de Seguridad (ENS).

5.1. Componentes y servicios afectados

Dentro de las pruebas llevadas a cabo, se ha tomado como objeto inicial de las mismas, la identificación de todos aquellos componentes de *MS Windows 10* que pudieran llegar a realizar exfiltración de información con conectividad a servicios de Microsoft o a otros proveedores.

En este sentido, se identifican los siguientes componentes y servicios:

- Sistema de *Telemetría*.
- *Tienda* de Microsoft.
- *Modern App*.
- Sistema Experiencia de Usuario.
- *Windows Defender*.
- Servicio *Cortana*.
- *Microsoft Edge*.
- *Microsoft Search*.
- *Microsoft Internet Explorer*.
- *Windows Smart Screen*.
- *Windows Update*.

Debe tenerse en consideración que algunos de los componentes citados son específicos de *MS Windows 10* tales como *Cortana* o *Microsoft Edge*, mientras que otros como *Windows Defender* ya existían en versiones previas del sistema operativo cliente Microsoft.

Los elementos mencionados no funcionan de forma idéntica en todas las versiones del sistema operativo MS Windows 10. En este sentido, la versión LTSB de MS Windows 10 Enterprise no incluye ninguna de las siguientes funcionalidades:

- Servicio Cortana.
- Microsoft Edge.
- Tienda de Microsoft.
- Aplicaciones METRO o Modern Apps.

6. COMUNICACIONES

En los procesos de análisis efectuados, se han identificado comunicaciones a diferentes direcciones IP públicas a través de puertos TCP. Los puertos identificados han sido 80 y 443, correspondientes a conexiones HTTP y HTTPS respectivamente.

Se proporciona a través del Anexo A un listado de servidores de Telemetría identificables por Microsoft a los que MS Windows 10 podría remitir información.

Como Anexo B del presente informe, se adjunta un archivo MS Excel con un ejemplo del listado de conexiones identificadas, así como las aplicaciones o procesos que las habrían originado. En dicho listado se pueden identificar conexiones efectuadas por los puestos de trabajo con sistemas remotos, bien cuando una aplicación es iniciada o bien cuando el equipo se encuentra sin actividad por parte del usuario.

Las conclusiones que se desprenden del análisis de las conectividades son:

- Existen múltiples procesos de conectividad hacia redes externas, fundamentalmente de los siguientes procesos: *SVCHOST*, *EXPLORER*, *SYNCHOST*, *INTERNET EXPLORER*, *EDGE*, *WSAPPX* Y *MSMPENG*.
- Los procesos de conectividad se originan fundamentalmente en la opción CBB desde los siguientes componentes: *Modern Apps*, *Tienda*, *Windows Defender*, *Cortana* y *Servicios de Telemetría*. En el caso de la opción LTSB, estos procesos se estarían produciendo desde los siguientes componentes *Tienda*, *Windows Defender* y *Servicios de Telemetría*.
- Se realizan conexiones puntuales bien cuando se ejecuta una aplicación o bien cuando se desencadena un proceso programado. Esta circunstancia para la opción CBB se da con los siguientes elementos: *Windows Update*, *Internet Explorer*, *Microsoft Edge* y *Windows Smart Screen*. En el caso de la opción LTSB, los elementos a considerar serían los siguientes: *Windows Update*, *Internet Explorer* y *Windows Smart Screen*.
- En el caso de la opción CBB, elementos como *Cortana*, *Modern Apps* o servicios vinculados a la telemetría, mantienen conexiones prácticamente constantes con servicios externos. En el caso de las *Modern Apps* requieren un proceso de actualización constante de la información que dichos componentes suministran al usuario. El servicio de *Cortana* se encuentra activo como mecanismo de ayuda al usuario, realizando también envíos de

información de forma continuada. Idéntica circunstancia se da con los servicios de telemetría donde el sistema envía valores de uso y conectividad de forma constante a Microsoft.

- En el caso de la opción LTSB, se limitaría dicha conectividad a los sistemas de telemetría.

7. APLICACIÓN DE SEGURIDAD

Teniendo en cuenta las condiciones de conectividad constante por parte de los sistemas y evidenciando que bajo determinadas condiciones puede evaluarse que información es remitida (conexiones HTTP) pero en otras esto no es factible (conexiones HTTPS), se procede a aplicar diferentes medidas de seguridad.

Estas acciones presentan como objeto determinar los controles existentes a nivel de condiciones de privacidad que permitan limitar el tipo de conexiones que se estarían produciendo. También se evalúa la posibilidad de limitar igualmente determinadas funcionalidades cuando así lo requieran las condiciones de seguridad del sistema.

Para ello se aplican diferentes medidas:

- Opciones de privacidad.
- Configuración de servicios y directivas a través de plantillas administrativas.

7.1. Opciones de privacidad

Los sistemas MS Windows 10 proporcionan opciones de privacidad que deberán ser gestionadas para controlar el envío de información como la ubicación, datos de usuario, navegación, usos del sistema, etc. Las mismas son establecidas por Microsoft y pueden ser gestionados por un usuario convencional.



Imagen 1.- Personalización de características iniciales de MS Windows 10.

De este modo, es posible deshabilitar una serie de elementos relacionados con la privacidad en las opciones iniciales, tal y como se muestra en las siguientes imágenes:

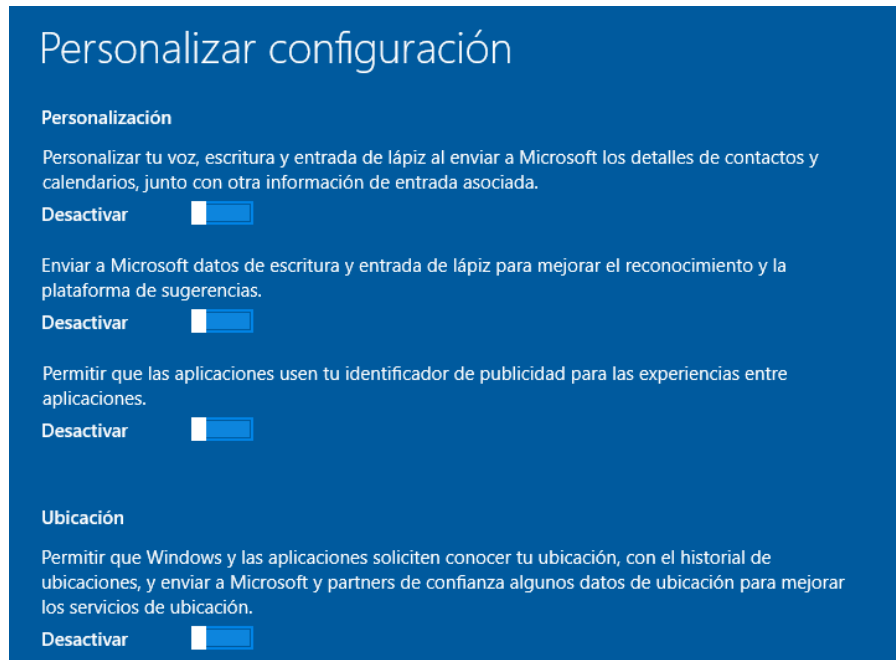


Imagen 2.- Personalización de la privacidad

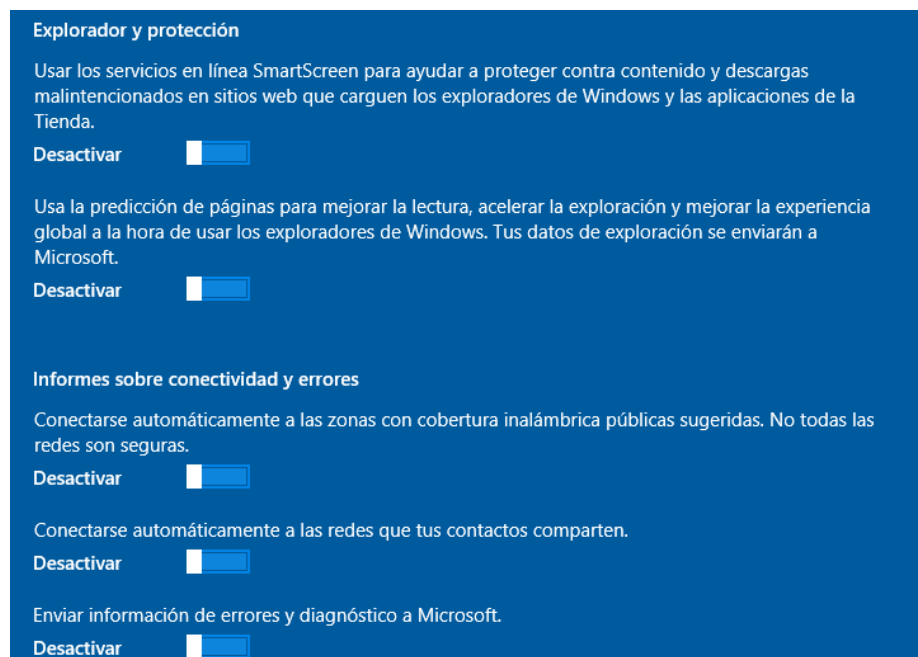


Imagen 3.- Privacidad exploración y protección.

En el caso de la opción LTSB de MS Windows 10 Enterprise no es necesario deshabilitar Cortana o Microsoft EDGE, ya que esta versión no incluye ninguno de estos dos elementos.

De igual modo no se incluyen tampoco la Tienda de Microsoft ni aplicaciones METRO o Modern Apps. Sin embargo, sería necesario deshabilitar el resto de las opciones anteriormente descritas en el presente documento.

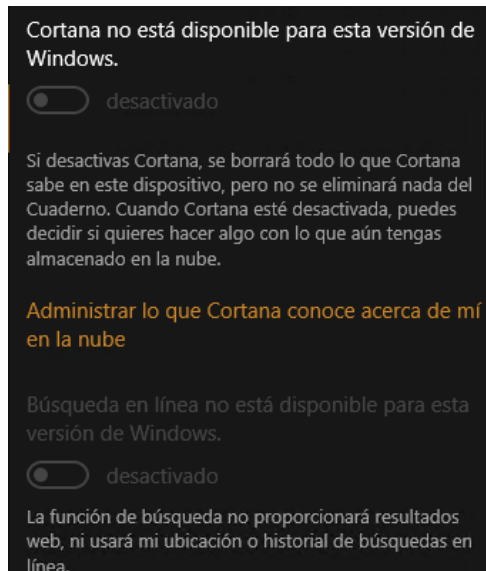


Imagen 4.- Cortana permanece desactivado en la versión LTSB de MS Windows 10 Enterprise.

Accediendo al menú de Configuración, se han deshabilitado más características relacionadas directamente con la privacidad del sistema. Para ello, en el apartado de Privacidad se han configurado una serie de parámetros tal y como se indica a continuación.

Se comprueba inicialmente que la Ubicación estaba desactivada previamente tras los pasos iniciales y tras ello se ha deshabilitado la herramienta que envía información a Microsoft sobre cómo escribe el usuario, ya que a priori se trata de una aplicación que registra teclado y podría estar recogiendo información a través de la captura de pulsaciones en el mismo.

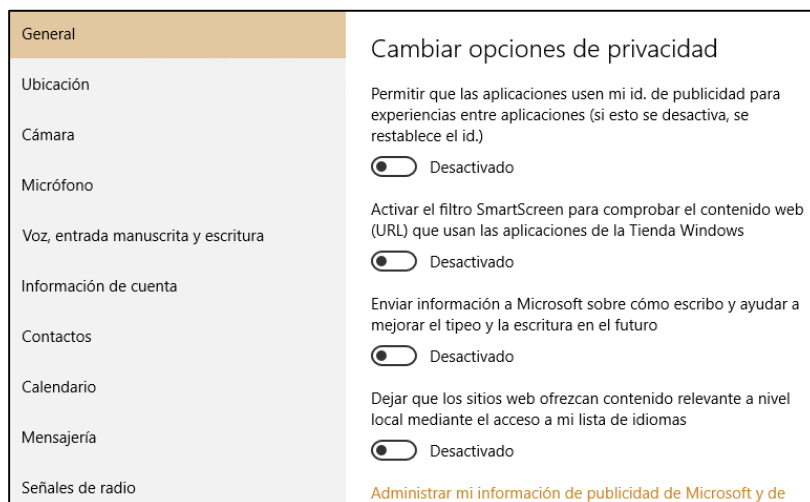


Imagen 5.- Opciones de privacidad

Se impide también que las aplicaciones puedan acceder a la cámara de forma automática.

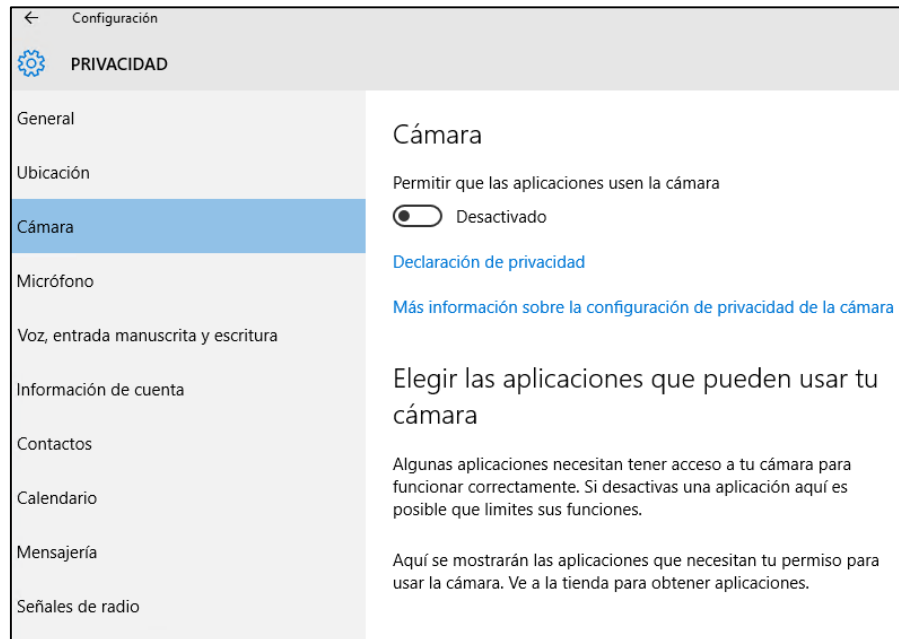


Imagen 6.- Opciones de privacidad de Webcam

Siguiendo la misma línea que en acciones anteriores, se desactiva la información relativa a las *Cuentas* y *Contactos*, que permitirían remitir información a Microsoft que puede considerarse sensible.

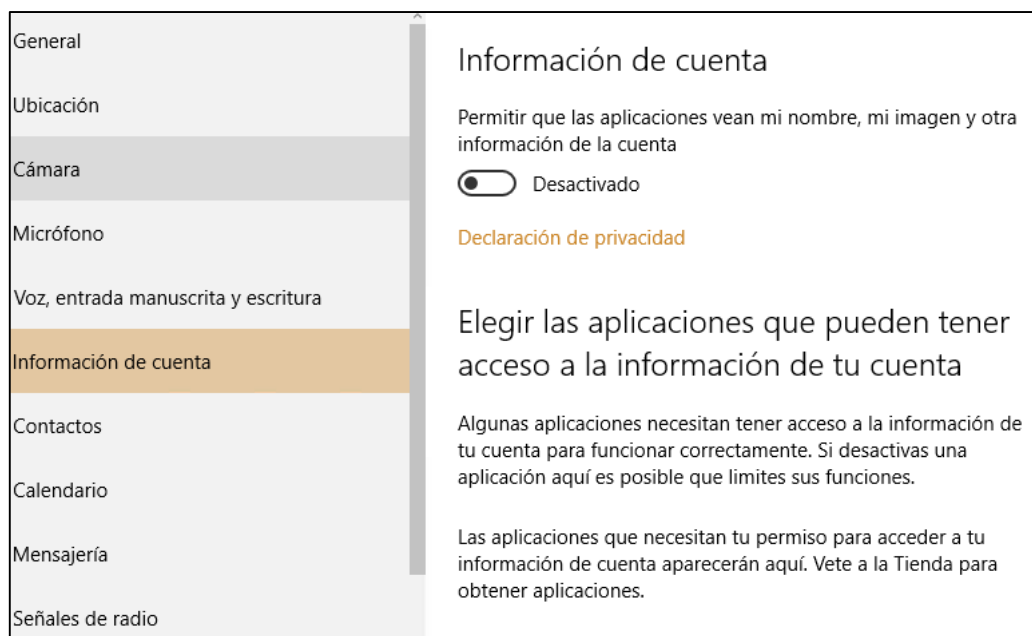


Imagen 7.- Opciones de privacidad de Cuenta

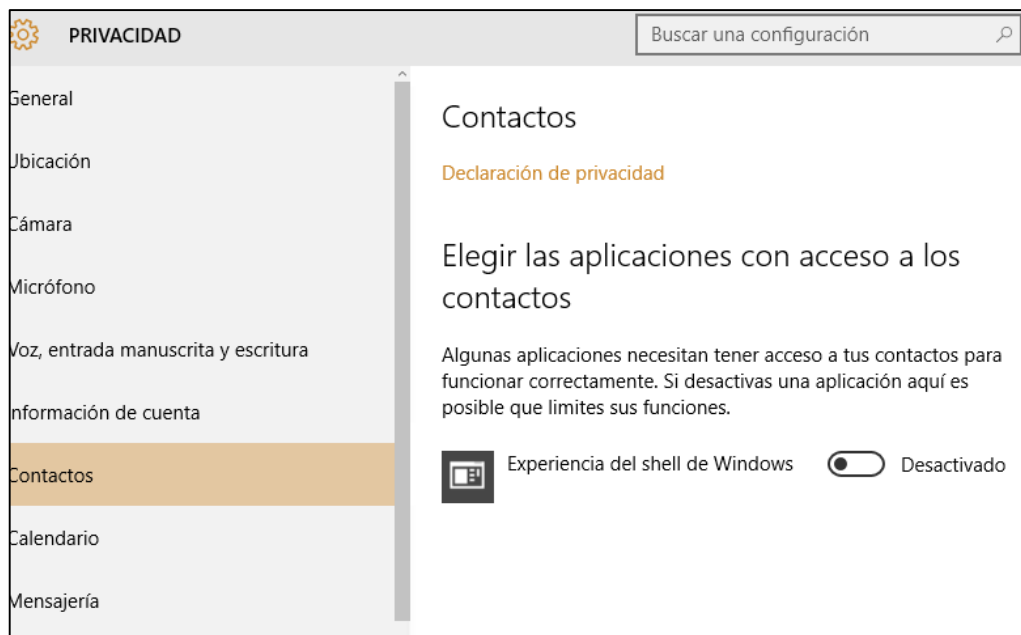
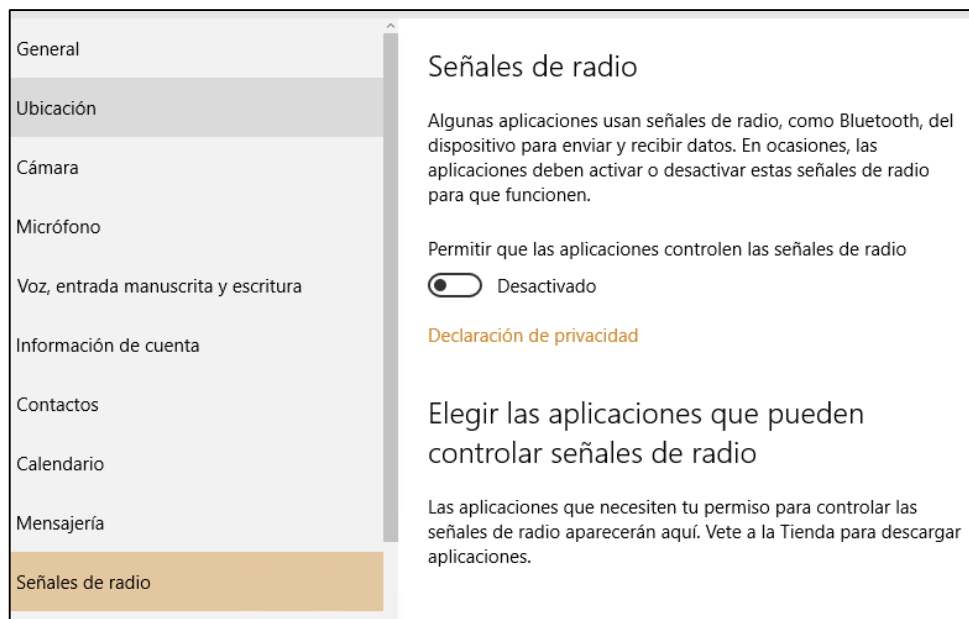
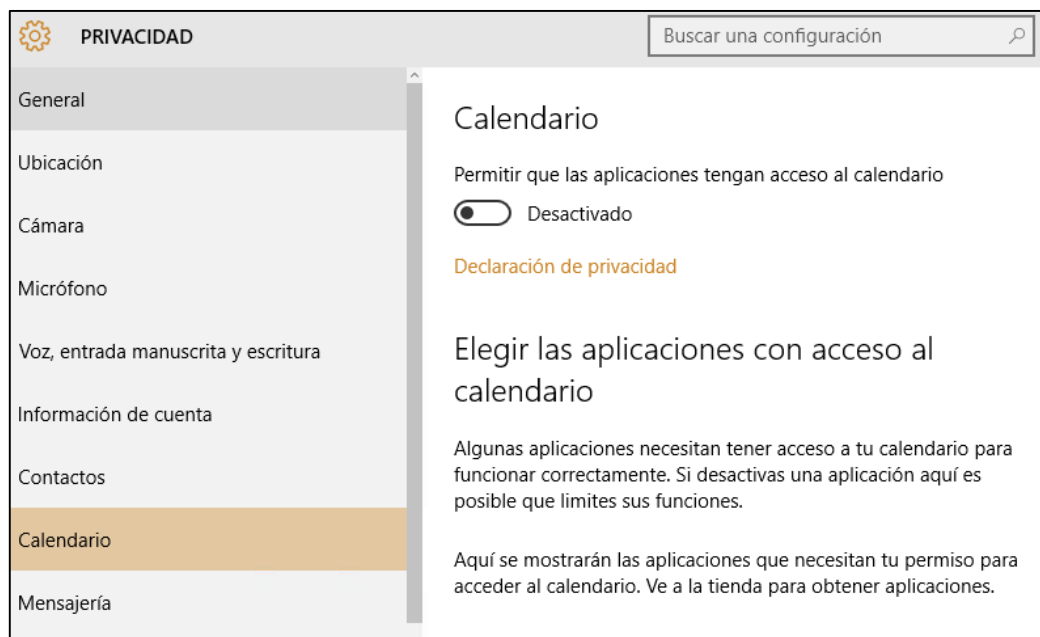


Imagen 8.- Opciones de privacidad de Contactos

Se desactiva el acceso al Calendario. Esta opción se podrá mantenerse desactivada siempre y cuando no sea necesario su uso por parte de una aplicación que acceda o necesite de dicha funcionalidad. Así mismo, se deshabilita el envío de MMS y las Señales de radio. Esta última característica solo se debería habilitar en caso de utilizar dispositivos *Bluetooth*.



Imagen 9.- Opciones de privacidad de mensajería

*Imagen 10.- Opciones de privacidad de radio**Imagen 11.- Opciones de privacidad de calendario.*

Del mismo modo, se deshabilita la *Sincronización* con otros dispositivos y se minimiza el envío de información de datos de diagnóstico que se enviará a *Microsoft*.

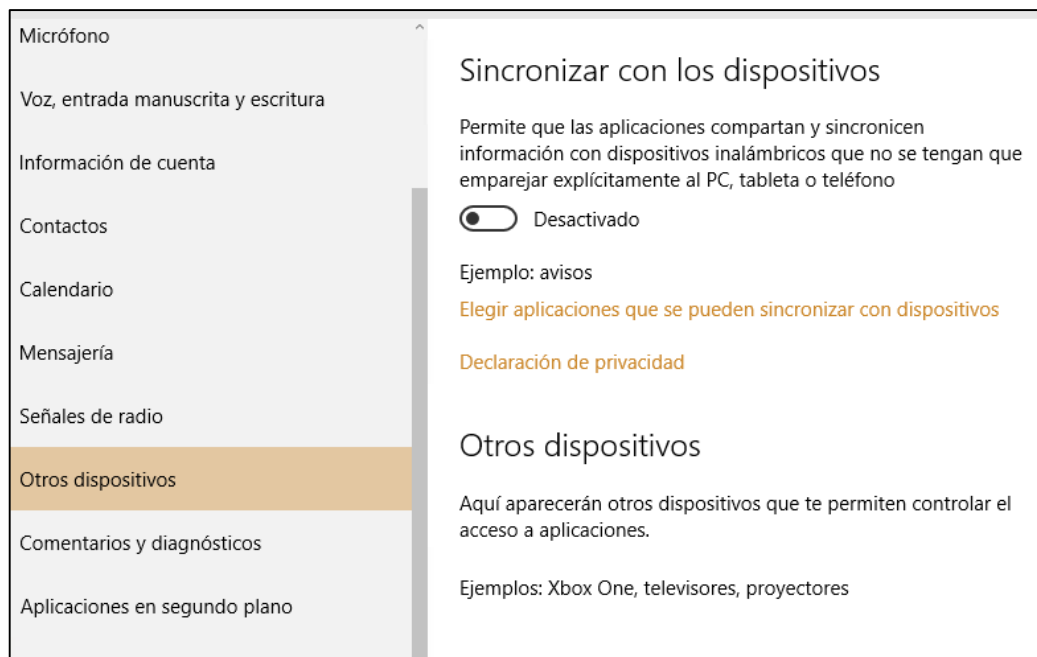


Imagen 12.- Opciones de sincronización de dispositivos.

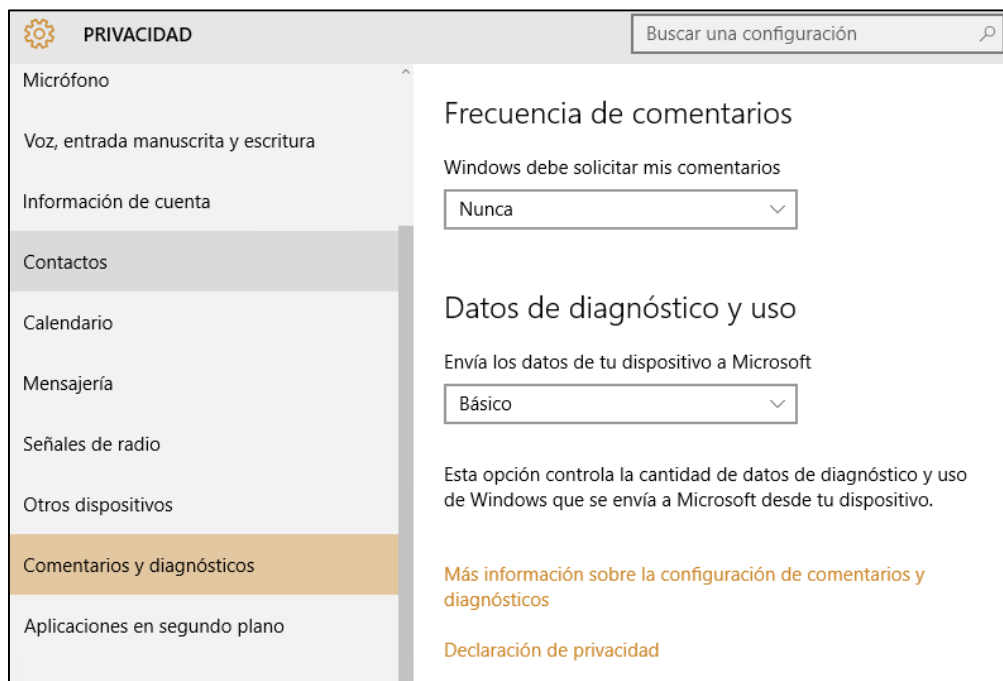


Imagen 13.- Opciones de comentarios.

En la configuración de las Cuentas se comprueba que la Sincronización de la configuración de cuentas con Microsoft se encuentra deshabilitada, tal y como se presenta en la siguiente imagen.

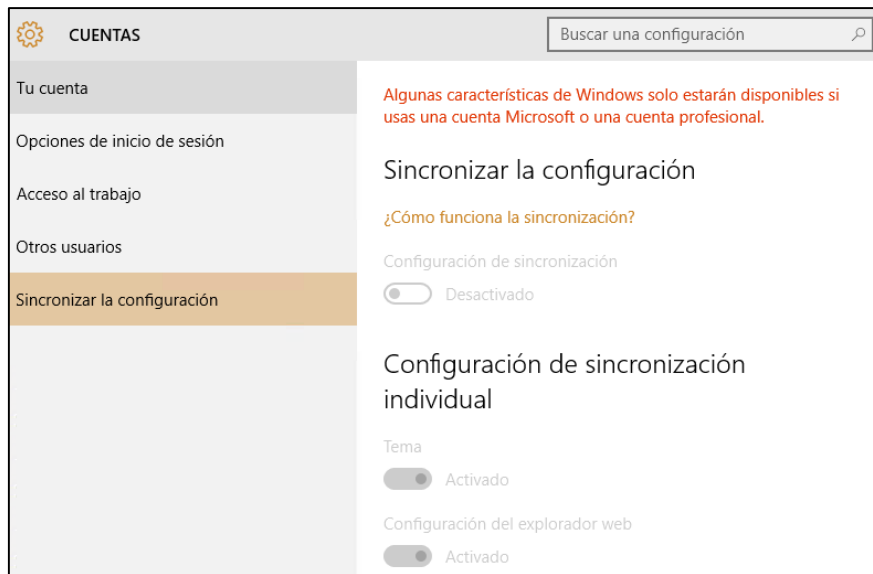


Imagen 14.- Sincronización de cuentas.

Un comportamiento diferente con respecto a versiones anteriores del sistema operativo cliente Windows es el hecho de que al reiniciar el sistema, algunos servicios deshabilitados a través de la consola de *Services.msc* vuelven a quedar habilitados. Es el caso de *Windows Update*, sin embargo si se acude al menú de *Configuración* y se deshabilita, este servicio quedaría definitivamente deshabilitado incluso al reiniciar el sistema.

Es posible desactivar también algunas de las funcionalidades de *Windows Defender* que remiten información hacia Internet, tales como riesgos de seguridad y muestras de ficheros.

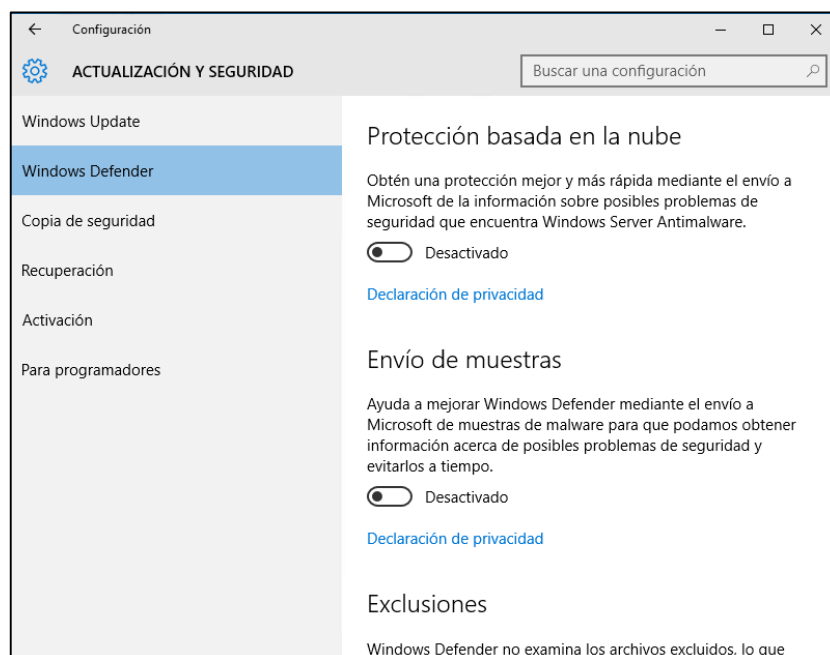


Imagen 15.- Configuración Windows Defender a nivel de privacidad.

Tras las anteriores acciones se realizan lecturas a diferentes horas del día y con diferentes niveles de actuación para comprobar en qué medida se continúa enviando información a *Microsoft* tras la configuración de estas características de seguridad y privacidad.

Los resultados obtenidos a través de las capturas de tráfico de red efectuadas en esta primera fase de aplicación de mecanismos de seguridad reflejan un decremento significativo en el envío de tráfico hacia Internet, aunque son notables todavía determinados procesos de conectividad relativos fundamentalmente a los sistemas de telemetría.

En el caso de la opción *LTSB* este envío de tráfico es menor que en las otras opciones indicadas con anterioridad.

7.2. Configuración de seguridad y aplicación de directivas a través de plantillas de seguridad

A continuación se aborda un siguiente nivel de aplicación de medidas de seguridad en el que se introducen otros elementos de bloqueo y control para limitar aún más las conectividades. Las mismas se establecen a través del uso de políticas de seguridad, bien de manera local o bien por dominio en los casos de escenarios implementados expresamente para ello.

En esta circunstancia se emplean las plantillas *ADMX* correspondientes a *MS Windows 10* y que ha facilitado el fabricante para el control de dichos sistemas operativos.

La aplicación de estas medidas de seguridad, tal y como se establece también en las guías CCN-STIC, se realiza en diferentes elementos:

- Deshabilitación de servicios por consola.
- Deshabilitación de servicios por registro.
- Configuración de directivas a través de plantillas de seguridad.

7.2.1. Configuración de servicios

Se citan a continuación otros servicios que permitirían el control de determinadas funcionalidades del sistema. Atendiendo a las condiciones de seguridad de cada organización o escenario sería factible limitar su funcionalidad. La relación de los mismos sería la siguiente:

- *DataCollectionPublishingService* (Servicio de telemetría).
- *Dmwappushsvc* (Servicio de telemetría).
- Experiencia de calidad de audio y vídeo de *Windows* en una plataforma de red (Experiencia de usuario).
- Escucha de grupo hogar (Experiencia de usuario).
- Partida guardada de *Xbox Live* (Experiencia de usuario).

- Registrador de configuración de *Windows Connect Now* (Experiencia de usuario).
- Servicio de datos del sensor (Servicio de telemetría).
- Servicio de enrutador *AllJoyn* (Experiencia de usuario).
- Servicio de geolocalización (Experiencia de usuario).
- Servicio de red de *Xbox Live* (Experiencia de usuario).
- Servicio de sensores (Servicio de telemetría).
- Servicio de supervisión de sensores (Servicio de telemetría).
- Servicio de zona con cobertura inalámbrica móvil de *Windows* (Experiencia de usuario).
- Servicio manos libres *Bluetooth* (Experiencia de usuario).
- Servicio de eventos *ETW* para *IE* (Servicio de telemetría).
- Servicio recopilador estándar del concentrador de diagnóstico de *MSFT* (Servicio de telemetría).
- *Wallet Services (Modern Apps)*.
- Servicio de seguimiento de diagnóstico (Experiencia de usuario).
- *WService* (Tienda Microsoft).
- *AppXSvc (Modern Apps)*.
- *Enterprise App Management Service* (Tienda Microsoft).

Esta lista correspondería a la opción *CBB*. En el caso de la opción *LTSB*, determinados servicios asociados a *Modern Apps* o la *Tienda Microsoft* no se encontrarían disponibles.

En el caso de querer deshabilitar los anteriores servicios a través de la consola de servicios, se podrá llevar a cabo la acción con la excepción de los siguientes:

- *WService* (servicio de Tienda Microsoft).
- *AppSvc*.
- *Enterprise App Management Service* (servicio de Tienda Microsoft).

Para estos tres (3) servicios y a través de la herramienta de edición del registro, se deberá establecer el valor de "*Start*" a 4, tal y como se muestra en las siguientes imágenes. Una vez modificados los valores y reiniciado el equipo, los servicios se encontrarán deshabilitados.

- WService (servicio de Tienda Microsoft).

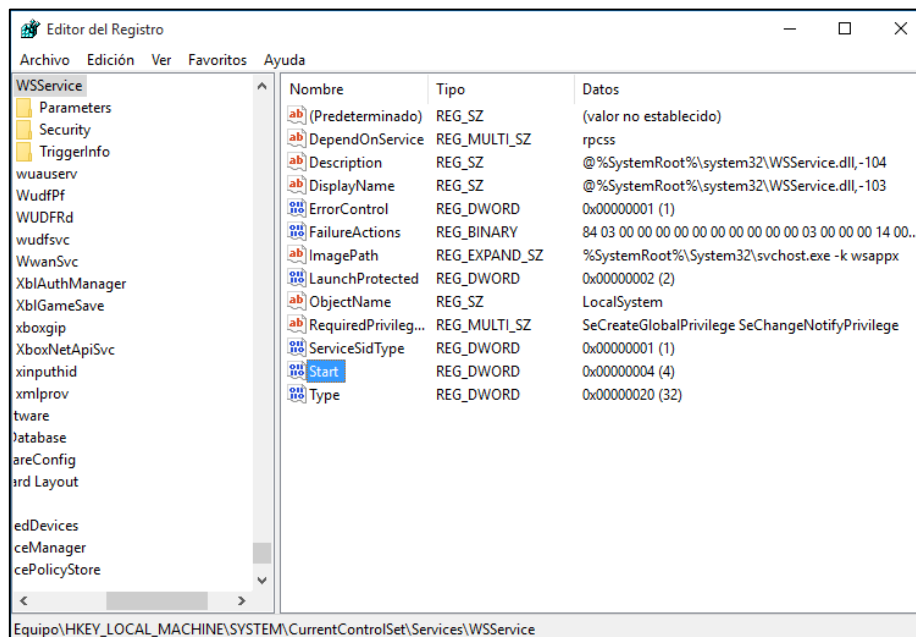


Imagen 16.- Deshabilitado por registro servicio WService.

- AppXSvc

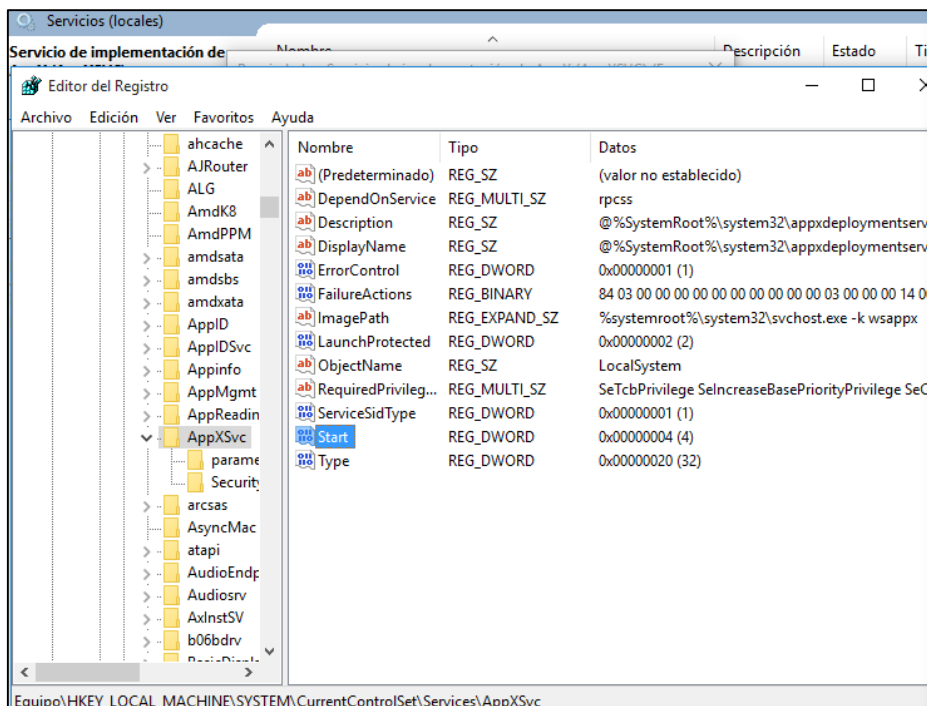


Imagen 17.- Deshabilitado por registro servicio AppXSvc.

- Enterprise App Management Service (Servicio de Tienda Microsoft).

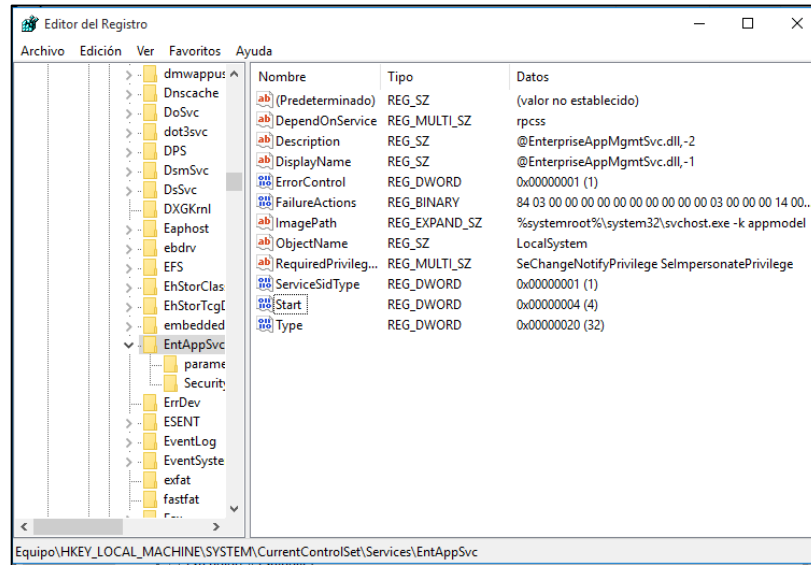


Imagen 18.- Deshabilitado por registro servicio EntAppSvc.

7.2.2. Plantillas administrativas configuradas

Adicionalmente a los servicios previos, se prevé también la posibilidad de establecer configuraciones de control para diferentes componentes de Windows a través de Plantillas Administrativas. Esto limitará la conectividad de diferentes servicios y aplicaciones con Internet, controlando la funcionalidad de los mismos.

Se citan dentro de las plantillas, los elementos a configurar así como los valores que se deberían aplicar. Estas configuraciones de seguridad a través de directivas en plantillas administrativas vienen agrupadas en:

- Componentes de Windows.
- Sistema.

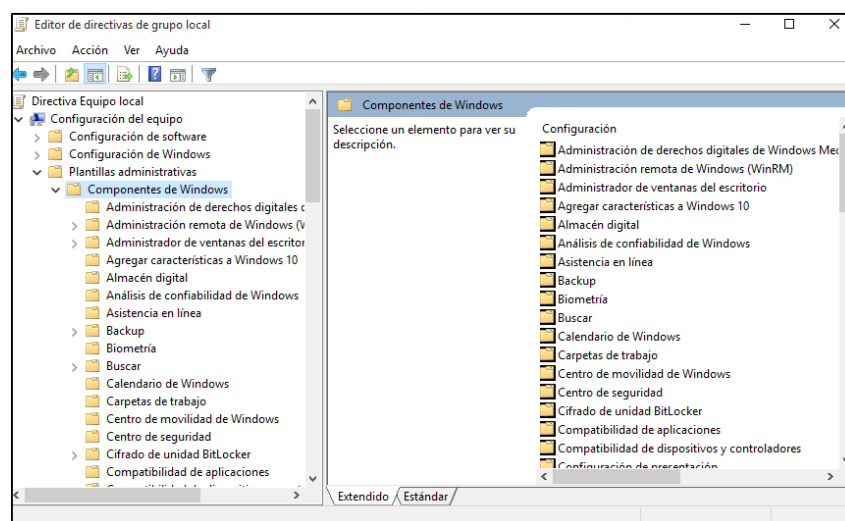


Imagen 19.- Plantillas de seguridad.

7.2.3. Componentes de Windows

- *Windows Defender.*
 - Desactivar *Windows Defender* - Habilitada
- Asistencia en línea.
 - Desactivar la asistencia en línea - Habilitada
- *EndPoint Protection.*
 - Desactivar *Endpoint Protection* - Habilitada
- Recopilación de datos y versiones preliminares.
 - Permitir telemetría - Deshabilitada
- Informe de errores de *Windows*.
 - Deshabilitar el informe de errores de *Windows* - Habilitada
 - No enviar datos adicionales - Habilitada
- *Internet Explorer.*
 - Permitir a los servicio de *Microsoft* ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones - Deshabilitada
 - Impedir administración del filtro *SmartScreen* - Deshabilitada
- *OneDrive.*
 - Impedir el uso de *OneDrive* para almacenar archivos - Habilitada
- *Windows Media Center.*
 - No permitir que se ejecute *Windows Media Center* - Habilitada
- Ubicaciones y sensores.
 - Desactivar *scripting* de ubicación - Habilitada
 - Desactivar ubicación - Habilitada
 - Desactivar sensores - Habilitada
 - Desactivar el servicio de localización de *Windows* - Habilitada

7.2.4. Sistema

- Perfiles de usuario.
 - Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio) - Habilitada / Siempre desactivado.
- Configuración de comunicaciones de Internet.
 - Desactivar informe de errores de reconocimiento de escritura a mano - Habilitada

- Desactiva el Programa para la mejora de la experiencia del usuario de Windows - Habilitada
- Desactivar los vínculos "Events.asp" del Visor de eventos - Habilitada
- Desactivar el contenido "¿Sabía que...?" del Centro de ayuda y soporte técnico - Habilitada
- Desactivar el informe de errores de Windows - Habilitada
- Desactivar el acceso a la Tienda - Habilitada
- Desactivar uso compartido de datos de personalización de escritura a mano - Habilitada

Es posible determinar que la existencia de envíos de tráfico son en esencia similares a los que podrían existir en un sistema anterior como MS Windows 7 con los resultados obtenidos a través de las capturas de tráfico de red efectuadas en esta segunda fase de análisis y una vez que las condiciones de seguridad han sido aplicadas.

8. COMPONENTES DE TELEMETRÍA

Dentro de los nuevos componentes existentes en MS Windows 10, el de Telemetría sería uno de los que mayor conectividad realiza hacia Internet. Sin embargo es también el que ofrece una mayor capacidad de granularidad para su control. Este servicio es empleado por Windows para analizar y solventar problemas de Windows.

Dicha funcionalidad de telemetría opera tanto de forma interna generando registros internos de actividad como remitiendo envíos de información a Microsoft en determinadas condiciones.

En MS Windows 10 se han establecido cuatro (4) niveles de configuración del estado de la telemetría:

- Seguridad.
- Básico.
- Avanzado.
- Completo.

Para ampliar información sobre la configuración de la telemetría y otros componentes de MS Windows 10 puede consultarse la siguiente dirección URL:

[https://technet.microsoft.com/en-us/library/mt577208\(v=vs.85\).aspx#BKMK_UTC](https://technet.microsoft.com/en-us/library/mt577208(v=vs.85).aspx#BKMK_UTC)

La siguiente imagen muestra la información que sería manejada por los diferentes niveles de telemetría.

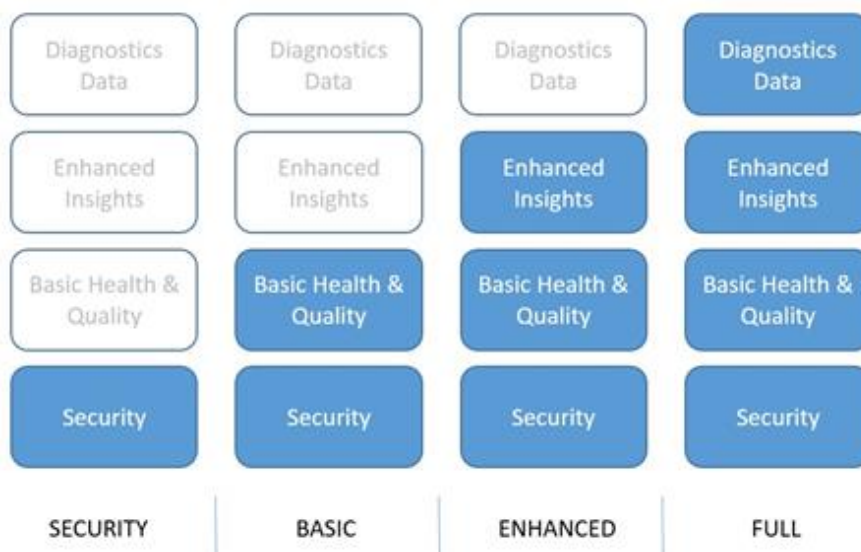


Imagen 20.- Niveles de funcionalidad de la telemetría.

Cada estado de telemetría incrementa el nivel de datos que estarían siendo manejados por el componente. De esta manera, se trataría la siguiente información en un nivel de configuración de Seguridad:

- Configuraciones base de experiencia de usuario. La información manejada sería información del sistema operativo, Id y clase de dispositivo.
- *Malicious Software Removal Tool*. Información tratada por la herramienta que puede descargarse a través de *Windows Update*.
- *Windows Defender*. Información tratada por la herramienta antimalware incorporada en *MS Windows 10*.

La configuración del componente telemetría en modo Básico manejaría la siguiente información adicional a la anterior:

- Información básica del dispositivo. Se incluyen como datos fundamentales atributos de los dispositivos, versión de navegador, atributos de procesador y memoria, edición de Windows junto a otros.
- Métricas cualitativas de experiencia de usuario. Se incluirían eventos relacionados con tiempos de carga o descarga de elementos.
- Funcionalidad de la compatibilidad de aplicaciones.
- Información de la *Tienda*, descarga y comportamiento de aplicaciones de la misma.

La configuración del componente telemetría en modo Avanzado manejaría la siguiente información adicional a las dos anteriores:

- Eventos del sistema operativo.
- Eventos de aplicaciones del sistema operativo.
- Eventos de determinados dispositivos.

La configuración del componente de telemetría en modo Completo, además de la información manejada en los anteriores niveles, emplearía también:

- Información incluida dentro del programa *Windows Insider*. La cual incluye cualquier contenido que dentro del acuerdo del programa, Microsoft pueda necesitar para dar respuesta al soporte solicitado.

Las pruebas efectuadas en laboratorio determinan un decremento del volumen de conexiones realizadas por los sistemas, al configurar los diferentes niveles para el Componente de Telemetría. Lógicamente, de los niveles existentes, el de Seguridad correspondería al de menor envío de información, siendo el mayor el correspondiente al de nivel Completo.

Tal y como informa el fabricante y con una clara intencionalidad de transparencia con respecto al uso de servicios, procesos y conexiones hacia Internet, desde *Microsoft Corporation* se está generando en la actualidad un documento en este sentido.

A través de dicho informe, junto a la información adicional que pudieran recibir a través de guías u otros medios, las organizaciones tendrán la capacidad de conocer el destino de las conexiones, pudiendo en consecuencia emplear, entre otras posibles medidas, el uso de listas blancas y/o negras para el mejor control de la información transmitida.

Dicho documento, por otra parte, podrá ser de utilidad para el control del destino de las comunicaciones, pudiendo de este modo identificar conexiones que aun pareciendo legítimas podrían ser creadas por código dañino.

El citado informe no sería vinculante para los sistemas sobre los que se enfoca el presente documento, debido a la falta de conectividad de éstos hacia Internet. Sin embargo, se estima como beneficioso el tenerlo en consideración como información de valor. De esta manera y con el listado en modalidad de tipología blanca o negra, podría emplearse para determinar elementos del sistema que intentasen realizar conexiones de tipo ilegítimas. Lo cual permitiría identificar comportamientos anómalos del sistema operativo, asociables por ejemplo con actividad de código dañino.

9. CONCLUSIONES

Completados los análisis efectuados, tal y como se ha descrito en apartados anteriores del presente informe, se establecen las siguientes conclusiones para el empleo del sistema operativo *MS Windows 10* sobre los puestos de trabajo de las diferentes **Administraciones Públicas**:

- De las diferentes versiones y opciones del sistema operativo verificadas para un entorno corporativo, se recomienda la instalación de versiones *MS Windows Pro* o *Enterprise* en su opción *CBB*. Esta afirmación deriva de las siguientes consideraciones:
 - La versión indicada en su opción *CBB* aporta todas las funcionalidades que ofrece *MS Windows 10*.

- La opción CBB aporta al administrador del sistema un mayor control y tiempo de prueba de los procesos de actualización que la opción CB, siendo su gestión considerablemente más flexible.
- El uso de la versión *Pro* o *Enterprise*, dependerá de los acuerdos y/o contratos existentes, o de la adquisición de versiones que pueda darse a la hora de adquirir un nuevo equipo informático.
- El sistema aporta mecanismos suficientes para controlar cada una de los componentes y funcionalidades que ofrecerían las versiones de *MS Windows 10 Pro CBB* y *MS Windows 10 Enterprise CBB*.
- A través de las políticas de grupo y otros elementos de configuración ya mencionados en el presente informe, es factible controlar y limitar las conectividades y funcionalidades de los componentes del sistema operativo.
- Se deberán tener en consideración para lograr una buena condición de seguridad, aplicar todas las opciones de privacidad que proporciona *Microsoft* para evitar el envío de información, tal y como se detalla en el punto 7.1 del presente informe.
- Existen, en función de las necesidades y la política de seguridad consolidada de la organización, mecanismos de control centralizados para determinar el empleo o no de aplicaciones tipo *Modern Apps* o la *Tienda de Microsoft*. Serán las circunstancias y escenarios propios de cada entidad u Organismo las que determinarán qué aplicaciones de esta tipología se deben encontrar o no disponibles para el uso por parte de los usuarios.
- En lo que corresponde al *Componente de Telemetría*, se deberá establecer su nivel operacional en función tanto de los acuerdos de soporte existentes como de las necesidades operativas de cada organización. Junto a lo anterior, los diferentes niveles del Esquema Nacional de Seguridad (ENS) permiten establecer criterios para garantizar los mecanismos de control más adecuado. La aplicación del nivel, como en las circunstancias anteriores, puede ser llevado a cabo de forma centralizada permitiendo incluso limitar su funcionalidad si se diera la necesidad de ello por razones de servicio.
- La implementación de la opción CBB, así como la aplicación de medidas de seguridad permitirían la limitación e incluso la inhabilitación de algunas de las funcionalidades que aporta *MS Windows 10*:
 - *Cortana*. Componente controlable a través de políticas de grupo y funcionalidad del servicio.
 - *Tienda de Microsoft*. Componente controlable a través de políticas de grupo y funcionalidad del servicio.
 - *Modern Apps*. Componente controlable a través de políticas de grupo y funcionalidad del servicio.
 - *Microsoft Edge*. Componente controlable a través de políticas de grupo y funcionalidad del servicio.

- *Windows Smart Screen*. Servicio gestionable en función de la necesidad organizativa.
- *Windows Search*. Servicio gestionable en función de la necesidad organizativa.
- *Sistema de Telemetría*. Servicio controlado a través de políticas de grupo. Bajo determinadas condiciones el servicio podrá ser deshabilitado temporal o permanentemente.
- *Windows Defender*. Servicio controlado a través de políticas de grupo. Podría ser inhabilitado si existiera una aplicación de terceros que cubriera las necesidades que aporta este componente.
- *Microsoft Internet Explorer*. Aplicación controlada a través de políticas de grupo.

Las guías CCN-STIC de la serie 800 (Esquema Nacional de Seguridad) relativas a *MS Windows 10* establecerán las condiciones de seguridad del propio sistema operativo y de sus componentes para el cumplimiento del Esquema Nacional de Seguridad. Se debe tener en cuenta que dichas guías no tienen como objetivo sustituir políticas consolidadas. Podrán ser utilizadas no obstante como mecanismos de referencia para garantizar la seguridad de las infraestructuras.

Dichas guías tendrán en consideración los resultados obtenidos en este documento, otros posibles test que se lleven a cabo en laboratorio, así como la documentación que fuera emitida por el fabricante.

A través de las guías se establecerán las condiciones de seguridad recomendadas para cada uno de los niveles contemplados en el Esquema Nacional de Seguridad. Se articularán también los mecanismos de control que podrán ser empleados por las organizaciones para la gestión de la funcionalidad de cada uno de los componentes contemplados en el presente informe.

Dentro de las guías de seguridad se establecerán otros posibles mecanismos de control derivados de documentos emitidos por el fabricante, que permitan evaluar la conectividad de los componentes de *MS Windows 10* de la organización hacia el exterior.

Como consideración final, se estima que una vez configuradas las opciones de privacidad y las configuraciones de seguridad adecuadas, se dispondrá de un sistema operativo *MS Windows 10* que en sus versiones *Pro CBB* o *Enterprise CBB* proporcionan condiciones de privacidad adecuadas para el cumplimiento del ENS u otras normas de seguridad similares.

Aplicando las medidas indicadas, *MS Windows 10* podría llegar a operar en un estado de seguridad similar al que presentaba un sistema *MS Windows 7*. Este informe evidentemente no tiene en consideración futuras funcionalidades que podría establecer Microsoft para *MS Windows 10* y que podrían alterar los resultados obtenidos en el presente estudio.

10. CONTACTO

Se puede ampliar cualquier punto del informe, utilizando como vía preferente de comunicación el portal <http://www.ccn-cert.cni.es>

- Teléfono: +34 91372 59 74
- E-Mail: ccn-cert@cni.es

ANEXO A. SERVIDORES DE TELEMETRÍA

Los siguientes servidores corresponden a aquellos donde los clientes MS Windows 10 envían información:

vortex.data.microsoft.com
vortex-win.data.microsoft.com
telecommand.telemetry.microsoft.com
telecommand.telemetry.microsoft.com.nsatc.net
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
sqm.telemetry.microsoft.com
sqm.telemetry.microsoft.com.nsatc.net
watson.telemetry.microsoft.com
watson.telemetry.microsoft.com.nsatc.net
redir.metaservices.microsoft.com
choice.microsoft.com
choice.microsoft.com.nsatc.net
df.telemetry.microsoft.com
reports.wes.df.telemetry.microsoft.com
wes.df.telemetry.microsoft.com
services.wes.df.telemetry.microsoft.com
sqm.df.telemetry.microsoft.com
telemetry.microsoft.com
watson.ppe.telemetry.microsoft.com
telemetry.appex.bing.net
telemetry.urs.microsoft.com
settings-sandbox.data.microsoft.com
vortex-sandbox.data.microsoft.com
survey.watson.microsoft.com
watson.live.com
watson.microsoft.com
statsfe2.ws.microsoft.com
corpext.msitadfs.glbdns2.microsoft.com
compatexchange.cloudapp.net
cs1.wpc.v0cdn.net
a-0001.a-msedge.net
statsfe2.update.microsoft.com.akadns.net
sls.update.microsoft.com.akadns.net
fe2.update.microsoft.com.akadns.net
diagnostics.support.microsoft.com
corp.sts.microsoft.com
statsfe1.ws.microsoft.com
pre.footprintpredict.com
il.services.social.microsoft.com
il.services.social.microsoft.com.nsatc.net
feedback.windows.com

feedback.microsoft-hohm.com
feedback.search.microsoft.com
rad.msn.com
preview.msn.com
ad.doubleclick.net
ads.msn.com
ads1.msads.net
ads1.msn.com
a.ads1.msn.com
a.ads2.msn.com
adnexus.net
adnxs.com
az361816.vo.msecnd.net
az512334.vo.msecnd.net

ANEXO B. LISTADO DE CONEXIONES ESTABLECIDAS

Adjunto al informe se encuentra un archivo MS Excel con un ejemplo del listado de conexiones identificadas, así como las aplicaciones o procesos que las habrían originado.

En dicho listado se pueden identificar conexiones efectuadas por los puestos de trabajo con sistemas remotos, bien cuando una aplicación es iniciada o bien cuando el equipo se encuentra sin actividad por parte del usuario.