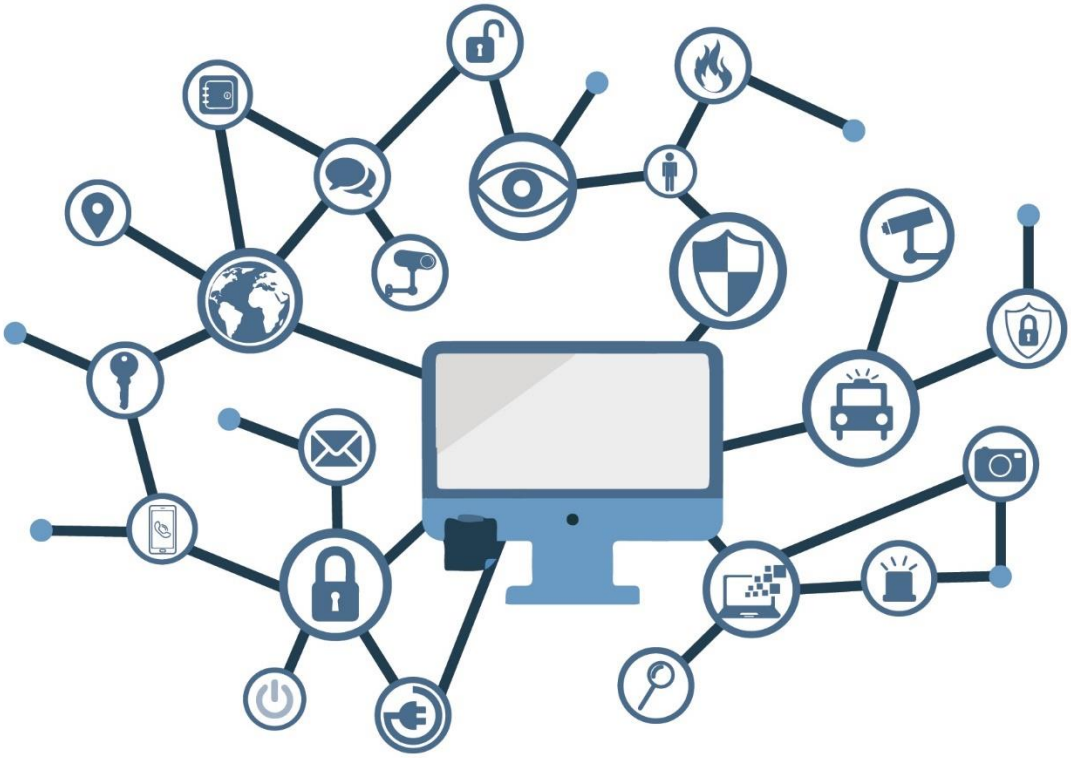
GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD SOBRE MICROSOFT WINDOWS 10 (CLIENTE MIEMBRO DE DOMINIO)



DICIEMBRE 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.05.29 10:53:11 +02'00'

NIPO: 785-17-053-4
Fecha de Edición: diciembre 2017

El Ministerio de Hacienda y Administraciones Públicas ha financiado el desarrollo del anexo A del presente documento.
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

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

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

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

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

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

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

Diciembre de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN STIC 500), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

La serie CCN STIC 500 se ha diseñado de manera incremental. Así, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. En este sentido se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

Por ejemplo, en el caso de un entorno que le sea de aplicación el ENS, para un servidor miembro de un dominio con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN STIC 870A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-873 Internet Information Services (IIS) 8.5.

c) Guía CCN STIC 880 Microsoft Exchange Server 2013 en Windows 2012 R2.

Por ejemplo, en el caso de un entorno de red clasificada, para un servidor con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN STIC 560A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-563 Internet Information Services (IIS) 8.5.

c) Guía CCN STIC 552 Microsoft Exchange Server 2013 en Windows 2012 R2.

2. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para implementar y garantizar la seguridad para una instalación del sistema “Microsoft Windows 10” en sus versiones “Enterprise” con sus opciones de mantenimiento “CB”, “CBB” o “LTSB” y “Professional” (en adelante, “Pro”), actuando como cliente miembro de un dominio. Otras versiones o productos disponibles para Microsoft Windows 10 no están soportados para la presente guía.

Para manejar información clasificada, la única versión del sistema operativo permitida es Microsoft Windows 10 Enterprise con opción de mantenimiento LTSB. Esta decisión se fundamenta en el Informe de Amenazas denominado “CCN-CERT IA-08-16 Privacidad W10 Redes Clasificadas”.

Nota: Deberá consultarse en cada caso, dependiendo de donde se implemente el sistema, qué versión de Microsoft Windows 10 va a ser instalada.

La configuración que se aplica a través de la presente guía se ha diseñado para ser lo más restrictiva posible, minimizando la superficie de ataque y, por lo tanto, los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del cliente, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione los servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las plantillas y normas de seguridad, se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

3. ALCANCE

La guía se ha elaborado para proporcionar información específica con objeto de asegurar un cliente con el sistema operativo “Microsoft Windows 10”, instalado en español en sus versiones Enterprise y Pro. Se incluyen, además, operaciones básicas de administración para la aplicación de las mismas, así como una serie de recomendaciones para su uso.

El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:

a) Implementación del ENS en un escenario de dominio de Directorio Activo Microsoft con clientes Windows 10.

b) Implementación de plantillas de seguridad en función de los niveles de seguridad establecidos en el ENS para clientes Microsoft Windows 10 miembros de un dominio de Directorio Activo Microsoft.

c) Implementación de seguridad en un escenario de red clasificada con un dominio de Directorio Activo Microsoft con clientes Microsoft Windows 10.

d) Aplicación de las plantillas de seguridad mediante el empleo de objetos de políticas de grupo.

Este documento incluye:

a) **Descripción de versiones, opciones de mantenimiento y licencias** para todos aquellos operadores que tengan experiencia en versiones previas, se proporciona la información sobre las diferentes versiones, opciones de mantenimiento y versiones de las que dispone el sistema.

b) **Descripción de las nuevas funcionalidades** para todos aquellos operadores que tengan experiencia en la versión previa de Windows 7, se incluyen las nuevas características del producto.

c) **Funcionalidades de seguridad local adicionales.** Completa descripción de aquellas características y servicios que, no encontrándose definidos por defecto, agregan seguridad adicional a una infraestructura de Microsoft Windows 10 como puesto de trabajo miembro de un dominio de Directorio Activo Microsoft.

d) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.

e) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

f) **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad en clientes Microsoft Windows 10 miembros de un dominio.

g) **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de los equipos cliente con respecto a las condiciones de seguridad que se establecen en esta guía.

h) **Configuración de cifrado de disco con Bitlocker.** Establece los mecanismos para la configuración del cifrado con Bitlocker que aporta Microsoft Windows 10.

i) **Solucionarios adicionales.** Guías paso a paso para la comprobación de la configuración de operativas sobre el puesto de trabajo

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de securización que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

a) Como paso previo a la instalación de Microsoft Windows 10, la organización deberá haber realizado una implementación de Directorio Activo, siguiendo los mecanismos definidos en las guías correspondientes dependiendo del entorno que se esté securizando:

   i. Entorno de ENS: CCN-STIC-870A – Implementación del ENS sobre Microsoft Windows Server 2012 R2.

   ii. Entorno de red clasificada: CCN-STIC-560A – Implementación de Microsoft Windows Server 2012 R2 – DC y Servidor miembro.

b) Deberá implementar la presente guía en función del entorno que requiera su organización.

c) Si el entorno que está securizando pertenece a una red clasificada, se deberá realizar la securización de Microsoft Internet Explorer 11 a través de la implementación de las políticas de seguridad definidas en la guía CCN-STIC-520 Internet Explorer 11 para un cliente miembro de dominio.

   Esta guía de seguridad está enfocada a sistemas clasificados, aunque puede ser tomada como base para la securización de IE 11 en aquellos sistemas que les sea de aplicación el ENS. En éste último caso, estas medidas deberán adaptarse a las necesidades de cada organización.

d) En el caso de que se requiera la securización de los equipos en una red clasificada para el uso de MS Office 2013, deberá realizar la aplicación de la guía codificada como CCN-STIC-529.

4.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos tipo puesto cliente con Sistema Operativo Microsoft Windows 10, en sus versiones Enterprise y Pro con opciones CB y CBB y Enterprise con opción LTSB en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

Para los entornos de ENS se podrá utilizar la versión de Microsoft Windows 10, con la opción de mantenimiento deseada, que más se adapte a las necesidades de cada organización.

En un entorno de red clasificada donde se maneja información clasificada la única versión autorizada del Sistema Operativo Microsoft Windows 10 es la versión Enterprise con opción de mantenimiento LTSB.

La guía ha sido desarrollada y probada en entorno de uso de servicios Microsoft con las versiones de Microsoft Windows 10 Enterprise y Pro.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V sobre Windows Server 2012 R2 Datacenter con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320
   i. Intel Pentium Xeon CPU ES 2430 2.20GHz.
   ii. HDD 1 TB.
   iii. 64 GB de RAM.
   iv. Interfaz de Red 1 Gbit/s.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Windows 10. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 o 32 bits (x64 o i386), con más de 1 GB de memoria RAM para la versión de 32 bits o 2 GB para la versión de 64 bits.

Se aconseja, no obstante, por seguridad y rendimiento, la implementación de versiones de 64 bits frente a las de 32 bits.

Nota: Puede comprobar los requisitos del sistema de Windows 10 en el siguiente enlace https://www.microsoft.com/es-xl/windows/windows-10-specifications.

La guía ha sido desarrollada con el objetivo de dotar a las infraestructuras con la seguridad adecuada dependiendo del entorno sobre el que se aplique. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios, roles o características deseadas.

Para garantizar la seguridad de los puestos de trabajo, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Microsoft Update. Las actualizaciones por lo general se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados. Deberá tener en consideración que las opciones de mantenimiento CB, CBB y LTSB ofrecen diferentes tiempos de implementación de actualizaciones. En líneas posteriores de la presente guía se tratarán las consideraciones oportunas.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que, en ocasiones, se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse el hecho de haber probado su configuración y comportamiento en un entorno aislado y controlado, en el cual se habrán aplicado las pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones sino a servir como línea base de seguridad. Esta línea deberá ser adaptada a las necesidades propias de cada organización.

4.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del sistema Microsoft Windows 10 dependiendo del entorno sobre el que vaya a ser aplicado, así como una diferenciación de la versión a utilizar.

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) Anexo A: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows 10 en sus versiones Enterprise y Pro a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) Anexo B: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows 10 en su versión Enterprise con opción de mantenimiento LTSB a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que en sus respectivos anexos se dotará de la información necesaria y concreta para cada tipo de implementación.

De manera adicional, en cada una de las carpetas “Scripts” que se adjuntan a los documentos, existe un directorio que almacena un informe en formato HTML con cada objeto de directiva de grupo (GPO) o directiva de grupo local (GPL) que se aplica.

5. VERSIONES, OPCIONES DE MANTENIMIENTO Y LICENCIAS EN MS WINDOWS 10

5.1 VERSIONES

Tradicionalmente, Microsoft ha proporcionado versiones para los entornos domésticos, profesionales y de negocio. La nomenclatura, en inglés, de dichas versiones son Home, Professional (también denominada Pro) y Enterprise. Adicionalmente, existen versiones específicas para educación. Cada una de ellas aporta diferentes funcionalidades, en función del entorno de implementación factible. Así, el usuario doméstico tenía a su disposición una solución que se adaptaba a sus necesidades: versión Home.

Para entornos de tipo corporativo, Microsoft, por ejemplo, había proporcionado dos líneas de productos diferenciadas, las versiones Profesional y Enterprise. La diferencia radicaba en que esta última aportaba una serie de características para un control corporativo mayor, implicando en ello, 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 este tipo de versionado que se mantiene en Microsoft Windows 10, aparece una nueva categorización basada en las opciones de mantenimiento. Esta nueva categorización atiende a la necesidad de dar respuesta a una necesidad más específica para, por ejemplo, asegurar que los sistemas se encuentren actualizados de tal forma que, ante una desactualización, el sistema limite su funcionamiento

El sistema operativo Windows 10 introduce una nueva forma de construir, desplegar y actualizar Windows: Windows como servicio. Microsoft ha modificado cada parte del proceso, para simplificar su gestión y permitir mantener una experiencia consistente de Windows 10 en los clientes.

Antes de MS Windows 10, Microsoft lanzaba nuevas versiones de Windows cada pocos años. Con este modelo, el cambio de una versión a otra implicaba un trabajo importante en los clientes, ya que el volumen de cambios existente requería unos procesos de validación y migración costosos. Con el modelo de Windows como Servicio, Microsoft lanzará nuevas funcionalidades de Windows 10 de forma periódica y continua en el tiempo, simplificando los procesos necesarios para mantener el sistema actualizado con las nuevas funcionalidades. Se lanzarán una media de dos actualizaciones de Windows 10 al año.

Windows 10 recibe dos tipos de actualizaciones:

a) Actualizaciones de calidad (Quality Updates). Incluye tanto actualizaciones de seguridad como actualizaciones recomendadas, en un modelo acumulativo.

b) Actualizaciones de características (Feature Updates). Donde se recogen las nuevas funcionalidades del producto, y a las que se hace referencia en el modelo de servicio de Windows 10.

5.2 OPCIONES DE MANTENIMIENTO

Además de este modelo de servicio, Microsoft ofrecerá una opción adicional de mantenimiento de Windows 10 a largo plazo, similar en concepto a las existentes para sistemas operativos previos. Las opciones de mantenimiento de Windows 10 determinan la rapidez con la que los sistemas recibirán las actualizaciones, una vez éstas son publicadas por Microsoft. Dentro de las opciones de mantenimiento de Microsoft Windows 10, se encuentran disponibles tres opciones:

a) CB (Rama actual o Current Branch). En este modelo, los equipos reciben las actualizaciones tan pronto como Microsoft las publica. Es el modelo que siguen, por ejemplo, los equipos de consumo. En empresa, se recomienda este modelo para pilotos o pruebas sobre Microsoft Windows 10.

b) CBB (Rama actual para empresas o Current Branch for Business). Las organizaciones normalmente siguen un ciclo de pruebas antes de desplegar de forma masiva nuevas características a los usuarios. Para Microsoft Windows 10, la fase de piloto y/o pruebas se cubriría dentro del plazo de la versión CB, mientras que el despliegue masivo se realizaría en CBB. Los clientes en el modelo CBB recibirán la misma versión de Microsoft Windows 10 que aquellos que están en el modelo CB, pero la recibirán en un período de tiempo posterior.

c) LTSB (Rama de mantenimiento a largo plazo para empresas o Long Term Servicing Branch). Esta opción de mantenimiento de Windows 10 está orientada a sistemas especializados y de misión crítica, que tradicionalmente requieren un ciclo de vida mayor y normalmente, no se benefician de nuevas funcionalidades, ya que habitualmente realizan una tarea única y concreta. En este modelo de actualización, estos equipos recibirán únicamente actualizaciones de calidad. Microsoft generará actualizaciones de características para este modelo aproximadamente una vez cada dos años, aunque no es de obligación su instalación inmediata.

Entre las diferentes opciones, CB, CBB y LTSB, que proporciona Microsoft para MS Windows 10, resulta reseñable, entre sus características, la disponibilidad de las actualizaciones y el ciclo de vida de mantenimiento:

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

b) Para la opción CBB, la duración mínima del ciclo de vida de mantenimiento es de 8 meses aproximadamente.

c) Para la opción LTSB, la duración mínima del ciclo de vida de mantenimiento es de 10 años.

Debe entenderse lo anterior como el plazo máximo en que un sistema podrá mantenerse operacional sin la debida actualización del sistema. Esto no indica, como es lógico, que sea adecuado mantener un sistema desactualizado durante un plazo de 8 meses. Las buenas prácticas de seguridad establecen la necesidad de mantener los sistemas actualizados con las últimas actualizaciones disponibles en materia de seguridad.

El ciclo de vida de las distintas opciones de mantenimiento de MS Windows 10 varía, según se esté siguiendo el modelo de servicio (CB/CBB) o el modelo tradicional (LTSB):

a) Microsoft va a soportar de forma simultánea en el tiempo dos Current Branch for Business (Rama actual para empresas), más un período de gracia de 60 días. De esta forma, cada actualización de características de Windows 10 en este modelo se soportará y actualizará un mínimo de 18 meses.

b) En el caso de la opción LTSB, el soporte completo de la misma será de 5 años desde la fecha de lanzamiento, más otros 5 años de soporte extendido.

c) Si un equipo configurado en el modelo de Windows como Servicio no se actualiza dentro del plazo fijado, dejará de recibir actualizaciones de calidad. Las buenas prácticas de seguridad establecen la necesidad de mantener los sistemas actualizados con las últimas actualizaciones disponibles en materia de seguridad. Hay que destacar que parte de las nuevas características de MS Windows 10 que se van lanzando en este modelo de servicio son también relativas a seguridad.

Nota: Para más información sobre las diferentes opciones de mantenimiento puede dirigirse a la siguiente dirección URL: https://technet.microsoft.com/es-es/itpro/windows/manage/waas-overview

Adicionalmente a las condiciones citadas anteriormente, debe conocerse que la opción LTSB, con respecto a las otras dos, mantiene diferencias en cuanto a las funcionalidades del producto. Así, ésta no aporta todas las características con las que contaría Microsoft Windows 10 Enterprise y Pro. Elementos tales como Cortana, Microsoft Edge o la tienda, entre otros, no se encontrarían disponibles para dicha opción de sistema.

La opción LTSB no tendrá el mismo mantenimiento de funcionalidad que las otras dos opciones existentes. Así, resultaría factible que mientras las opciones CB y CBB mantienen mejoras funcionales de producto, así como las características del mismo, éstas no estarían disponibles para la versión LTSB. Sí mantendría en su ciclo de vida las actualizaciones de seguridad, pero no de aquellas actualizaciones que correspondan a mejoras funcionales.

Debe tomarse también en consideración que la opción CB se encuentra disponible para las versiones Home, Education, Pro y Enterprise; la opción CBB se encuentra disponible para las versiones Education, Pro y Enterprise; y la opción LTSB se encontraría disponible, solamente, para la versión Enterprise.

Nota: Para más información sobre las diferentes opciones de mantenimiento puede dirigirse a la siguiente dirección URL: https://technet.microsoft.com/es-es/library/mt598226(v=vs.85).aspx

5.3 LICENCIAS

Por ultimo al igual que ocurría en versiones anteriores de Windows existen diferentes mecanismos de adquisición de licencias los cuales se detallan a continuación:

a) Licencias Windows OEM. Son las licencias que vienen preinstaladas en los equipos nuevos que se adquieren para entornos de negocio. La característica principal de este tipo de licencias es que están asociadas al dispositivo con el que se adquieren, y no se pueden reinstalar en un dispositivo distinto.

b) Licencias de Retail. Son las licencias que se adquieren en tiendas físicas o a través de internet. A su vez, pueden ser licencias completas (Full Packaged Product), que pueden instalarse en cualquier equipo, o bien licencias de actualización, que requieren que el equipo sobre el que se instale disponga de una versión ya instalada de sistema operativo. Normalmente, las licencias de actualización se utilizan para pasar de una versión más antigua a una más moderna de sistema operativo.

c) Licencias por Volumen. Son las licencias que una organización adquiere a través de un acuerdo corporativo con Microsoft. Son licencias de actualización, es decir, requieren una licencia de Windows OEM en el equipo sobre el que se van a instalar. Existen distintas configuraciones para la adquisición de licencias por volumen de Microsoft Windows 10, que vamos a describir a continuación, cada una de las cuales proporciona un conjunto distinto de funcionalidades adicionales.

Las configuraciones más habituales para empresa relativas a las licencias de volumen de MS Windows 10 son las siguientes:

a) Microsoft Windows 10 Pro Upgrade. Proporciona derechos de actualización a Microsoft Windows 10 Pro para equipos que dispongan de licencias de sistema operativo anteriores (por ejemplo, Microsoft Windows 8.1 Pro). Además, proporciona otros derechos adicionales sobre las licencias OEM, como por ejemplo el derecho de reimagen de los equipos.

b) Microsoft Windows 10 Enterprise LTSB. Proporciona la funcionalidad adicional incluida en la versión Enterprise de Microsoft Windows 10, destinada especialmente a mejorar las capacidades de seguridad y gestión de las grandes organizaciones. Algunas de las funcionalidades que se incluyen en esta versión son por ejemplo Direct Access, que es una solución de VPN transparente para el usuario o Credential Guard y Device Guard, dos de las nuevas funcionalidades de seguridad de Windows 10. Esta licencia permite el uso de las funcionalidades de Microsoft Windows Enterprise en el modelo de versionado denominado Long Term Servicing Branch (LTSB).

c) Microsoft Windows 10 Enterprise con Software Assurance (renombrado Windows 10 Enterprise E3). Proporciona la funcionalidad adicional incluida en la versión Enterprise de Microsoft Windows 10 más una serie de beneficios adicionales, como el derecho de uso del paquete Microsoft Desktop Optimization Package (MDOP). Este paquete incluye, entre otras, la solución de seguridad Microsoft Bitlocker Administration and Monitoring (MBAM), que permite la gestión centralizada de Bitlocker, la herramienta de cifrado de Windows. Además, con esta opción es posible utilizar las funcionalidades de Windows Enterprise tanto en el modelo de versionado LTSB como en el nuevo modelo de servicio Current Branch for Business (CBB).

d) Microsoft Windows 10 Enterprise E5. Es una nueva oferta de licenciamiento para Windows 10, que incluye los derechos de uso incluidos en Windows 10 Enterprise E3 más la opción de utilizar el nuevo servicio de seguridad Windows Defender Advanced Threath Protection.

Nota: La comparativa completa entre la funcionalidad de las distintas versiones de MS Windows 10 se puede consultar en el siguiente enlace:
https://www.microsoft.com/es-es/WindowsForBusiness/Compare

6. NUEVAS FUNCIONALIDADES Y COMPONENTES EN MICROSOFT WINDOWS 10

Microsoft Windows 10 incorpora nuevas funcionalidades y componentes que bien no existían en versiones previas o bien han cambiado de forma significativa.

Se enumerarán y se dará una breve descripción sobre las mismas, completando, posteriormente, con un detalle más significativo de aquellos elementos más críticos. No obstante, se debe tener en consideración que algunas de las funcionalidades y/o componentes citados no se encontrarán disponibles en la opción LTSB o bien se encontrarán deshabilitados o limitados con las funcionalidades de seguridad que se aplican tras la fortificación del sistema a través de la presente guía.

Las nuevas funcionalidades que se incorporan son las siguientes:

a) **Entorno de escritorio.** La nueva revisión del escritorio de Windows abandona el interfaz metro de Microsoft Windows 8 y adquiere similitudes con el escritorio tradicional de Windows, apoyado sobre Modern App.

b) **Autenticación: Microsoft Passport y Windows Hello.** Microsoft Windows 10 ofrece continuidad a los mecanismos de autenticación que ya presentaba Microsoft Windows 8 y que mejoraron algunos aspectos de Microsoft Windows 7. Adicionalmente, incorpora una forma más personal de iniciar sesión en los dispositivos a través de Windows Hello (autenticación biométrica). Realmente la novedad importante y que cambia totalmente los mecanismos de Autenticación es Microsoft Passport. Este mecanismo permite implementar una autenticación de doble factor mediante la autenticación con credenciales vinculadas a un dispositivo y la autenticación de Windows Hello o un PIN.

Nota: Para más información de estos componentes consulte la siguiente dirección URL.
https://technet.microsoft.com/es-es/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511

c) **Sistema de telemetría.** Dentro de los mecanismos de mejora y soporte de Microsoft, Microsoft Windows 10 incorpora un servicio de recolección de datos y telemetría con el fin de mejorar las condiciones de soporte. Los datos serán remitidos a Microsoft para ofrecer mejoras en los servicios.

d) **Tienda de Microsoft.** Microsoft Windows 8 incorporó la funcionalidad de la tienda para dar respuesta a una necesidad de usuario de aplicaciones integradas a la usanza de las empleadas en dispositivos móviles o tabletas. Microsoft Windows 10 mantiene dicha funcionalidad incorporando nuevas mejoras como la Tienda para empresas. Con la nueva Tienda Windows para empresas, las organizaciones pueden realizar compras por volumen de aplicaciones de Windows. La Tienda para empresas ofrece compras de aplicaciones basadas en identidad organizativa, opciones flexibles de distribución y la capacidad de recuperar o reutilizar las licencias. Las organizaciones también pueden usar la Tienda para empresas y crear una tienda privada para sus empleados, que incluye aplicaciones de la tienda, así como aplicaciones privadas de línea de negocio (LOB). Este componente no se encuentra disponible en la opción de mantenimiento LTSB.

e) **Aplicaciones para la Plataforma universal de Windows (UWP).** También conocidas como Appx o Modern App. Este tipo de aplicaciones representan el nuevo concepto de aplicaciones universales que difiere del modelo tradicional de aplicaciones. Disponibles en todas las versiones de producto, pueden ser implementadas sobre un puesto de trabajo o un dispositivo móvil. Debe tenerse en consideración que determinados paneles del escritorio son aplicaciones de este tipo. Este componente se encuentra limitado en la opción LTSB, al no disponer de la tienda de Microsoft, y controlado mediante la implementación de políticas de grupo.

f) **Sistema Experiencia de Usuario.** Microsoft proporciona al usuario una serie de nuevas funcionalidades en el uso del dispositivo y la comunicación con Internet. Ofrece capacidad de respuesta ante nuevas necesidades facilitando datos y respuesta ante las necesidades del usuario. Este hecho requiere, en numerosas condiciones, el envío de datos y/o usos del sistema.

g) **Servicio Cortana.** Es el nuevo asistente personal que suministra información al usuario y permite facilitar información del sistema y/o Internet. Este componente no está disponible en la opción de mantenimiento LTSB.

h) **Internet Explorer 11 y Microsoft Edge.** Microsoft Windows 10 incorpora dos navegadores diferentes. Internet Explorer supone el concepto tradicional de navegación, mientras que Microsoft Edge ofrece nuevas funcionalidades que se adaptan a las condiciones de navegación de Internet en la actualidad y supone una nueva experiencia de usuario. La opción de mantenimiento LTSB no incluye Microsoft Edge, solamente incluye Internet Explorer 11.

6.1 INTERFAZ

Uno de los cambios más significativos que ofrece Microsoft Windows 10 lo constituye la interfaz. Microsoft Windows 8 y Microsoft Windows Server 2012 incorporaron la interfaz Metro, abandonando la interfaz de escritorio más tradicional.

Microsoft Windows 10 para puestos de trabajo recupera la esencia del escritorio tradicional, pero incluyendo un nuevo menú inicio modernizado con elementos visuales similares a Metro. Desde el punto de vista del usuario, el sistema tiene una semejanza mayor al concepto tradicional de Microsoft Windows 7 frente al concepto Metro que incorporó Microsoft Windows 8.

En este entorno de fusión se incluye la “Plataforma Universal de Windows – UWP”, también conocidas como Appx. Se tratan de aplicaciones que se incluyen precargadas en Microsoft Windows 10 y que añaden funciones añadidas para Windows y que pueden ser adquiridas a través de la Tienda de Microsoft.

No obstante, debe conocerse que determinados componentes como el menú inicio o determinados paneles de administración son realmente Appx. Es, por lo tanto, requerido el funcionamiento del servicio de gestión de Appx (AppXSvc) para que la actividad del usuario no se vea mermada al inhabilitarse paneles esenciales para el trabajo diario mediante la desactivación del servicio.

6.2 TELEMETRÍA

Dentro de los nuevos componentes existentes en Microsoft Windows 10, el de Telemetría sería uno de los que mayor conectividad realizaría hacia Internet. Sin embargo, también es el que ofrece una mayor capacidad de granularidad para su control. El servicio de telemetría es empleado por Windows para analizar y solventar problemas del Sistema Operativo. Dicha funcionalidad de telemetría opera tanto de forma interna, generando registros internos de actividad, como remitiendo en determinadas condiciones envíos de información a Microsoft. La telemetría proporciona las siguientes características:

a) Comprobar, y llevar a cabo la actualización del sistema operativo.

b) Mantener el sistema operativo seguro, confiable y eficaz.

c) Mejorar el sistema operativo mediante el análisis de los datos agregados de uso de Windows en una enorme muestra representativa de máquinas.

En Microsoft Windows 10 se han establecido 4 niveles de comportamiento de la telemetría:

a) Seguridad.

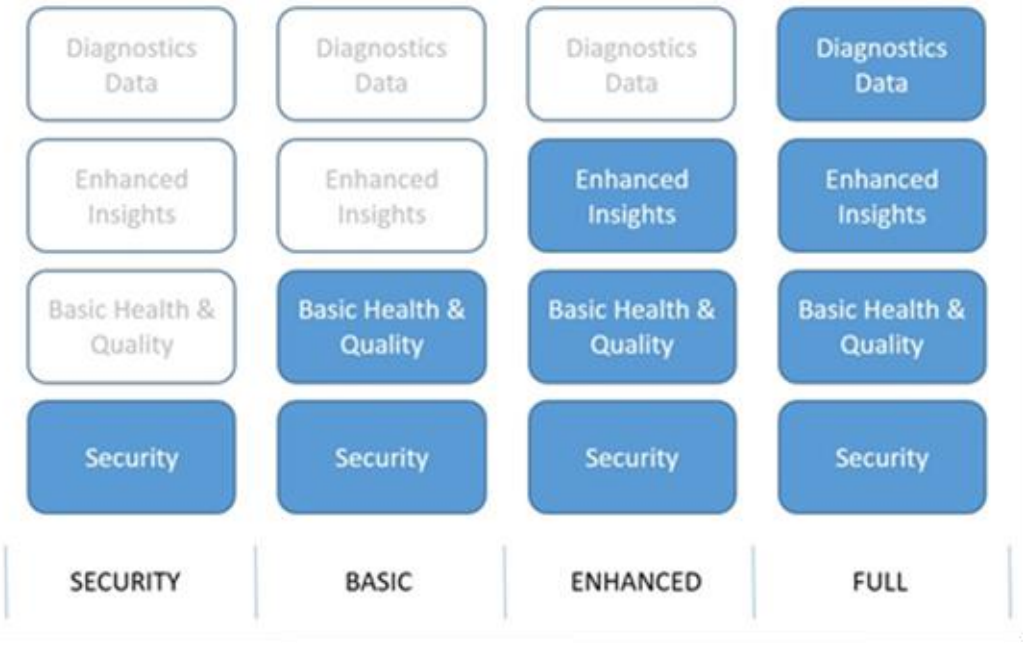
b) Básico.

c) Avanzado.

d) Completo.

Estos niveles están disponibles en todas las ediciones móviles y de escritorio de Microsoft Windows 10, con la excepción del nivel de Seguridad, que está limitado a Windows 10 Enterprise, Windows 10 Education, Windows 10 Mobile Enterprise, Windows10 IoT Core (IoT Core) y Windows Server2016.

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



Cada nivel de telemetría incrementa el nivel de datos que estarían siendo manejados por dicho componente:

a) La configuración del nivel de telemetría en nivel de seguridad trataría la siguiente información:
   i. Configuraciones base de experiencia de usuario. La información manejada sería información del Sistema Operativo, Id de dispositivo y clase de dispositivo.
   ii. Malicious Software Removal Tool. Información tratada por la herramienta que puede descargarse a través de Windows Update.
   iii. Windows Defender. Información tratada por la herramienta antimalware con la que contaría Microsoft Windows 10.

b) La configuración de telemetría en modo básico, adicionalmente a la seguridad, manejaría la siguiente información:
   i. Información básica del dispositivo. Se incluyen como fundamentales atributos de los dispositivos versión de navegador, atributos de procesador y memoria, edición de Windows y otros.
   ii. Métricas cualitativas de experiencia de usuario. Se incluirían eventos relacionados con eventos de tiempos de carga o descarga de componentes.
   iii. Funcionalidad de la compatibilidad de aplicaciones.
   iv. Información de la tienda, descarga y comportamiento de aplicaciones de la misma.

c) La configuración de telemetría en modo avanzado, manejaría la siguiente información adicionalmente a la citada en el modo de seguridad y básico:
   i. Eventos del sistema operativo.
   ii. Eventos de aplicaciones del sistema operativo.
   iii. Eventos de determinados dispositivos.

d) La configuración de telemetría en modo completo, además de la información manejada en los anteriores niveles, establecería el empleo de la siguiente información:
   i. Información incluida dentro del programa Windows Insider. Esto incluye cualquier contenido que, dentro del acuerdo del programa, Microsoft pueda necesitar para dar respuesta al soporte solicitado.

De los niveles existentes, el de seguridad correspondería al de menor envío de información, siendo el mayor el correspondiente al de nivel completo.

Nota: Para más información sobre la configuración de la telemetría y otros componentes de Microsoft Windows 10 consulte la siguiente dirección URL:
https://technet.microsoft.com/en-us/library/mt577208(v=vs.85).aspx#BKMK_UTC

6.3 AUTENTICACIÓN

La autenticación es un proceso que comprueba la identidad de un objeto, un servicio o una persona. Cuando se autentica un objeto, el objetivo es comprobar que el objeto es quien dice ser (auténtico), por ejemplo, cuando se autentica un servicio o un usuario, el objetivo es validar que las credenciales presentadas sean auténticas.

En un contexto de redes, la autenticación es el acto de probar la identidad a una aplicación o recurso de red. Por lo general, la identidad se demuestra mediante una operación criptográfica que utiliza una clave que solo el usuario conoce o una clave compartida. La parte del servidor encargado del intercambio de autenticación compara los datos firmados con una clave criptográfica conocida, para validar el intento de autenticación.

Microsoft Windows 10 presenta cambios en el modelo de autentificación con respecto a las versiones previas del Sistema Operativo. Estos cambios podrían llegar a afectar a algunas de las funcionalidades que pudieran encontrase en producción, por lo que es necesario conocerlas y valorarlas.

Estos son los cambios más significativos en cuanto a los procesos de autenticación:

a) **Kerberos.** Ha sufrido cambios en la delegación restringida entre dominios internos del bosque. Compatibilidad con datos de autorización de notificaciones. Protección de Kerberos a través de túnel seguro de autenticación flexible (FAST). Todos los cambios relativos a la autenticación Kerberos se encuentran en la siguiente dirección URL.

   https://msdn.microsoft.com/es-es/library/hh831747(v=ws.11).aspx

b) **Biometría.** Presenta mejoras en los cambios rápidos de usuarios con dispositivos biométricos y en la compatibilidad con proveedores de credenciales. Se incorpora también la funcionalidad de Windows Hello como mecanismo adicional para el inicio de sesión.

c) En Microsoft Windows 10, Microsoft Passport reemplaza las contraseñas con autenticación segura en dos fases que consta de un dispositivo inscrito y Windows Hello (biométrico) o PIN. Microsoft Passport permite a los usuarios autenticarse en una cuenta Microsoft, en una cuenta de Active Directory, en una cuenta de Microsoft Azure Active Directory (AD) o en un servicio Microsoft que admita la autenticación mediante Fast ID Online (FIDO). Después de una comprobación inicial de dos pasos durante la inscripción a Microsoft Passport, éste se configura en el dispositivo del usuario y posteriormente el usuario establece un modo de autenticación biométrica (huella dactilar, iris o reconocimiento facial) basada en Windows Hello o un PIN. El usuario proporciona el gesto para comprobar la identidad y Windows usa Microsoft Passport para autenticar al usuario y permitirle el acceso a recursos y servicios protegidos.

d) **Tarjetas inteligentes virtuales.** Se agrega soporte para tarjetas inteligentes virtuales. Éstas imitan la funcionalidad de las Smart Card físicas. Usan el chip TPM para almacenar la tarjeta virtual estando siempre disponible en el equipo y pudiendo acceder el usuario, a través del chip criptográfico, a su tarjeta bajo demanda. El chip TPM puede almacenar diferentes tarjetas para múltiples usuarios que estuvieran empleando el equipo.

6.4 OPCIONES DE PRIVACIDAD

Debido a las características de nuevo uso de dispositivos y a la experiencia de usuario, existen muchos mecanismos de intercambio de información hacia Internet. El sistema operativo ofrece mecanismos para garantizar la confidencialidad del uso del sistema y la información tratada en el mismo.

Las opciones de privacidad existentes en Microsoft Windows 10 afectan a los siguientes componentes:

a) General.

b) Ubicación.

c) Cámara.

d) Micrófono.

e) Voz, entrada manuscrita y escritura.

f) Información de cuenta.

g) Contactos.

h) Calendario.

i) Mensajería.

j) Señales de radio.

k) Otros dispositivos.

Dichas opciones de privacidad pueden ser configuradas en el proceso de instalación, posteriormente tras la instalación o por políticas de grupo.

6.5 CONTROL DE CUENTAS DE USUARIO

El control de cuentas de usuario (UAC) fue introducido en Microsoft Windows Vista y Microsoft Windows Server 2008 como un mecanismo para limitar las acciones administrativas de aquellos usuarios que no eran conscientes del empleo de sus privilegios. UAC permite a los usuarios iniciar sesión en sus equipos con una cuenta de usuario estándar. Los procesos lanzados utilizando un token de usuario estándar pueden realizar tareas mediante los derechos de acceso concedidos a un usuario estándar. Por ejemplo, el explorador de Windows automáticamente hereda permisos de nivel de usuario estándar. Además, todos los programas que se ejecutan mediante el explorador de Windows (por ejemplo, haciendo doble clic en un acceso directo de la aplicación) también se ejecutan con el conjunto estándar de permisos de usuario. Muchas aplicaciones, incluyendo las que se incluyen con el sistema operativo, están diseñadas para funcionar de esta manera.

No obstante, otras aplicaciones, especialmente aquellas que no fueron diseñadas específicamente otorgando prioridad a la configuración de la seguridad, a menudo requieren permisos adicionales para poder ser ejecutadas con éxito. Este tipo de programas se denominan aplicaciones heredadas. Además, acciones como instalar nuevo software y realizar cambios de configuración en programas como Firewall de Windows, requieren más permisos que los que están disponibles en una cuenta de usuario estándar.

Cuando una aplicación tiene la necesidad de ejecutar con derechos de usuario más estándar, la UAC puede restaurar grupos de usuarios adicionales para el token. Esto permite al usuario tener un control explícito de programas que están haciendo cambios de nivel de sistema para su máquina. Tras la revisión de la directiva P3P de privacidad del sitio web, el usuario podrá especificar cómo desea que internet administre las cookies de dicho sitio web o si se permite o no que el sitio web almacene cookies en el equipo. Esto, se hará a través de la comparación de la directiva de privacidad del sitio con la configuración de privacidad del usuario. Para ello, el usuario deberá activar la casilla “Comparar la directiva de privacidad de las cookies con mi configuración”.

En MS Windows 10 la funcionalidad del UAC es mejorada para:

a) Permitir que un usuario con privilegios de administrador pueda configurar la experiencia UAC a través del Panel de Control.

b) Proporcionar directivas de seguridad local adicional que permitan que un administrador local cambie el comportamiento de los mensajes UAC, para administradores locales, en modo de aprobación de administrador.

c) Proporcionar directivas de seguridad local adicional que permitan que un administrador local cambie el comportamiento de los mensajes UAC para los usuarios estándar.

7. FUNCIONALIDADES ADICIONALES DE SEGURIDAD EN LA VERSIÓN MICROSOFT WINDOWS 10 ENTERPRISE

Durante la presente guía solo se tienen en consideración el uso de las versiones Enterprise y Pro para Microsoft Windows 10.

Nota: Es necesario evaluar cada anexo de este documento para establecer qué medidas de seguridad se van a implantar en los sistemas a securizar, dependiendo de si el entorno del sistema pertenece a una red clasificada, o es un entorno de aplicación dentro del ENS.

MS Windows 10 en su versión Enterprise incorpora una serie de funcionalidades que aportan características de seguridad no incluidas en la versión Pro. Las organizaciones deberán tener en cuenta dichas características a la hora de identificar la versión más adecuada para la implementación de los puestos de trabajo.

Dichas funcionalidades son las siguientes:

a) AppLocker.

b) MBAM.

c) Direct Access.

d) Windows To Go.

e) Credential Guard.

f) Device Guard.

7.1 APPLOCKER

AppLocker es una característica heredada de Microsoft Windows 8 y presente en la versión Enterprise de Microsoft Windows 10. Esta característica reemplaza la característica Directivas de restricción de software. AppLocker controla la manera en que se accede a los archivos por parte de los usuarios y su uso.

AppLocker 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.

Las reglas de AppLocker permiten o impiden el inicio de una aplicación. AppLocker no controla el comportamiento de las aplicaciones después de que éstas se han ejecutado. En la práctica, una aplicación que está permitida por AppLocker podría utilizar indicadores para pasar por alto las reglas definidas a través de él e iniciar procesos secundarios. Para entornos altamente críticos, se debería realizar un análisis de las aplicaciones investigándolas de forma minuciosa antes de permitir que se ejecuten mediante reglas de AppLocker.

Esta funcionalidad resulta especialmente útil en la protección contra la ejecución de aplicaciones de código dañino de tipología Cryptolocker. Estos se ejecutan habitualmente desde el contexto del usuario. Una buena configuración de AppLocker impedirá su ejecución por ejemplo desde el perfil del usuario, lugar habitual desde el que se lanzan. Aplicaciones portables u otras, también pueden ser contraladas a través de las reglas de AppLocker.

La versión Pro de Microsoft Windows 10 incluye la funcionalidad de AppLocker, pero solo para el modo auditoría. En este caso no permite el bloqueo de las aplicaciones.

7.2 MBAM

MBAM (Microsoft Bitlocker Administration and Monitoring) es una característica de Microsoft Windows 10 Enterprise que hace referencia a la administración y supervisión de Microsoft BitLocker, proporcionando la capacidad de administración de forma empresarial y simplificada tanto para Bitlocker To Go como para BitLocker.

Facilita mecanismos para implementación de las claves de cifrado y recuperación, junto con los mecanismos para la recuperación de las mismas.

Ofrece además la posibilidad de establecer procesos de supervisión en el acceso a las claves, así como la generación de informes sobre el cumplimiento.

MBAM permite:

a) Automatizar los procesos de cifrado mediante Bitlocker en los clientes.

b) Proporciona un portal de autoservicio para la obtención de las claves de recuperación de aquellos dispositivos que se encuentren cifrados.

c) La administración de hardware y la generación de informes.

d) Determinar el estado de cumplimiento de los equipos cliente.

e) Auditar el acceso a las claves de recuperación tanto de los administradores como de los propios usuarios, tanto para el portal de Help-Desk, como el de autoservicio.

7.3 DIRECT ACCESS

DirectAccess es un tipo avanzado de red virtual privada (VPN) ya que crea automáticamente una conexión bidireccional entre los clientes y la red a la que se conectan.

Es el resultado de la combinación del protocolo de seguridad de Internet o IPsec y el protocolo de Internet versión 6 o IPv6. DirectAccess utiliza IPsec con la finalidad de asegurar las comunicaciones que se establecen por Internet. A su vez también utiliza IPsec para autenticar al cliente. lo que permite la administración del equipo por parte del personal responsable de forma previa a que se produzca el inicio de sesión del usuario.

El servidor DirectAccess actúa como puerta de enlace entre el cliente y la intranet mediante el uso de un túnel IPsec para el tráfico IPv6. Microsoft Windows 10 proporciona un mejor soporte para las características de DirectAccess que mejoran el rendimiento y disponibilidad y a la vez es más fácil de implementar y mantener. La implementación de DirectAccess en varias ubicaciones geográficas facilita a grandes organizaciones y a sus clientes Microsoft Windows 10 la conexión ya que son conocedores de todos los despliegues de DirectAccess seleccionando siempre el punto más cercano.

Microsoft Windows 10 incluye soporte para cifrado mediante IP-HTTPS null encryption, esta característica mejora considerablemente la escalabilidad en el servidor de DirectAccess mediante la eliminación de la doble encriptación necesaria en anteriores clientes reduciendo el consumo de recursos del servidor y permitiendo más conexiones de clientes de Direct Access.

A través de Direct Access un equipo que inicia la sesión tendrá a su disposición el acceso a los recursos de la organización tales como el acceso a las Políticas de Grupo u otros elementos de configuración importantes para la misma. El sistema por lo tanto no se encontrará limitado ante la necesidad de realizar una conexión física a la infraestructura organizativa.

Este componente resulta extremadamente útil para el personal desplazado de media o larga duración.

7.4 WINDOWS TO GO

La versión Enterprise de Microsoft Windows 10 permite generar en un Pendrive un sistema operativo para el arranque desde el mismo. Windows to GO es una interesante característica de productividad móvil empresarial que permite instalar, transportar y ejecutar el escritorio completo de un usuario en una unidad de almacenamiento externo, posibilitando a los departamentos TI apoyar la tendencia BYOD (Bring your own device) sin comprometer la seguridad del entorno corporativo.

Windows to GO no está destinado a reemplazar equipos de escritorio, equipos portátiles ni suplantar otras ofertas de movilidad, pero permite usar los recursos de manera eficaz en escenarios de área de trabajo alternativos. El área de trabajo de Windows To Go funciona igual que cualquier otra instalación de Windows con algunas excepciones:

a) Los discos internos están desconectados.

b) No se usa el Módulo de plataforma segura (TPM)

c) La hibernación está deshabilitada de manera predeterminada.

d) No está disponible el Entorno de recuperación de Windows.

e) No se admite la actualización ni el restablecimiento de un área de trabajo de Windows To Go.

7.5 CREDENTIAL GUARD

Credential Guard es una nueva característica introducida en Microsoft Windows 10 Enterprise que utiliza la seguridad basada en virtualización para aislar información confidencial de tal manera que únicamente el software con privilegios suficientes pueda acceder a ella. Credential Guard evita ataques de Pass-the-Hash mediante la protección de los hashes de contraseñas y de los tickets Kerberos. Por motivos de seguridad, el proceso LSA aislado no hospeda ningún controlador de dispositivo. En su lugar, solo hospeda un pequeño subconjunto de binarios del sistema operativo que solo son necesarios para la seguridad. Todos estos binarios se firman con un certificado de confianza de la seguridad basada en la virtualización y estas firmas se validan antes de iniciar el archivo en el entorno protegido.

Credential Guard aísla secretos que versiones anteriores de Windows almacenaron en la autoridad de seguridad local (LSA) mediante seguridad basada en la virtualización. Antes de Windows 10, la LSA almacenaba secretos usados por el sistema operativo en la memoria del proceso. Con Credential Guard, el proceso de LSA en el sistema operativo se comunica con un nuevo componente denominado proceso LSA aislado que almacena y protege estos secretos. Los datos almacenados mediante el proceso LSA aislado se protegen con la seguridad basada en la virtualización y no son accesibles para el resto del sistema operativo. LSA usa llamadas a procedimiento remoto para comunicarse con el proceso LSA aislado. Además, Credential Guard no admite variantes anteriores de conjuntos de cifrado y protocolos de autenticación de Kerberos y NTLM al usar credenciales derivadas predeterminadas, incluidas NTLMv1, MS-CHAPv2 y tipos de cifrado Kerberos menos seguros, como DES.

Credential Guard proporciona las siguientes características:

a) Seguridad de hardware Credential Guard. Aumenta la seguridad de las credenciales de dominio derivadas de sacar provecho de las características de seguridad de la plataforma, como el arranque seguro y la virtualización.

b) Seguridad basada en la virtualización. Los servicios de Windows que administran las credenciales de dominio derivadas y otros secretos se ejecutan en un entorno protegido que está aislado del sistema operativo en ejecución.

c) Mejor protección contra las amenazas permanentes avanzadas. Si se protegen las credenciales de dominio derivadas con la seguridad basada en la virtualización, se bloquean las técnicas de ataques de robo de credenciales y herramientas que se usan en muchos ataques dirigidos. Con la ejecución de malware en el sistema operativo con privilegios administrativos no se pueden extraer secretos que están protegidos con la seguridad basada en la virtualización. Aunque Credential Guard es una mitigación eficaz, los ataques de amenazas persistentes probablemente cambiarán por nuevas técnicas de ataque y también deberías incorporar Device Guard y otras arquitecturas y estrategias de seguridad.

d) Facilidad de uso. Se puede administrar Credential Guard mediante la directiva de grupo, WMI, desde un símbolo del sistema y de Windows PowerShell.

Esta importante mejora de seguridad previene frente a ataques tradicionalmente empleados por atacantes o código dañino para el robo de credenciales.

7.6 DEVICE GUARD

Device Guard es una combinación de características de seguridad de hardware y software relacionadas con la empresa que, configuradas conjuntamente, bloquean un dispositivo para que solo pueda ejecutar aplicaciones de confianza. Si la aplicación no es de confianza, no se podrá ejecutar. Esto también significa que incluso si un atacante consigue controlar el kernel de Windows, es mucho menos probable que pueda ejecutar código malintencionado después de que el equipo se reinicie debido a la forma en que se toman las decisiones sobre qué se puede ejecutar y en qué momento.

Device Guard usa la nueva seguridad basada en virtualización de Microsoft Windows 10 Enterprise para aislar el servicio de integridad de código del propio kernel de Microsoft Windows, lo que permite al servicio usar firmas definidas por la directiva controlada por la empresa para determinar qué es de confianza. De hecho, el servicio Integridad de código se ejecuta en el kernel dentro de un contenedor de Windows protegido por hipervisor.

La confianza entre Device Guard y las aplicaciones se produce cuando las aplicaciones están firmadas con una firma que se considera de confianza. No funcionará cualquier firma. Esta firma se puede realizar mediante:

a) **El proceso de publicación de la Tienda Windows.** Todas las aplicaciones que provienen de Microsoft Store se firman automáticamente con firmas especiales que se pueden implementar en la entidad de certificación (CA) o en la entidad propia.

b) **Certificado propio digital o infraestructura de clave pública (PKI).** Los ISV (Independent Software Vendors o Proveedores de Sofware Independiente) y las empresas pueden firmar sus propias aplicaciones clásicas de Windows y agregarse a sí mismos a la lista de firmantes de confianza.

c) **Una entidad de firma que no es Microsoft.** Los ISV y las empresas pueden usar una entidad de firma de confianza que no es Microsoft para firmar sus propias aplicaciones clásicas de Windows.

d) **Un servicio web proporcionado por Microsoft (disponible a lo largo de este año).** Los ISV y las empresas podrán usar un servicio web proporcionado por Microsoft más seguro para firmar sus aplicaciones clásicas de Windows.