centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN MICROSOFT OFFICE 2016 SOBRE MICROSOFT WINDOWS 10

FEBRERO 2019

MINISTERIO DE DEFENSA

Edita:

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
2019.02.15 12:41:21 +01'00'

NIPO: 083-19-119-2
Fecha de Edición: febrero de 2019

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, actualizado 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.

febrero de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación 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.

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, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. 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 Microsoft 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 Server 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 Server 2012 R2.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para la implementación y garantizar la seguridad del sistema mediante el tratamiento de archivos ofimáticos utilizados por la suite de aplicaciones Microsoft Office 2016. Se entiende para ello la necesidad de realizar una instalación segura del producto, así como la aplicación de los mecanismos que disminuyan el riesgo y la superficie de ataque que pudiera derivar del uso de ficheros de tipo ofimático.

La presente guía tiene como objeto la instalación y uso seguro de la suite de aplicaciones Microsoft Office 2016, en dos posibles condiciones:

a) Puestos de trabajo que se encuentren integrados en una infraestructura de dominio.

d) Puestos de trabajo independientes que no se encuentren unidos a un dominio.

La instalación, así como los usos del paquete ofimático se han diseñado para que la implementación sea lo más restrictiva posible, minimizando la superficie de ataque y por lo tanto los riesgos que pudieran existir. Es factible que el uso de determinadas funcionalidades de MS Office 2016 requiera modificar las configuraciones que se plantean con la presente guía.

No es objeto de este documento las ediciones de “Microsoft Office 365”, las cuales se basan en un uso tipo online, principalmente, y aquellos paquetes no destinados a entornos empresariales, como Office Hogar y Estudiantes.

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.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica para realizar una implementación del paquete ofimático Microsoft Office 2016 en sus ediciones Standard y Professional Plus, especialmente esta segunda. Se plantean también las posibles operaciones de administración y aquellas acciones que deben ser llevadas a cabo para el mantenimiento de la solución.

Los escenarios en el los cuales se basa la presente guía cuentan con las siguientes características técnicas:

a) Implementación de la solución en equipos Microsoft Windows 10 Enterprise o Pro con opciones de mantenimiento CB, CBB y versiones Enterprise con opción de mantenimiento LTSB pertenecientes a un bosque de Directorio Activo Windows 2016.

b) Implementación de la solución en equipos Microsoft Windows 10 Enterprise o Pro con opciones de mantenimiento CB, CBB y versiones Enterprise con opción de mantenimiento LTSB independientes que no se encuentran vinculados a un dominio.

Esta guía (el documento presente y los ficheros relacionados) incluye:

a) **Descripción de las ediciones y de los tipos de licenciamiento:** se centra en los productos editados por Microsoft para empresas.

b) **Descripción de las amenazas y contramedidas para garantizar la seguridad en Microsoft Office 2016:** completa descripción de los riesgos existentes en la utilización de productos ofimáticos, así como las contramedidas que pueden aplicarse para contrarrestar las amenazas.

c) **Mecanismos para la implementación de la solución:** se incorporan mecanismos para la implementación de la solución de forma automatizada, por ejemplo, scripts.

d) **Mecanismos para la aplicación de configuraciones:** se incorporan mecanismos para la planificación de las configuraciones de seguridad susceptibles de ello.

e) **Descripción de los componentes de la suite:** se describen todos los productos de la edición Microsoft Office 2016 Professional Plus (el empaquetado más amplio).

f) **Guías paso a paso:** que permiten implantar y establecer las configuraciones de seguridad en puestos de trabajo miembros del dominio o independientes.

g) **Guía de administración:** que capacita para realizar tareas de administración en el entorno de seguridad establecido.

h) **Lista de comprobación:** que posibilita verificar el grado de cumplimiento de un equipo con respecto a las condiciones de seguridad que se establecen en esta misma guía.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad es conveniente explicar el proceso de refuerzo de la seguridad que describe y los recursos que proporciona. Este procedimiento constará, a grandes rasgos, de los siguientes pasos:

a) Deberá configurarse el sistema operativo base de manera segura utilizando la guía codificada como CCN-STIC-599A18 o CCN-STIC-599B18, en función de si el puesto cliente es Windows 10 miembro o no de un dominio respectivamente.

b) Instalar, configurar y aplicar la plantilla de seguridad, que corresponda, de Microsoft Office 2016, tal y como se describe en la presente guía.

5.1 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, ambos 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.

Así mismo, se ha diseñado para reducir la superficie de exposición de los puestos de trabajo y aplicar contramedidas para garantizar un uso correcto y seguro de las aplicaciones existentes en la suite Microsoft Office 2016 Standard o Microsoft Office 2016 Professional Plus. Si instala la suite Microsoft Office 2016 Standard pudiera encontrar diferencias con la información dispuesta en la presente guía puesto que conlleva un menor número de aplicaciones que las que pueden instalarse junto con MS Office 2016 Professional Plus además de requerir una instalación distinta. Más adelante se detallan las principales características de los distintos paquetes y versiones, así como una comparativa.

Nota: En cada uno de los apartados se indicará expresamente sobre qué edición de Office 2016 se opera, si no fuese así es porque aplica solo a las ediciones Professional Plus y Standard.

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

a) Servidor Dell PowerEdge™ T320:
   i. Intel Pentium Xeon Quad Core.
   ii. HDD 1 TB.
   iii. 32 GB de RAM.
   iv. Interfaz de red 1 GB.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Microsoft Windows. Esto quiere decir que se requieren equipos con más de 2 GB de memoria RAM, 3 GB de espacio en disco y procesador de 32 o 64 bits a 1 GHz o superior. Tenga en cuenta además los requerimientos mínimos de los que necesita el sistema operativo cliente Windows 10 en cada una de sus versiones.

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

Nota: Puede ver las recomendaciones de Microsoft, con más detalle, en la siguiente URL: https://products.office.com/es-es/office-system-requirements.

Hay que tener en cuenta que la aplicación de la seguridad en un puesto de trabajo miembro del dominio requiere de una infraestructura de Directorio Activo para aplicación de las plantillas de seguridad.

En el caso de puestos de trabajo independientes, la aplicación de políticas se hará a nivel local. Por lo tanto, en caso de realizar una modificación a posteriori, deberá tenerse en cuenta que se mantengan los valores configurados para garantizar la seguridad de la solución MS Office 2016.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura involucrada de la seguridad máxima. Es posible que algunas de las funcionalidades de los productos hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitarlas en las aplicaciones dependientes de MS Office 2016.

Para garantizar la seguridad de las estaciones de trabajo, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Windows Update. Las actualizaciones, por lo general, se liberan el segundo martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento. Se deberá observar la implementación de las actualizaciones tanto para el sistema operativo como para la solución MS Office 2016, que afecta a la presente guía.

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

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado donde se hayan aplicado los test y cambios en la configuración que se ajusten a los criterios específicos de su organización.

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

Adicionalmente en el directorio “Scripts” que se adjunta a este documento existe un directorio denominado “Informes” el cual contiene la configuración de los diferentes objetos GPO y GPL en formato “.htm”.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación de Microsoft Office 2016 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 el producto MS Office 2016 en su versión Professional Plus a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar el producto MS Office 2016 en su versión Professional Plus 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.

6. EDICIONES Y LICENCIAS DE OFFICE

6.1 EDICIONES DE MICROSOFT OFFICE 2016

Microsoft Office 2016 es una suite, o grupo de programas, orientado al trabajo en la oficina y que se presenta en distintos agrupamientos, o paquetes, de esas aplicaciones según el sector o tamaño de la entidad a la que se dirigen: empresa, estudiantes, hogar, etc.

En esta guía se tratan solo aquellas versiones destinadas a la empresa, independientemente del tamaño de ésta.

Desde hace unos años Microsoft ha liberado una versión, con varias ediciones, destinada a todos los sectores (desde el hogar a la gran empresa) que trabaja directamente en nube (cloud), aunque permite también el uso desconectado. Esta versión es conocida de forma genérica como Office 365, pero no es objeto de estudio en esta guía.

Los productos que no se incluyen en ningún paquete, Visio y Project, deben ser adquiridos de forma individual. Puede hacerse con licencias por volumen o retail.

Puede encontrar información adicional de las diferentes ediciones de MS Office 2016 en las siguientes direcciones URL:

https://www.microsoft.com/es-es/licensing/product-licensing/office.aspx

6.2 VERSIONES DE MICROSOFT OFFICE 2016

Independientemente del paquete por el que se opte, Office 2016 se presenta en dos versiones: 32 y 64 bits.

Esta guía tiene en cuenta que el sistema operativo con el que cuenta el cliente es de 64 bits por lo que puede optar por cualquiera de las dos. Microsoft indica entre sus recomendaciones que, de no tener una necesidad expresa, instale en todas las ocasiones la versión de 32 bits, si bien le limitará el tamaño de los ficheros a manejar en Excel y Project, le proporcionará mayor compatibilidad con otras aplicaciones, desarrollos o módulos. Puede ver esta recomendación en la siguiente URL:

https://support.office.com/es-es/article/elegir-entre-la-versi%C3%B3n-de-64-o-la-de-32-bits-de-office-2dee7807-8f95-4d0c-b5fe-6c6f49b8d261

Dependiendo del software que haya adquirido, puede encontrar ciertas diferencias en las carpetas presentes ya que se puede encontrar con el DVD, o imagen descargada desde Microsoft, de la edición de 64 bits, la edición de 32 bits, o la que incluye ambas.

Si utiliza el DVD o imagen descargada de Microsoft que incluye las dos ediciones, 32/64 bits, y ejecuta el fichero “setup.exe” que se encuentra en la raíz o en la carpeta x86 del DVD, la instalación que se realiza es la de 32 bits mientras que si ejecuta “setup.exe” desde la subcarpeta x64 lo hará la edición análoga a ese nombre.

Por todo lo expuesto anteriormente, en esta guía se ha optado por la instalación de Microsoft Office 2016 Professional Plus, edición de 32 bits, a partir de la imagen, tipo iso (descargada del repositorio de Microsoft para licencias por volumen), que incluye las dos ediciones, 32 y 64 bits.

6.3 TIPOS DE LICENCIAS

Microsoft ofrece distintos tipos de licenciamiento pensados para cubrir las distintas necesidades de sus clientes según el entorno y número de equipos: hogar, gran empresa, estudiantes, pequeña empresa, etc.

Los distintos tipos de licencias también incluyen distintos tipos de empaquetados de las aplicaciones y distintas funcionalidades, especialmente para la instalación y administración del producto, ya que considera que no requiere el mismo tratamiento una red de cuatro equipos que una de trescientos, por ejemplo.

Los distintos licenciamientos son:

a) Por volumen.

b) Individual o retail.

Para licencias por volumen puede optar entre Office Standard (no incluye Access, además de ciertas funcionalidades) y Office Professional Plus (versión completa para entornos empresariales).

El licenciamiento por volumen está destinado a medianas y grandes empresas que compran a partir de cinco licencias. Este tipo de licenciamiento permite con un único código de activación licenciar varios equipos, lo que permite disminuir la carga administrativa.

Las instalaciones de Office 2016 bajo este tipo de licencia que no hayan activado el producto pasados unos días, 25 habitualmente, recibirán un aviso para que completen el proceso y si aún no se hiciese aparecerá, bajos los menús de las respectivas aplicaciones, una barra roja avisando de la ilegalidad de la instalación.

En licencias individuales, se puede optar, teniendo como objetivo un entorno empresarial, entre Office Hogar y Empresas (no incluye Access, Publisher, ni ciertas funcionalidades para medianas y grandes empresas) y Office Standard (no ofrece ciertas funcionalidades para medianas y grandes empresas). Las licencias preinstaladas, también conocidas como OEM, no existen ya en Microsoft Office 2016.

El proceso de activación variará de forma significativa según el tipo de licenciamiento, independientemente de la edición que se disponga.

Nota: No se recogen en este documento otro tipo de licenciamientos: Office 365, Office para estudiantes, etc.

Los discos o imágenes de instalación de los distintos tipos de licenciamiento no son intercambiables entre ellos. Por ejemplo, no se podrá activar un Office instalado con un DVD asociado a una licencia por volumen con un código de activación de Office individual.

6.4 RESUMEN DE EDICIONES DE MICROSOFT OFFICE 2016

La siguiente tabla muestra las principales características de los paquetes Office 2016 orientados a la empresa.

Edición (Tipo de licencia)	Standard (volumen)	Professional Plus (volumen)	Hogar y Estudiantes (retail)
Word	☑	☑	☑
Excel	☑	☑	☑
PowerPoint	☑	☑	☑
OneNote	☑	☑	☑
Outlook	☑	☑	
Publisher	☑	☑	
Access		☑	
Skype Empresarial		☑	
Project			
Visio			
Directiva de grupo	☑	☑	
OCT	☑	☑	
Activación por volumen	☑	☑	
Office Web Apps	☑	☑	

Visio y Project no se incluyen en ninguno de los paquetes y deben ser adquiridos con licencias propias.

6.5 ACTIVACIÓN DE MICROSOFT OFFICE 2016

Dependiendo del tipo de licencia, volumen o retail, que se adquiera, Microsoft Office 2016 dispone de distintas herramientas y/o métodos de activación.

En todos los casos, la activación del producto debe ser realizada para poder utilizarlo legalmente.

En algunos casos, el producto no podrá instalarse o utilizarse hasta su activación mientras que en otros se dispone de un periodo de tiempo, variable, hasta que el producto queda marcado definitivamente como no licenciado.

En la versión Office 2016 casi todos los métodos y tipos de licencias requieren de conexión a Internet, sea de forma directa o en, al menos, un equipo de la red para la activación.

La forma de activación de equipos con **licencias por volumen** dependerá de cómo seleccionen los administradores del sistema entre los siguientes métodos:

a) **Servicio de administración de claves (KMS):** Modelo de cliente-servidor en el que debe instalar y activar una clave KMS en un equipo host de KMS. Esto establece un servicio de activación local en el entorno. Los equipos cliente de Office 2016 se conectan al host de KMS local de Office 2016 para la activación, que es el único que requiere conexión a Internet.

b) **Clave de activación múltiple (MAK):** Si usa una MAK, los equipos cliente de Office 2016 se activan en línea a través de los servidores de activación hospedados en Microsoft o bien telefónicamente. En este tipo, se puede optar entre:

   i. Activación **independiente de MAK:** Esta activación requiere que cada equipo se conecte de forma independiente y se conecte con Microsoft, ya sea por **Internet** o por **teléfono**. Resulta más adecuada en equipos que no mantienen una conexión con la red corporativa e indispensable en redes sin conexión a Internet.

   ii. **Activación proxy de MAK con VAMT:** Permite hacer una solicitud de activación centralizada en nombre de varios equipos que tienen una conexión con Microsoft. La activación proxy de MAK se configura con VAMT (Herramienta de administración de activación por volumen). Es apropiada para entornos en los cuales el acceso directo a Internet o a la red corporativa podría estar restringido por cuestiones de seguridad. También es adecuada para laboratorios de desarrollo y prueba que no tienen esta conectividad.

c) **Activación basada en Active Directory:** Solo está disponible para Office 2016 a partir de Windows 8 y de Windows Server 2012 en adelante. La activación basada en Active Directory puede activar todos los clientes con licencia por volumen de Office 2016 de todo un dominio. Esta activación se configura con los Servicios de dominio de Active Directory (AD DS) desde un equipo con una edición de licencia por volumen de Windows para los equipos o una máquina con Windows Server.

Durante el proceso de instalación con una licencia por volumen, no se solicita ningún tipo de código de activación, independientemente del método de activación que se haya usado o si se ha activado o no el producto.

Tenga en cuenta que los métodos arriba indicados pueden requerir conexión a Internet, sea del servidor delegado de las mismas o los propios equipos clientes y que es posible que su organización no disponga del mismo. En las licencias por volumen siempre podrá optar por la activación por teléfono con una clave MAK.

Los plazos para la activación son (pueden variar por distintas condiciones):

a) Cuando se instala **Office Professional Plus** con la imagen descargada desde la web de Microsoft se dispone de un plazo de 25 días antes de quedar marcado el producto como “Producto sin licencia”. Pasado el plazo casi todas las funcionalidades siguen disponibles.

b) Una vez se introduce una clave válida en **Office Professional Plus** se dispone de una semana antes de activarlo.

c) **Office Standard** se comporta de igual forma que Office Professional Plus.

Nota: Para conocer más sobre la activación por volumen consulte la siguiente dirección: https://docs.microsoft.com/en-us/DeployOffice/vlactivation/plan-volume-activation-of-office?toc=/deployoffice/office2016/toc.json

La licencia individual se puede adquirir por separado o preinstalada en equipos nuevos.

Para la versión Office 2016 es indispensable la conexión a Internet para poder obtener Office con una licencia individual, ya que en ningún caso se proporciona CD-ROM o DVD del producto, conteniendo la caja de venta solo la clave de activación.

Una vez completada la primera instalación del equipo es posible bajar, del sitio web de Office, una imagen del DVD del producto.

Cuando se realiza una instalación individual con conexión a Internet, el código de activación queda ligado al equipo y no podrá volver a utilizarse en otro equipo si antes no se desinstala del primero. En caso de pérdida del equipo original, Microsoft acepta un procedimiento que involucra la llamada telefónica para esta excepción.

Para comenzar el proceso de activación/instalación de Office Professional Plus se debe verificar que el equipo dispone de acceso a Internet, pero dado que es posible que los equipos que se han securizado siguiendo las directrices de las guías codificadas como 599A18 y 599B18, en un entorno de alta seguridad, no dispongan de ese acceso de forma predeterminada, por lo que este procedimiento podría ser imposible de realizar. Consulte con el administrador para encontrar alternativas.

Los plazos para la activación son (pueden variar por distintas condiciones):

a) Cuando se instala Office Professional Plus desde la web, el producto queda activado durante el proceso.

b) Cuando se instala Office Professional Plus con el DVD descargado de la web (no es posible hasta después de la primera activación) se debe activar durante la instalación. Si no se realiza, el producto queda reducido a un conjunto de visores (solo lectura) de documentos.

Microsoft Word, del paquete Office Professional Plus de licencia individual, con el periodo de activación vencido y con todas las funcionalidades de edición desactivadas.

6.6 HERRAMIENTAS DE ACTIVACIÓN

Microsoft proporciona muchos métodos de activación, como se ha detallado anteriormente, y también múltiples herramientas para utilizarlos o completarlos. Algunos métodos de activación no necesitan de ninguna de estas herramientas.

El script de la plataforma de protección de software de Office (ospp.vbs), el script del Administrador de licencia de software (slmgr.vbs) y la Herramienta de administración de activación por volumen (VAMT) ayudan a configurar y validar ediciones de licencia por volumen de Office 2016.

En la presente guía dentro de su Anexo B dedicado a Redes Clasificadas, solo se utilizará como método válido el único que no requiere ningún tipo de conexión a Internet, la activación telefónica.

Nota: Puede obtener más información sobre las herramientas de ayuda a la activación en la URL https://docs.microsoft.com/es-es/deployoffice/vlactivation/tools-to-manage-volume-activation-of-office

7. AMENAZAS DE SEGURIDAD PARA MS OFFICE 2016

El tratamiento de documentos de tipo ofimático y el uso del servicio de correo electrónico ofrecidos por el conjunto de aplicaciones MS Office 2016, se pueden ver afectados por diferentes riesgos de seguridad.

Dentro de las categorías existentes, tres de ellos son los que más preocupan en lo que al tratamiento de los ficheros respecta:

a) Riesgos de confidencialidad.

b) Riesgos de integridad.

c) Riesgos de disponibilidad.

Los **riesgos de confidencialidad** representan aquellas amenazas contra la propiedad intelectual, el acceso a información sensible u otras derivadas de accesos no autorizados, bien sean por parte de personas o por códigos malintencionados.

Los **riesgos de integridad** representan las amenazas que tienen como objeto la alteración de la información sin control poniendo en peligro a los activos de negocio, o bien el empleo de mecanismos enfocados a la suplantación de personas y/o elementos de la entidad.

Los **riesgos de disponibilidad** representan aquellas amenazas que intentan perjudicar el modo de funcionalidad de los procesos de la organización y el modo en que los trabajadores realizan su trabajo. Dichas amenazas se materializan en la eliminación parcial o total de los datos o anulando la capacidad para el tratamiento de los mismos.

El modelo de seguridad de MS Office 2016 ayuda a la mitigación de cinco tipos de amenazas reconocidas. Cada una estas categorías incluyen diferentes vectores de ataque que vulneran la seguridad de los datos o de los servicios que los gestionan. Estas amenazas son:

a) De acceso no autorizado.

b) De contenido activo.

c) De contenido externo.

d) De vulnerabilidad de día cero.

e) De explorador.

7.1 AMENAZAS DE ACCESO NO AUTORIZADO

Representan todos aquellos riesgos potenciales cuando usuarios no autorizados intentan acceder a la información.

Estas amenazas afectan a la confidencialidad, la pérdida de integridad y la disponibilidad de los datos.Los riesgos existentes son accesos a archivos de documentos, a su contenido y la publicación de ficheros con la presencia de metadatos sensibles.

Si usuarios no autorizados tienen acceso a los documentos o a su contenido, además de poder leerlos, podrán sustituirlos, dañarlos o eliminarlos. De tal forma, además del riesgo de divulgación o indisponibilidad de la información, un atacante podría alterar el contenido produciendo confusión o engaño en los datos.

Los metadatos constituyen una fuente auxiliar de información que se incluye en las propiedades del fichero. De forma predeterminada, incluyen información, tal como el nombre del usuario que lo ha creado o el equipo donde se ha generado. Esto puede suponer un riesgo para la organización por la divulgación de dicha información. Los metadatos ayudan, a un potencial atacante, a conocer datos confidenciales de la persona o la organización sin tener el mínimo contacto con los mismos ni utilizar técnicas complejas o ilícitas.

Los accesos no autorizados se pueden dar en el uso de medios internos de la organización, pero son más frecuentes cuando los ficheros sensibles se exponen fuera de la misma.

El riesgo aumenta cuando los documentos, especialmente los confidenciales o de contenido sensible, se encuentran fuera del alcance de protección que ofrecen los sistemas internos. Deberán extremarse las medidas aplicadas, garantizando en todo caso que la pérdida de ficheros o accesos no autorizados nunca supongan un riesgo contra la confidencialidad de los datos manejados.

7.2 AMENAZAS DE CONTENIDO ACTIVO

Tradicionalmente, una las amenazas más explotadas en el tratamiento de documentos ofimáticos, lo constituye la explotación de contenido incrustado en los ficheros ofimáticos.

La ejecución de macros de dudosa procedencia o de componentes no controlados permite a un atacante acceder al contenido de un fichero o incluso poder llegar más lejos, comprometiendo la seguridad del sistema sobre el que se trata el documento.

La utilización de códigos malintencionados, incrustados en los documentos, constituye una forma habitual de explotar la seguridad de la organización. A veces, son generados para un uso indiscriminado, aunque también pueden ser especialmente creados para atacar un elemento concreto de la seguridad de una organización.

Abrir documentos de orígenes externos sin una garantía de seguridad puede afectar, de forma directa, a la confidencialidad y a la disponibilidad. De forma indirecta, podría afectar a la integridad de los datos manejados.

Más recientemente, el uso de macros ha derivado en la utilización de complementos o ActiveX de una forma habitual en las diferentes arquitecturas informáticas, pero con consecuencias negativas similares si no se conoce su procedencia o qué comportamiento presentan.

Es posible deshabilitar la ejecución de macros o permitir solo aquellas que estén firmadas de digitalmente y reconocidas por la organización. Esto puede ser una carga de trabajo extra o un inconveniente en algunos casos, por ejemplo, las bases de datos de Access deberían estar firmadas digitalmente para poder ser abiertas, pero proporciona una seguridad requerida en entornos de alta seguridad.

7.3 AMENAZAS DE CONTENIDO EXTERNO

En ocasiones, los documentos o los correos manejados por las aplicaciones de Office 2016, contienen enlaces o hipervínculos que apuntan a direcciones web externas a la organización. El acceso, a través de estos enlaces, puede desembocar en la ejecución desde el sistema interno de contenido externo malicioso, no controlable por parte del usuario.

Este hecho puede desembocar, no solamente en riesgos para la confidencialidad de la información manejada, sino, por ejemplo, que también permite que un atacante genere conexiones de datos a orígenes de datos a los que, de forma predeterminada, tampoco tendría acceso. De esta manera, podría manipular o acceder a datos sensibles de la organización.

Los correos electrónicos también son objeto de este tipo de ataques. Además de los ya conocidos mecanismos de ***phishing***, empleados fundamentalmente para conducir a una persona a una web falsa con contenido similar a la legítima, se emplean otras amenazas de contenido externo. Por ejemplo, se incluye en los correos, a través de un

vínculo invisible, una imagen. Cuando el usuario abre el correo electrónico, el vínculo se activa descargándose la imagen. En sí, la imagen no tiene porqué representar un riesgo para el sistema, pero puede enviar al atacante remoto información sensible del equipo, dirección de correo o el direccionamiento IP empleado.

Hay que tener presente que, a menudo, lo que muestra un texto, por ejemplo, de un enlace web, no implica necesariamente que lo que se ejecute por debajo se corresponda exactamente con ese texto.

7.4 AMENAZAS DE VULNERABILIDAD DE DÍA CERO

La seguridad de las aplicaciones y servicios es, constantemente, puesta a prueba tanto por las propias empresas que las desarrollan como por otras personas ajenas a las mismas. Fruto de dichos análisis son publicados los expedientes de seguridad que afectan o pueden afectar a diferentes componentes.

A través de dichos expedientes se hacen públicas las vulnerabilidades que pueden afectar de muchas formas y con múltiples consecuencias a los sistemas informáticos de una organización.

La publicación de un expediente de seguridad no implica siempre que esa vulnerabilidad no haya sido conocida previamente y/o explotada por potenciales atacantes con el objeto de causar perjuicio a una determinada organización o usuario. La publicación, simplemente, hace público el riesgo materializándose la necesidad de aplicar una corrección bien a través de una actualización de seguridad o mediante la adopción de algún procedimiento o la aplicación de algún mecanismo de seguridad.

Se habla de vulnerabilidad de día cero cuando personas ajenas a los propios desarrolladores son conscientes de un riesgo y lo aprovechan en su beneficio o en el de otros. Cuando el mecanismo para la explotación de la vulnerabilidad de día cero se hace público, se establece una ventana de tiempo crítica para la creación de la solución, habitualmente una actualización y la aplicación de la misma.

Cuanto mayor sea esa ventana de tiempo, mayor será el riesgo que sufra una organización o un sistema de verse afectado por la amenaza.

A lo largo de los años, se han descubierto en los productos de MS Office numerosas vulnerabilidades de día cero. La gran difusión de los productos y el alcance a múltiples organizaciones hacen que sean objeto de análisis por parte de muchas personas ajenas a los propios desarrolladores.

Garantizar una buena seguridad global, la aplicación de los controles para no abrir ficheros de dudosa procedencia y mantener los sistemas actualizados reducen el riesgo de ser afectados por una vulnerabilidad de día cero.

7.5 AMENAZAS DE EXPLORADOR

Esta amenaza se materializa cuando una aplicación o un documento utilizan, por programación, alguna funcionalidad de un explorador web. Se considera esencial la seguridad de los documentos puesto que cualquier amenaza que exista para el explorador también se haría extensiva para la aplicación o el propio documento.

Existen complementos vinculados al navegador que permiten visualizar o tratar ficheros ofimáticos directamente en el mismo. Por lo tanto, la seguridad del navegador interfiere directamente en el tratamiento de los ficheros.

Controles ActiveX dañinos o complementos instalados en el navegador, sin control de su procedencia, pueden comprender una amenaza cuando desde un documento se realiza una llamada al navegador o simplemente se trata el fichero en esta aplicación.

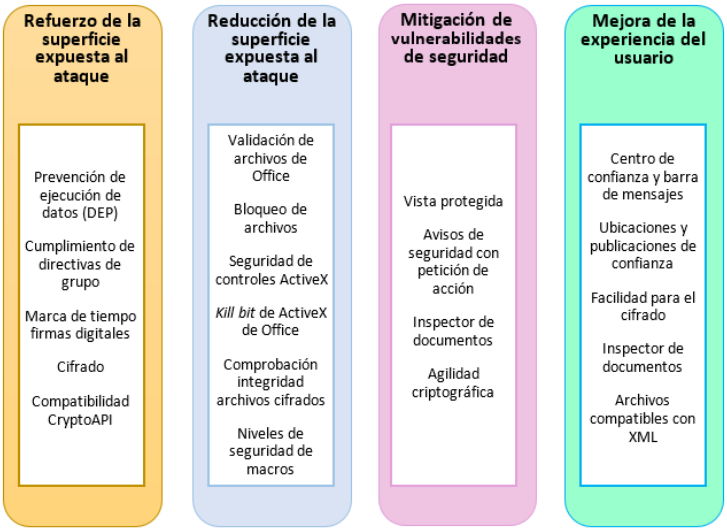
8. SEGURIDAD EN MICROSOFT OFFICE 2016

Microsoft Office es el paquete ofimático líder del mercado corporativo, incluyendo las aplicaciones de tratamiento de documentación, servicios de colaboración y acceso a servicios de correo electrónico.

Tienen funcionalidades de seguridad que ofrecen, a los administradores y usuarios de la solución, una forma de crear una defensa robusta frente a las amenazas existentes, al mismo tiempo que se garantiza el mantenimiento de la productividad en el tratamiento de la información.

La arquitectura de seguridad en MS Office se basa en la aplicación de una estrategia de seguridad en niveles. Las medidas se aplican desde el mismo momento en el que un usuario intenta abrir un fichero con cualquiera de los programas de MS Office, estando presentes hasta que se produce el cierre del mismo. Los niveles en los que estructura la seguridad Office son:

a) Endurecimiento de la superficie expuesta al ataque.
b) Reducción de la superficie expuesta al ataque.
c) Mitigación de vulnerabilidades de seguridad.
d) Mejora de la experiencia de usuario.



Niveles en los que se estructura la seguridad de MS Office.

Adicionalmente a los niveles en los que se estructura la seguridad de MS Office, se aplican también una serie de contramedidas que permiten garantizar la integridad y confidencialidad de los datos manejados.

Los mecanismos de garantía de integridad y confidencialidad de los ficheros suponen una evolución con respecto a las versiones previas de las soluciones MS Office.

El conjunto de aplicaciones de MS Office 2016 permiten diferentes configuraciones de cifrado y el uso de firma digital ofreciendo un modelo seguro para la salvaguarda de los ficheros utilizados.

Desde la versión 2013, Office permite recuperar archivos cifrados, por miembros del dominio, a administradores. De este modo, se evita la pérdida de documentación por cambios de personal u otros motivos.

8.1 ENDURECIMIENTO DE LA SUPERFICIE EXPUESTA AL ATAQUE

La **Prevención de Ejecución de Datos** o **DEP** (del inglés *Data Execution Prevention*) es una característica de seguridad del sistema operativo que ayuda a impedir daños en el equipo producidos por virus y otras amenazas a la seguridad.

Este nivel de protección plantea como objetivo endurecer la seguridad de la superficie expuesta al ataque de las aplicaciones, entre ellas Office, mediante la aplicación de esta contramedida del sistema operativo, DEP.

El sistema de Prevención de ejecución de datos protege frente a los ataques que intentan ejecutar código desde una parte de la memoria reservada a albergar exclusivamente datos que no tienen características de ejecución.

Los ficheros que se abren con las aplicaciones pertenecientes a Office podrían suponer un riesgo para la seguridad del equipo portando códigos maliciosos, al infectar el equipo, ejecutándose desde ubicaciones de memoria reservadas. Este mecanismo constituye una de las múltiples formas que aplicaciones maliciosas han utilizado para infectar y poder expandirse.

Si el módulo de DEP advierte que un programa del sistema intenta hacer un uso de la memoria ilícito lo cierra y envía una notificación al usuario con dicho hecho.

De forma predeterminada, la característica de prevención de ejecución de datos se encuentra habilitada para las aplicaciones de la suite MS Office 2016 y no es accesible desde el Centro de confianza ni por medio de directivas.

Nota: Puede consultar más información sobre la Prevención de ejecución de datos, DEP, en la siguiente dirección web:
https://docs.microsoft.com/en-us/windows/desktop/memory/data-execution-prevention

Microsoft ha reforzado los **sistemas de cifrado** de Office adaptándolos a estándares y a los requerimientos criptológicos del momento.

8.2 REDUCCIÓN DE LA SUPERFICIE EXPUESTA AL ATAQUE

Este nivel de protección limita los tipos de archivos que las aplicaciones pueden abrir, a la vez que evitan que se puedan ejecutar determinados tipos de códigos que pueden encontrarse en un fichero. Este tipo de código pueden ser macros, scripts o componentes de ActiveX que pudieran llegar a ser perjudiciales para el sistema.

Para limitar la superficie de ataque Microsoft ha dispuesto seis contramedidas esenciales:

a) Validación de documentos de Office.

b) Bloqueo de archivos.

c) Bit de cierre, kill bit, de ActiveX.

d) Habilitar o deshabilitar la configuración de controles ActiveX en archivos de Office.

e) Comprobación de la integridad de archivos cifrados.

f) Niveles de seguridad de macros.

El componente de Validación de documentos de Office se encarga de examinar los archivos en busca de diferencias o deficiencias en el formato. Los cambios en los formatos han sido utilizados frecuentemente para generar un comportamiento anómalo en la aplicación al intentar abrir un tipo de archivo determinado. A través de estos fallos, pudiera llegar a ejecutarse código sin el control del usuario que ha abierto el fichero.

Según la configuración que se haya implementado, podría impedirse que se abriera un archivo para su edición si el módulo correspondiente ha detectado un formato no válido o alterado expresamente para hacer uso de un fin malicioso.

La característica de Validación de documentos se encuentra de forma predeterminada habilitada en Excel 2016, PowerPoint 2016 y Word 2016.

Nota: Puede consultar cómo planear la configuración de validación de documentos de Office para Office 2016 en la siguiente URL:
https://docs.microsoft.com/es-es/deployoffice/security/prevent-file-format-attacks-by-using-file-validation-in-office

Con el bloqueo de ficheros de Office 2016, se pueden bloquear determinados tipos de archivos para impedir que se abran o se guarden en Excel 2016, PowerPoint 2016 y Word 2016. Para ello, se deben configurar opciones en la directiva de grupo o la Herramienta de personalización de Office (OCT).

La configuración de bloqueo de archivos se usa principalmente para tres acciones:

a) Utilizar un catálogo de formatos limitado para una cierta organización

b) Mitigar los ataques de seguridad de día cero

c) Impedir que una organización abra archivos que se guardaron en formatos anteriores o versiones preliminares de Office y, por tanto, de seguridad inferior.

El bloqueo de archivos fue introducido en la versión MS Office 2007, al abrir o guardar determinados tipos de archivos, si bien ha sufrido cambios para permitir nuevos formatos.

La configuración permite determinar qué puede suceder cuando se abre un tipo de archivo. Por ejemplo, si se realiza la apertura de un determinado tipo de archivo que de forma predeterminada se abrirá en modo de vista protegida, impidiendo, por ejemplo, su edición.

La configuración permite también la posibilidad de habilitar o deshabilitar la configuración de controles ActiveX, así como obtener información sobre aquellos que se están cargando en Word, Access, Excel, PowerPoint, Publisher y Visio.

Hay que tener en cuenta que los controles ActiveX pueden ser empleados por diferentes aplicaciones y que la ejecución de los mismos pudiera tener consecuencias diferentes para cada una de ellas. Los controles ActiveX de confianza, en Office, se cargan en modo seguro con valores persistentes y no se realiza una notificación a los usuarios que los cargan. Se consideran de confianza todos aquellos ActiveX que tengan la firma de un editor de confianza, aquellos en que el documento se abra desde una ubicación de confianza o bien que se haya definido como un documento de confianza.

Los controles ActiveX que no son de confianza se cargan de forma distinta y en base a como estén marcados y en base a la existencia de un proyecto de aplicaciones para Visual Basic (VBA) junto al control ActiveX en el propio archivo. En este último caso, el centro de confianza es más restrictivo ya que podría contener macros.

El módulo de bit de cierre de ActiveX de Office es una característica que aparece en la versión 2007 y que controla la ejecución de determinados controles de ActiveX de forma independiente a lo que se haya configurado en Microsoft Internet Explorer.

El bit de cierre permite marcar ciertas claves del registro como inseguras ayudando a cerrar agujeros de seguridad. Dichos avisos se distribuyen como actualizaciones de Windows a través de Windows Update.

Office proporciona varias opciones de configuración de seguridad que permiten controlar el comportamiento de los controles ActiveX y el modo en que se informa a los usuarios acerca de aquellos que podrían ser no seguros. Al configurar estas opciones, podrá realizar las siguientes tareas:

a) Deshabilitar controles ActiveX.

b) Modificar el modo en que los controles ActiveX se inicializan en función de los parámetros de modo seguro; seguro para inicialización (SFI) y no seguro para inicialización (UFI).

Si desea controlar el comportamiento de Visual Basic para Aplicaciones (VBA) y las macros de VBA, puede cambiar la configuración de VBA y de las macros de VBA de Office 2016 para las aplicaciones siguientes: Access, Excel, PowerPoint, Publisher, Visio, y Word.

La configuración es global para todas las aplicaciones. De forma predeterminada, Microsoft Office 2016 VBA está habilitado y las macros de VBA de confianza se pueden ejecutar. En entornos de alta seguridad, se deberá deshabilitar la ejecución de VBA.

De forma predeterminada, la barra de confianza aparecerá para todas las macros, firmadas o no. Existe la posibilidad de modificar el comportamiento de Office 2016 frente a VBA en las aplicaciones que se inician mediante programación, así como el modo de examinar las macros VBA cifradas.

La configuración de seguridad predeterminada para las macros es diferente en Outlook.

Se pueden establecer niveles de seguridad de macros. Office puede cambiar la configuración de seguridad de las macros para especificar qué macros se ejecutarán, y en qué circunstancias, al abrir un archivo. Por ejemplo, se puede permitir la ejecución de macros si están firmadas digitalmente por un desarrollador de confianza (una persona que escribe código de programación) y que no se abran en los demás casos, que se deshabiliten todas las macros y el usuario no reciba notificación alguna, u otras opciones.

En Office 2016 se puede hacer una comprobación de la integridad de archivos cifrados para impedir que enmascaren código malicioso aprovechando esa característica.

Las características descritas pueden configurarse a través de las directivas de seguridad en equipos de un dominio o con el OCT en equipos independientes, excepto el deshabilitado de VBA que solo es posible con el primero de los métodos

Nota: Puede consultar cómo planear la configuración de seguridad para macros de VBA para Office 2016 en la siguiente URL:
https://docs.microsoft.com/es-es/deployoffice/security/plan-security-settings-for-vba-macros-in-office

8.3 MITIGACIÓN DE VULNERABILIDADES DE SEGURIDAD

En ocasiones, se puede llegar a abrir un fichero sin tener confianza en la procedencia del mismo. Con objeto de mitigar el riesgo, MS Office 2016 contiene el entorno de Vista protegida, pero sin impedir la lectura, aunque limitando casi todas las opciones de edición, incluso la impresión.

Ésta es una característica que se introdujo en Office 2010 y reduce el aprovechamiento al abrir archivos en el contenedor restringido de aplicaciones de espacio aislado "lowbox" de manera que se pueden examinar antes de ser modificados. Cuando un archivo es abierto en Vista protegida, el usuario es avisado en la barra de notificaciones.

El módulo de Vista protegida abre un fichero considerado de no confianza, por su ubicación u origen (Internet, adjunto a un correo, hipervínculo desde Internet Explorer, etc.), en un entorno aislado y controlado.

La ejecución de cualquier acción se produce exclusivamente en el entorno aislado, de tal forma que no afectará en ninguna medida ni a la propia aplicación que lo ha abierto, ni a otra o el propio sistema operativo.

Un archivo se abre en Vista protegida cuando no ha superado las comprobaciones de seguridad al intentar abrirse el fichero. Esto se puede dar porque su origen se establezca como potencialmente peligroso. Por ejemplo, ficheros abiertos directamente desde el navegador de Internet, documentos adjuntos a correos electrónicos o bien abiertos desde ubicaciones consideradas como no seguras.

Cuando se detecta un posible riesgo de seguridad, aparece una barra de mensajes mostrada por el componente de Vista protegida, en color amarillo o rojo según el tipo de notificación.

Si el usuario sabe que el archivo procede de una fuente de confianza, puede salir del modo de Vista protegida. Cuando un fichero se encuentre en este modo de vista protegida, se podrá leer su contenido, pero no el resto de funcionalidades como editar, guarda, imprimir o la ejecución de código anexo al mismo.

Los administradores pueden ampliar la lista de ubicaciones potencialmente no seguras para incluir carpetas adicionales que también consideren no seguras.

8.4 MEJORAR LA EXPERIENCIA DE USUARIO

Con objeto de que el usuario sea consciente del tratamiento de los ficheros en vista protegida o no, se facilitan herramientas como la barra de confianza, o barra de mensajes.

A través de la misma, se proporciona la información relacionada con la seguridad de los ficheros, de tal forma que se notifica cuando un fichero se encuentra, por ejemplo, en modo solo lectura por no haberse superado los chequeos correspondientes.

Si un usuario confía en la procedencia del mismo, puede habilitar su edición a través de dicha barra. En ese caso, Office dejará de comprobar, a futuro, el fichero.

Nota: Se deberá tener mucha precaución cuando se salga de Vista protegida y asegurar que el origen es de confianza. También es posible que el administrador haya bloqueado esta acción y no sea posible abandonar la "Vista protegida".

Una vez deshabilitada la Vista protegida, el documento pasa a ser de confianza y supera los controles, automáticamente, la siguiente vez que este sea abierto.

9. PLANIFICACIÓN DE LA SEGURIDAD EN MS OFFICE 2016

La seguridad en el tratamiento de ficheros e información que se ofrece en Office 2016 se debe evaluar desde la planificación. Esta planificación no debe estar enfrentada con la propia productividad que se demanda de las aplicaciones, pero debe ser una consecuencia de la misma.

Planificar la seguridad consiste en definir los modelos, mecanismos y medios que garantizarán un uso seguro de las aplicaciones y del tratamiento de los datos. La seguridad se aplicará a través de directivas de seguridad o por medio del OCT, pero para ello previamente deben ser comprendidas y en qué medida serán aplicadas.

Hay que ser conscientes del hecho de que determinadas medidas serán de aplicación general, otras dependerán de la propia aplicación y otras de los propios usuarios que manejan determinados ficheros. Por ejemplo, la configuración de ubicaciones de confianza mantendrá una configuración general para todos los usuarios, sin embargo, la definición de zonas, como la dirección URL del servidor MS SharePoint que pudiera existir en la organización, es una configuración que deberá definirse de forma específica a través de las directivas de seguridad.

9.1 CONFIGURACIÓN DE SEGURIDAD DE UBICACIONES DE CONFIANZA

MS Office 2016 permite diferenciar aquellos archivos que son seguros de los que potencialmente pueden ser peligrosos según su procedencia. Para ello, se hace uso del mecanismo de configuración que permite declarar ubicaciones de confianza para evitar que sean comprobados por el Centro de confianza o que sean abiertos en la Vista protegida.

Esta designación de fuentes de confianza puede especificarse tanto a recursos locales como a recursos accesibles a través de la red. Asignando un origen de confianza todo el contenido del fichero será habilitado y se encontrará activo para su uso, no siendo notificado ningún riesgo posible que pudiera contener el archivo y permitiendo las funcionalidades de edición.

Para el uso de ubicaciones de confianza, MS Office 2016 proporciona una serie de acciones de configuración. Éstas permiten:

a) Deshabilitar el sistema de ubicaciones de confianza.

b) Impedir que los usuarios designen ubicaciones de confianza.

c) Establecer las ubicaciones de confianza globales, o bien aquellas específicas para cada aplicación.

d) Configurar la existencia de ubicaciones de confianza en recursos accesibles a través de la red.

De los productos existentes en MS Office 2016, esta característica se encuentra disponible para: MS Word, MS Excel, MS PowerPoint, MS Access y MS Visio.

Si se piensa que el contenido activo de un archivo procede de un origen confiable, es más recomendable mover el documento a una ubicación de confianza, en lugar de cambiar la configuración predeterminada del Centro de confianza a configuración de seguridad de macros menos segura.

Se define, a continuación, la configuración predeterminada para la característica de ubicaciones de confianza:

a) La característica se encuentra habilitada y para cada una de las rutas locales predeterminadas de cada aplicación según la instalación predeterminada.

b) Los usuarios pueden agregar carpetas locales a la lista de ubicaciones de confianza.

c) Los usuarios no pueden designar recursos de red como ubicaciones de confianza, pero esta opción puede ser modificada a través del Centro de confianza.

d) Se combinan las ubicaciones definidas tanto por el usuario como las asignadas a través de la directiva.

9.1.1 UBICACIONES DE CONFIANZA DE MS WORD 2016

Ubicaciones de confianza predeterminadas	Descripción de la carpeta	Subcarpetas de confianza
..\Program Files\Microsoft Office 16\Root\ Templates\	Plantillas de aplicación	Permitido
..\Users\nombre_del_usuario\AppData\Roaming\Microsoft\ Templates\	Plantillas de usuario	No permitido
..\Users\nombre_del_usuario\AppData\Roaming\Microsoft\ Word\Startup\	Inicio de usuario	No permitido

Nota: Las ubicaciones indicadas son para una instalación de Office sobre Windows 10, según las guías CCN-STIC-599A18 y CCN-STIC-599B18, en base a una instalación por defecto. En instalaciones personalizadas pueden variar.

9.1.2 UBICACIONES DE CONFIANZA DE MS EXCEL 2016

Ubicaciones de confianza predeterminadas	Descripción de la carpeta	Subcarpetas de confianza
..\Program Files\Microsoft Office 16\Root\ Templates\	Plantillas de aplicación	Permitido
..\Users\nombre_del_usuario\AppData\Roaming\Microsoft \Templates\	Plantillas de usuario	No permitido
..\Program Files\Microsoft Office 16\Root\ Office16\ XLSTART\	Inicio de Excel	Permitido
..\Users\nombre_del_usuario\AppData\Roaming\Microsoft \Excel\XLSTART\	Inicio de usuario	No permitido
..\Program Files\Microsoft Office 16\Root\ Office16\STARTUP\	Inicio de Office	Permitido
..\Program Files\Microsoft Office 16\Root\ Office16\Library\	Complementos	Permitido

Nota: Las ubicaciones indicadas son para una instalación de Office sobre Windows 10, según las guías CCN-STIC-599A18 y CCN-STIC-599B18, en base a una instalación por defecto. En instalaciones personalizadas pueden variar.

9.1.3 UBICACIONES DE CONFIANZA DE MS POWERPOINT 2016

Ubicaciones de confianza predeterminadas	Descripción de la carpeta	Subcarpetas de confianza
..\Program Files\Microsoft Office 16\Root\Templates\	Plantillas de aplicación	Permitido
..\Users\nombre_del_usuario\AppData\Roaming\Microsoft \Templates\	Plantillas de usuario	No permitido
..\Users\nombre_del_usuario\AppData\Roaming\Microsoft \Addins\	Complementos	Permitido
..\Program Files\Microsoft Office 16\Root\Document Themes 16\	Temas de aplicación	Permitido

Nota: Las ubicaciones indicadas son para una instalación de Office sobre Windows, según las guías CCN-STIC-599A18 y CCN-STIC-599B18, en base a una instalación por defecto. En instalaciones personalizadas pueden variar.

9.1.4 UBICACIONES DE CONFIANZA DE MS ACCESS 2016

Ubicaciones de confianza predeterminadas	Descripción de la carpeta	Subcarpetas de confianza
..\Program Files\Microsoft Office 16\Root\Office16\ACCWIZ\	Bases de datos del asistente	No permitido

Nota: Las ubicaciones indicadas son para una instalación de Office sobre Windows, según las guías CCN-STIC-599A18 y CCN-STIC-599B18, en base a una instalación por defecto. En instalaciones personalizadas pueden variar.

9.1.5 IMPLEMENTACIÓN DE UBICACIONES DE CONFIANZA

Las ubicaciones de confianza afectan a todo el contenido de un archivo. Esto incluye los controles ActiveX, los hipervínculos, vínculos a orígenes de datos y las macros de VBA.

La definición de ubicaciones puede establecerse de forma global o específicamente para cada aplicación.

Cada aplicación puede personalizarse de forma independiente, pudiendo deshabilitarse esta característica en una o más de ellas mientras se mantiene en otras.

De forma predeterminada, solo se permiten ubicaciones de confianza en rutas locales existentes en el equipo de los usuarios. Si se desea establecer ubicaciones fuera del equipo deberá habilitarse previamente la opción "Permitir ubicaciones de confianza que estén en la red (no recomendado)".

No deben establecerse como rutas de confianza la raíz del disco duro (por ejemplo C:\) o lugares donde se descarguen de forma predeterminadas ficheros desde Internet tales como repositorios o carpetas existentes en todos los equipos Windows ("Mis Documentos", "Documentos" o "Descargas").

Pueden establecerse carpetas web como ubicaciones de confianza. Por ejemplo, rutas de acceso tipo "http://". Sin embargo, solo se reconocerán como ubicaciones de confianza las carpetas web compatibles con los protocolos: "sistema distribuido de creación y control de versiones Web (WebDAV)" o la llamada a procedimiento remoto de extensiones de servidor de FrontPage (FPRPC)".

Nota: Para comprobar si una carpeta web es compatible con los protocolos WebDAV o FPRPC se deberá comprobar si al abrir un fichero a través de la web, en la lista de archivos de uso recientes del sistema operativo, aparece en la ruta del servidor remoto y no la carpeta de archivos temporales de Internet.

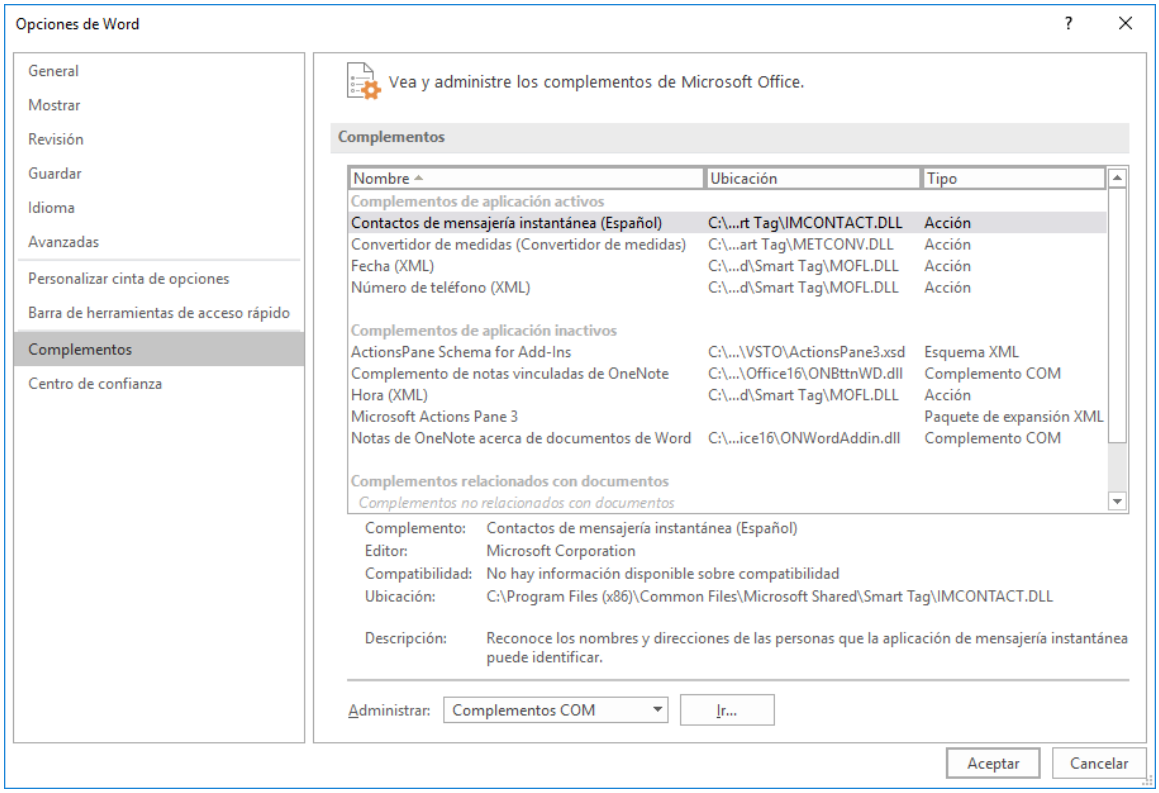
Se puede optar por marcar "Deshabilitar todas las ubicaciones de confianza", lo que permite evitar utilizarlas sin borrar las definiciones existentes. Esta acción puede ayudar a tomas medidas temporales, por ejemplo.

La designación de ubicaciones de confianza puede realizarse a través de la asignación de directivas de seguridad, configuración de usuarios o la herramienta OCT (herramienta de personalización de Office). En la presente guía, se hará uso del mecanismo de directivas de seguridad a través de la aplicación de objetos de políticas de grupo.

Nota: Los mecanismos de asignación de ubicaciones de confianza definidos a través de la presente guía utilizarán la metodología de empleo de directivas de seguridad. Éstas serán de aplicación a través de objetos de directivas de grupo en dominio o localmente a través de las políticas locales en función del tipo de escenario en el que se encuentre el puesto cliente Windows.

9.2 CONFIGURACIÓN DE SEGURIDAD PARA COMPLEMENTOS PARA MICROSOFT OFFICE 2016

Los complementos son funcionalidades instaladas que agregan comandos personalizados y nuevas funciones a los programas de MS Office 2016 pueden ser utilizados para trabajar con nuevas funcionalidades o mejorar la productividad.



Ventana de configuración en la opción "Complementos" de Microsoft Word 2016.

De forma predeterminada con el proceso de instalación de MS Office 2016 se instalan una serie de complementos. No obstante, éstos se ejecutan sin ninguna notificación de seguridad puesto que son considerados, por defecto, como seguros.

Sin embargo, nuevos complementos podrían ser aprovechados por intrusos para causar daños malintencionados, robar información o modificar el comportamiento de un sistema. Para ello, el control de complementos notificará, mediante una advertencia de seguridad, la desactivación de parte del contenido por detección de un complemento inseguro que no cumple con los criterios establecidos.

Los complementos pueden ser deshabilitados en función de la aplicación, bien requerir que los complementos estén firmados por un editor de confianza o bien ser deshabilitadas las notificaciones para los complementos sin firmar. MS Office 2016 proporciona una configuración que permite deshabilitar los complementos. Si ésta se activa puede suponer un problema a usuarios que trabajan con complementos.

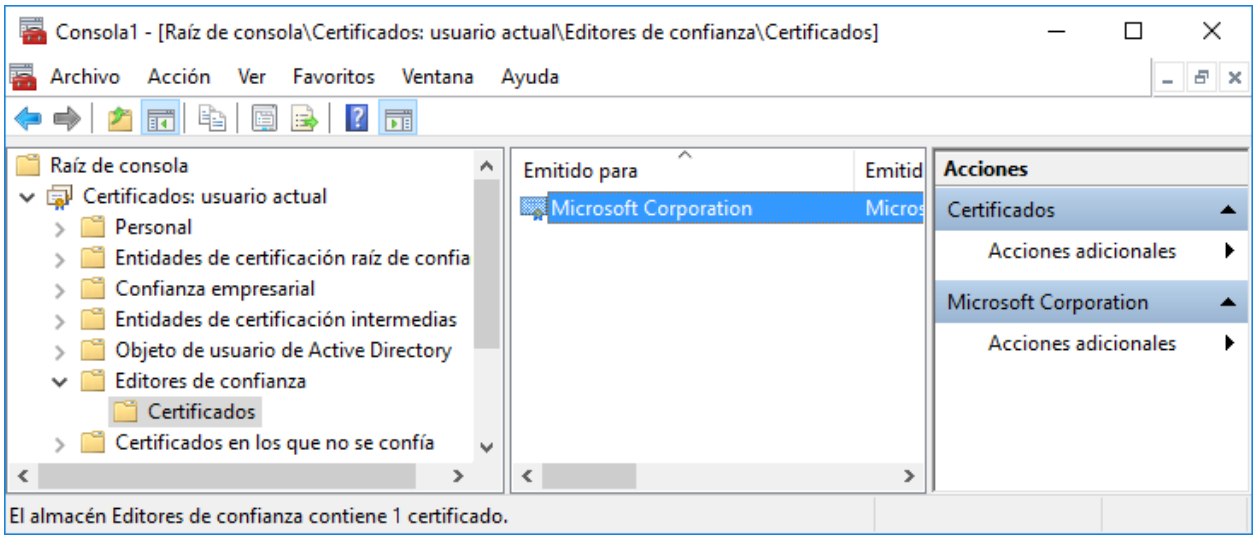
Existe la posibilidad de requerir que los complementos de la aplicación estén firmados por un editor de confianza. Un editor es alguien que ha creado un proyecto de código que podrá tener diferentes objetivos. Los editores de confianza son programadores que cumplen simultáneamente los siguientes criterios:

a) El proyecto está firmado por el programador con una firma digital.

b) La firma digital es válida, no encontrándose caducada.

c) El certificado asociado a la firma digital ha sido emitido por una Entidad Certificadora en la que se confía;

d) Se ha agregado la firma digital como editor de confianza.



Consola MMC con el complemento Certificados mostrando el repositorio de Editores de confianza.

Los certificados de editores de confianza se alojarán en el repositorio de Internet Explorer, común a todas las aplicaciones del sistema operativo.

Si se intenta ejecutar un código que no cumpla los anteriores criterios, se deshabilitará y aparecerá un mensaje indicando que el editor puede no ser seguro.

Las notificaciones para los complementos sin firmar pueden ser deshabilitados para que los usuarios no vean la advertencia en la barra de mensajes si un complemento no ha superado las verificaciones correspondientes. Esto impedirá al usuario generar la excepción, quedando bloqueada la ejecución de complementos. Esta opción, habitualmente, es habilitada en organizaciones que tienen un entorno de seguridad altamente restrictivo. Esta configuración de seguridad está presente en todas las aplicaciones del paquete ofimático MS Office 2016.

9.3 CONFIGURACIÓN DE SEGURIDAD DE CONTROLES ACTIVEX PARA MICROSOFT OFFICE 2016

MS Office 2016 ofrece varias opciones de configuración de seguridad para controlar el comportamiento de los controles ActiveX y la manera en la que los usuarios son informados de aquellos que podrían ser potencialmente peligrosos.

Los controles ActiveX pueden ser deshabilitados o bien puede modificarse el modo en el que estos se inicializan en función de:

a) Los parámetros de modo seguro, seguro para inicialización (SFI, por Safe for Initialization).

b) Los parámetros de modo no seguro para inicialización (UFI, por Unsafe for Initialization).

Los programadores pueden controlar el modo de inicialización al crear los controles ActiveX. De esta manera, el control se puede inicializar de dos formas: en modo seguro y en modo no seguro:

a) En el modo seguro se aplican determinadas restricciones al control que limitan su funcionalidad.

b) En modo no seguro no se aplican restricciones de seguridad.

Por ejemplo, un ActiveX que tiene como funcionalidad leer y escribir archivos, si se inicia en modo seguro solo podría leer archivos, sin embargo, si se inicializa en modo no seguro podría tanto leer como escribir. Los controles ActiveX que son SFI son los únicos que se pueden iniciar en modo seguro, mientras que los UFI siempre se inician en modo no seguro.

De forma predeterminada, los controles ActiveX de confianza se cargan en modo seguro (Safe for Initialization) con valores persistentes y no se notifica a los usuarios que los cargan. Un control ActiveX de confianza es aquel que cuenta con la firma de un editor de confianza o se encuentra incluido en un fichero abierto desde una ubicación de confianza o un documento de confianza. Los controles que no son de confianza se cargan en función de cómo se encuentren marcados y de si existe también en el documento un proyecto de VBA. El comportamiento predeterminado es el siguiente:

a) Si un control ActiveX está marcado como seguro para inicialización (SFI) y está en un documento que no contiene un proyecto de VBA, se carga en modo seguro con valores persistentes. No aparecerá la barra de mensajes y no se notificará a los usuarios la presencia del control ActiveX. Para que este comportamiento se produzca todos los controles del documento deberán estar marcados como SFI.

b) Si un control ActiveX está marcado como no seguro para inicialización (UFI) y está incluido en un documento sin proyecto VBA, se notificará a los usuarios, en la barra de mensajes, la existencia de los controles ActiveX pero que estos se encuentran deshabilitados. El usuario podrá habilitarlos a través de la barra de mensajes, cargándose en modo seguro con valores persistentes.

c) Si un control ActiveX, marcado como UFI o SFI, está incluido en un fichero que presenta un proyecto de VBA, se notificará a los usuarios en la barra de mensajes la existencia de los controles ActiveX pero que éstos se encuentran deshabilitados. El usuario podrá habilitarlos a través de la barra, cargándose en modo seguro con valores persistentes.

d) Si se ha configurado el bit de cierre en el Registro para un control ActiveX, el control no se cargará, no pudiendo habilitarse y no produciéndose tampoco la notificación a través de la barra de mensajes.

El Panel de telemetría de Office 2016 permite observar datos de control de uso de ActiveX. Esta opción puede ser activada desde el menú de inicio de Windows en la carpeta **"Herramientas de Microsoft Office 2016 → Panel de telemetría para Office 2016"**. El panel de telemetría y su registro operan desde la aplicación Excel de la propia suite.

Nota: El Panel de telemetría es un marco de supervisión de compatibilidad que ayuda a identificar las soluciones y los documentos de Office más importantes para una organización con el objetivo de acelerar las implementaciones de Office. Aunque esta herramienta no es objeto de estudio en esta guía, puede obtener más información en la web:
https://docs.microsoft.com/es-es/deployoffice/compat/deploy-telemetry-dashboard

9.4 CONFIGURACIÓN DE SEGURIDAD DE OBJETOS COM PARA OFFICE 2016

Los objetos COM (Component Object Model) fueron introducidos en la década de 1990 por Microsoft para permitir la comunicación entre procesos y para la creación dinámica de objetos. Implementados, a través de diferentes interfaces, representan objetos neutrales independientes del lenguaje en el que se han desarrollado. Por ejemplo, un tipo de objeto COM lo representa una tabla de Excel incrustada en un fichero de MS Word. Los objetos COM integrados en Office pueden incluir objetos ActiveX, vinculación en incrustación de objetos (OLE, por Object Linking and Embedding), servidores RealTimeData (RTD) de Excel y proveedores de orígenes de datos de Office Web Components (OWC).

En la configuración de seguridad de MS Office 2016, éste comprobará en primera instancia si hay alguna opción de configuración de la directiva de grupo establecida para la categorización de objetos COM. Si alguna opción está habilitada, se comprobará si los objetos analizados están correctamente categorizados dentro del registro. Si no fuera así, el objeto no será cargado.

Para habilitar la categorización de un objeto COM, primero se deberá determinar la configuración de seguridad de la directiva de grupo y a continuación agregar el identificador de categoría correspondiente a los objetos COM de destino dentro del registro.

Para la configuración de seguridad de la directiva de grupo en la categorización de objetos COM existen cuatro opciones:

a) Comprobar proveedores de orígenes de datos de OWC.

b) Comprobar servidores RTD de Excel.

c) Comprobar objetos OLE.

d) Comprobar objetos ActiveX.

9.4.1 COMPROBAR PROVEEDORES DE ORÍGENES DE DATOS DE OWC

El componente de orígenes de datos OWC (Office Web Components) es un conjunto de controles COM utilizado para la publicación de hojas de cálculo, gráfico y bases de datos, habilitando la visualización de los componentes a través de un navegador web y permitiendo la publicación interactiva de datos como parte de una página web. Microsoft proporciona una herramienta que permite ver los controles publicados a través de un navegador web.

La configuración de seguridad para los orígenes de datos de OWC tiene dos posibles valores: habilitada o deshabilitada. Cuando la opción es habilitada, MS Office 2016 solo cargará los objetos COM que están correctamente categorizados.

9.4.2 COMPROBAR SERVIDORES RTD DE EXCEL

MS Excel 2016 proporciona una función de hoja de cálculo, la función RDT (RealTimeData), que permite la llamada a un servidor de Automatización del modelo de objetos componentes, COM, con el fin de recuperar datos en tiempo real. La función RDTR recupera datos de un servidor RTD para ser utilizados en los libros Excel. El resultado de dicha función se actualiza cada vez que hay nuevos datos disponibles en el servidor y el libro puede aceptarlos. El servidor espera a que Excel esté inactivo para realizar la actualización.

La configuración de seguridad para la comprobación de servidores RTD de Excel tiene dos posibles valores: habilitada o deshabilitada. Cuando la opción está habilitada Office 2016 solo cargará los objetos COM que estén correctamente categorizados.

9.4.3 COMPROBAR OBJETOS OLE

La incrustación y enlazado de objetos (OLE) es un mecanismo empleado para que el contenido generado en una aplicación pueda estar disponible en otro programa, por ejemplo, insertar un diagrama de Visio en un documento de Word, manteniendo sus características.

La copia de la información puede realizarse como objeto vinculado u objeto incrustado. La diferencia principal entre uno y otro reside en dónde se almacenan los datos y cómo se actualiza el objeto una vez que se ha colocado en el archivo destino. Por ejemplo, en el caso de Excel un objeto incrustado se almacena en el libro en el que se ha insertado y no se actualiza. Sin embargo, si el objeto fuera vinculado permanecería como archivo independiente y podría actualizarse.

La configuración de seguridad de MS Office 2016 permite tres opciones:

a) No comprobar: MS Office carga los objetos OLE sin realizar ninguna comprobación de si están correctamente categorizados.

b) Invalidar lista de bits de cierre de Internet Explorer: Es el comportamiento predeterminado y para ello Office usa la lista de categorías para invalidar las comprobaciones de bits de cierre de Internet Explorer. Este uso implica que el objeto COM no categorizado como seguro podría cargarse en Internet Explorer, pero no en las aplicaciones de Office.

c) Lista de permitidos estricta: Office solo carga los objetos OLE categorizados correctamente.

9.4.4 COMPROBAR OBJETOS ACTIVEX

Adicionalmente a las comprobaciones de seguridad de los objetos ActiveX definidos anteriormente, pueden ser cargados como componentes COM.

La configuración de seguridad de MS Office 2016 permite tres opciones para la comprobación de objetos ActiveX:

a) No comprobar: MS Office 2016 carga los objetos ActiveX sin realizar ninguna comprobación en cuanto a la categoría correcta.

b) Invalidar lista de bits de cierre de Internet Explorer: Es el comportamiento predeterminado y para ello MS Office usa la lista de categoría para invalidar las comprobaciones de bits de cierre de Internet Explorer. Este uso implica que el objeto ActiveX no categorizado como seguro podría cargarse en Internet Explorer, pero no en las aplicaciones de MS Office.

c) Lista de permitidos estricta: MS Office solo carga los objetos ActiveX categorizados correctamente.

9.5 CONFIGURACIÓN DE SEGURIDAD DEL MODO VISTA PROTEGIDA DE MICROSOFT OFFICE 2016

La vista protegida ayuda a salvaguardar contra diferentes tipos de vulnerabilidades cuando se procede a abrir documentos, presentaciones o libros, haciéndolo en un entorno de espacio aislado. Este espacio aislado es la parte de la memoria de un sistema o un proceso que se encuentra aislado, por seguridad, de ciertos componentes del sistema operativo y el resto de las aplicaciones.

Este entorno protegido aísla los programas y componentes del resto del sistema, por ser considerados como potencialmente peligrosos. Este aislamiento minimiza el riesgo de sus acciones evitando potenciales ataques o la desestabilización del propio sistema.

En modo vista protegida, no se tendrá acceso a los detalles de las firmas digitales que pudieran haberse empleado para firmar un documento, presentación o libro.

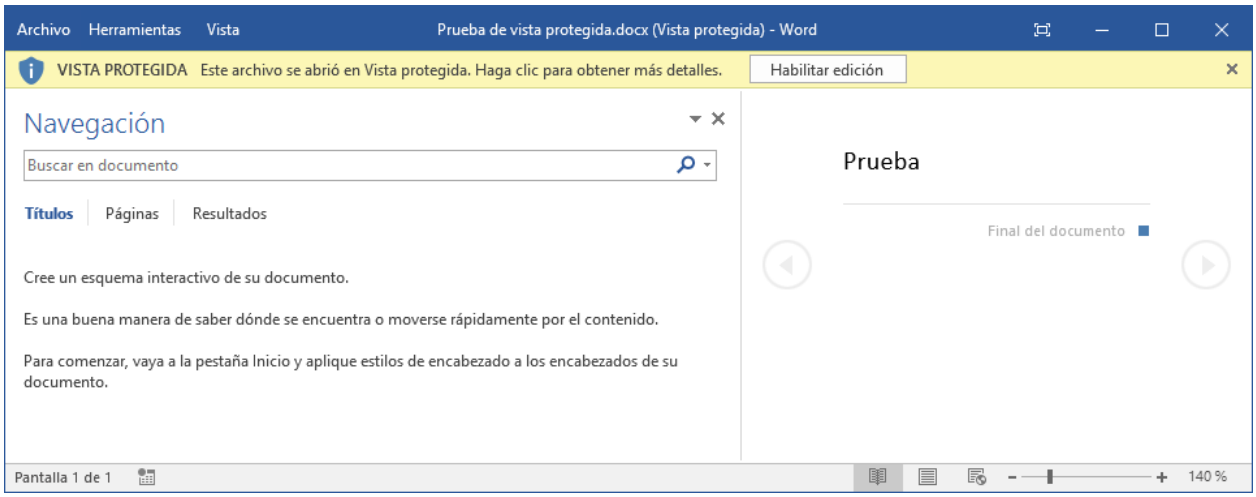
De forma predeterminada, la vista protegida se encuentra habilitada para MS Word 2016, MS Excel 2016 y MS PowerPoint 2016, pero solo para determinados tipos de archivos. Por ejemplo, los ficheros que se abren desde las ubicaciones de confianza o archivos definidos de confianza no se abren en el modo vista protegida. Los archivos se abrirán en modo vista protegida si se cumple una de las siguientes condiciones:

a) Si un archivo omite o no pasa la validación de documentos de Office. Esta característica de seguridad examina archivos con objeto de determinar si existen vulnerabilidades en el formato de archivo. Si se identifica una posible vulnerabilidad falla la comprobación y el fichero se abrirá en vista protegida.

b) Si la información de zona de AES determina que un archivo no es seguro. El servicio de ejecución de datos adjuntos (AES, por Attachment Execution Service) agrega información de zona a los archivos que se descargan con Microsoft Outlook o Microsoft Internet Explorer. Si la información de zona de un archivo indica que este procede de un sitio web que no es de confianza o bien es de la zona de Internet, el archivo descargado se abrirá en la vista protegida.

c) Un usuario abre un fichero en modo vista protegida. Los usuarios pueden abrir archivos directamente en modo vista protegida a través del menú de diálogo “Abrir en Vista protegida” cuando se selecciona un fichero manteniendo pulsado la tecla “Mayúscula”.

d) Un archivo se abre desde una ubicación no segura. De forma predeterminada se consideran ubicaciones no seguras las carpetas de archivos temporales de Internet y la carpeta de programas descargados. Podrán seleccionarse otras zonas no seguras haciendo uso de las directivas de grupo.



Fichero de Word 2016 abierto con Vista Protegida. En la barra de mensaje aparece el indicador de Vista protegida avisando del peligro y de la recomendación de mantenerla si no es indispensable desactivar este modo.

Se puede cambiar el comportamiento del modo vista protegida para adaptarse a requisitos de seguridad especiales. Las opciones que pueden aplicarse son:

a) Impedir que los archivos descargados de Internet se abran en la Vista protegida: Esta configuración fuerza a los archivos a omitir la Vista protegida si la información de zona de AES indica que el archivo se descargó de la zona Internet con el navegador Internet Explorer.

b) Impedir que los archivos almacenados en ubicaciones no seguras se abran en la Vista Protegida: Esta opción omite la lista de ubicaciones no seguras, permitiendo la apertura normal de ficheros, aunque se encontraran en dichas ubicaciones.

c) Impedir que los datos adjuntos de Microsoft Outlook 2016 se abran en la vista protegida: Esta configuración fuerza a los archivos a omitir la Vista protegida si la información de zona de AES indica que archivos de MS Word 2016, MS Excel 2016 o MS PowerPoint 2016 se abren desde MS Outlook 2016.

Nota: No deberá cambiarse el comportamiento de las tres primeras opciones de seguridad, puesto que altera significativamente la estrategia de protección por niveles planteada en MS Office 2016. Solo deberán modificarse si se plantean soluciones de protección alternativas por parte de la organización y por necesidad de requisitos de seguridad especiales.

Las características de bloqueo de archivo y validación de documentos que incorpora MS Office 2016 presentan opciones de configuración que permiten forzar la apertura de archivos en la Vista protegida si se cumplen determinadas condiciones:

a) Usar bloqueo de archivos para forzar la apertura de archivos en la Vista protegida: La característica de bloqueo de archivos impide que se pueda abrir o guardar cierto tipo de archivos. Cuando esta configuración se encuentra activa, se pueden elegir tres acciones de bloqueo de archivo:
   i. Bloqueado y no habilitado para editar: Los archivos se abren en modo normal pero no pueden editarse.
   ii. Bloqueado y abierto solo en la Vista protegida: Este modo evita que los usuarios puedan habilitar la edición.
   iii. Bloqueado y abierto en la Vista protegida: Los usuarios pueden habilitar la edición.
b) Usar la configuración de Validación de archivos de Office para forzar la apertura de archivos en la Vista protegida. Esta característica de seguridad analiza los ficheros para determinar si existe una vulnerabilidad de formato. Existen tres opciones posibles para los archivos que no pasan la validación de archivo de MS Office:
   i. Bloquear completamente: Los archivos que no pasan la Validación de archivos de MS Office no se pueden abrir en Vista protegida ni se pueden editar.
   ii. Abrir en Vista protegida y deshabilitar la edición: Los archivos que no pasan la Validación de archivos de MS Office se abren en la Vista protegida, pero los usuarios no pueden editarlos.
   iii. Abrir en Vista protegida y permitir la edición: Los archivos que no pasan el control de Validación de archivos de MS Office se abren en el modo de Vista protegida y los usuarios pueden habilitar su edición. Este es el modo predeterminados de MS Office 2016.

Los anteriores mecanismos de validación se encuentran disponibles solo para MS Word 2016, MS Excel 2016 y MS PowerPoint 2016. Se puede establecer una configuración diferente para cada una de las aplicaciones.

9.6 CONFIGURACIÓN DE LA VALIDACIÓN DE DOCUMENTOS DE OFFICE 2016

La Validación de documentos de MS Office 2016 ayuda a detectar y prevenir un tipo de vulnerabilidad conocido como ataque de formato de archivo o ataque de pruebas de exploración de vulnerabilidades mediante datos aleatorios en archivos. El ataque aprovecha la integridad de un archivo para elevar el privilegio de cuentas que tienen restricciones en el equipo.

Este sistema de seguridad compara la estructura de un archivo con un esquema de archivo predefinido a través de un conjunto de reglas que determinan la apariencia de un archivo legible. Si se detecta que la estructura de un archivo no sigue todas las reglas descritas en el esquema, el archivo no supera el proceso de validación.

El sistema de validación de documentos examina y valida los siguientes tipos de archivos:

a) Archivos de libro de Excel 97-2003. Estos archivos tienen una extensión .xls e incluyen todos los archivos con Formato de archivo de intercambio binario 8 (BIFF8).

b) Archivos de plantilla de Excel 97-2003. Estos archivos tienen una extensión ".xlt" e incluyen todos los archivos BIFF8.

c) Archivos de Microsoft Excel 5.0/95. Estos archivos tienen una extensión ".xls" e incluyen todos los archivos BIFF5.

d) Archivos de presentación de PowerPoint 97-2003. Estos archivos tienen una extensión de tipo ".ppt".

e) Archivos de presentación con diapositivas de PowerPoint 97-2003. Estos archivos tienen una extensión ".pps".

f) Archivos de plantilla de PowerPoint 97-2003. Estos archivos tienen una extensión ".pot".

g) Archivos de documento de Word 97-2003. Estos archivos tienen una extensión ".doc."

h) Archivos de plantilla de Word 97-2003. Estos archivos tienen una extensión ".dot"

El comportamiento de las características de Validación de documento de Office puede modificarse haciendo uso de varias opciones de configuración:

i) Deshabilitar el componente de Validación de documento de Office.

j) Especificar el comportamiento del documento cuando un archivo no pasa la validación.

k) Impedir que Office 2016 envíe información sobre Validación de documento de Office a Microsoft.

De forma predeterminada, esta característica se encuentra habilitada en Excel 2016, PowerPoint 2016 y Word 2016. Si un fichero no supera el control, se abren en el modo Vista protegida, pudiendo los usuarios habilitar su edición.

En entornos restringidos, se puede cambiar el comportamiento de los documentos cuando se producen errores de validación. Para ello, puede seleccionarse una de las tres opciones siguientes:

a) Bloquear archivos completamente. Los archivos con errores de validación no se abren.

b) Abrir archivos en vista protegida y deshabilitar la edición. Los archivos se abren en la Vista protegida. Los usuarios pueden ver el contenido, pero no editarlos.

c) Abrir archivos en vista protegida y permitir la edición. Los archivos se abren en la Vista protegida y los usuarios pueden activar la opción de editarlos. Esta es la opción predeterminada.

Se recomienda no cambiar la configuración predeterminada de la Validación de documento de Office a no ser que se encuentre en uno de los siguientes supuestos:

a) **Organizaciones que restringen el acceso a Internet:** Se debería impedir que la Validación de documento de Office envíe la información a Microsoft.

b) **Organizaciones que tienen entornos de seguridad altamente restrictivos:** Se puede configurar la Validación de documento de Office de modo que los archivos que no aprueben la validación no se puedan abrir o solo se puedan abrir en vista protegida. Esta configuración es más restrictiva que la predeterminada.

c) **Organizaciones que no desean enviar sus archivos a Microsoft:** Si el usuario lo permite, la Validación de documento de Office envía a Microsoft una copia de todos los archivos que no aprueban la validación. Puede configurar la Validación de documento de Office para que no se les solicite a los usuarios enviar información de validación a Microsoft.

9.7 OPCIONES DE PRIVACIDAD PARA OFFICE 2016

La experiencia **Bienvenido a Office** se ejecutará la primera vez que un usuario accede a Office, a no ser que el administrador elimine esta opción.

Debido a que la experiencia Bienvenido a Office permite que los usuarios habiliten o deshabiliten varios servicios basados en Internet, puede que se desee evitar que el cuadro de diálogo aparezca y, en su lugar, configurar estos servicios por otros medios, por ejemplo, de las directivas de grupo de dominio o locales.

MS Office proporciona varias configuraciones que permiten controlar la divulgación de información sensible de los ficheros. Estas configuraciones pueden habilitarse o deshabilitarse en función de las condiciones de seguridad de la organización (en entornos con demanda de alta seguridad se debería deshabilitar cualquier opción de conectar con el exterior desde Office, y especialmente aquellas que permiten la salida de cualquier tipo de información):

a) Opciones de contenido en línea.

b) Recibir automáticamente pequeñas actualizaciones para mejorar la confiabilidad.

c) Habilitar el programa para la mejora de la experiencia del usuario.

d) Mejorar la herramienta de corrección.

e) Otras opciones de privacidad.

9.7.1 OPCIONES DE CONTENIDO EN LÍNEA

La regla **Opciones de contenido en línea** controla si el sistema de Office 2016 puede descargarse contenido de Office.com como, por ejemplo, para la ayuda. Puede seleccionarse una de las opciones siguientes:

a) No permitir que Office se conecte a Internet: las aplicaciones de Office no se conectarán a Internet para tener acceso a los servicios en línea o para descargar el contenido más reciente de Office.com. Las características de Office 2016 con conexión se mostrarán deshabilitadas.

b) Permitir que Office se conecte a Internet: las aplicaciones de Office usan los servicios en línea y descargan el contenido en línea más reciente de Office.com cuando los PC de los usuarios se conectan a Internet. Las características de Office 2016 con conexión se mostrarán habilitadas. Esta opción aplica la configuración predeterminada. Si se habilita esta configuración y se hace uso de la opción no mostrar nunca el contenido de conexión o los puntos de entrada o bien buscar solamente contenido sin conexión cuando esté disponible, los usuarios no podrán acceder a temas de la Ayuda actualizados ni las plantillas existentes en Office.com.

En entornos de alta seguridad se debería deshabilitar esta opción o al menos se debe evaluar la posibilidad.

9.7.2 RECIBIR AUTOMÁTICAMENTE PEQUEÑAS ACTUALIZACIONES PARA MEJORAR LA CONFIABILIDAD

La configuración para recibir pequeñas actualizaciones para mejorar la confiabilidad controla si los equipos clientes descargan periódicamente pequeños archivos que permiten que Microsoft diagnostique problemas del sistema.

Si está habilitada esta opción de configuración, Microsoft recopila información sobre errores específicos y la dirección IP del equipo.

Ninguna información personal, a excepción de la dirección IP, es remitida a Microsoft.

De forma predeterminada, las aplicaciones pueden descargar regularmente pequeños archivos del tipo descrito.

En entornos de alta seguridad, se debería deshabilitar esta opción o, al menos, se debe evaluar la posibilidad.

9.7.3 HABILITAR EL PROGRAMA PARA LA MEJORA DE LA EXPERIENCIA DEL USUARIO DE OFFICE

Esta configuración controla si los usuarios participan en el Programa para la mejora de la experiencia (CEIP, por *Customer Experience Improvement Program*) del usuario con objeto de ayudar a Microsoft a mejorar la suite MS Office 2016.

Habilitar esta opción implica el envío de información automática a Microsoft de cómo se hace uso de las aplicaciones. La participación en el Programa para la mejora de la experiencia del usuario no recopila nombres, direcciones u otra información que identifique a los usuarios, excepto las direcciones IP del equipo que se usa para enviar los datos.

Durante la instalación se le ofrecerá la posibilidad de adherirse al programa, así como una detallada explicación del mismo.

En entornos de alta seguridad se debería deshabilitar esta opción o al menos se debe evaluar la posibilidad.

9.7.4 MEJORAR LA HERRAMIENTA DE CORRECCIÓN

Esta configuración controla si la característica **Ayudar a mejorar las herramientas de corrección** envían datos de uso a Microsoft. Ésta recoge datos del uso de la herramienta de corrección y adiciones al diccionario. Transcurrido seis meses desde su activación la característica deja de enviar datos a Microsoft y elimina el archivo de recopilación de datos del equipo del usuario.

Si se habilita esta configuración, hay que tener en cuenta que, aunque esta característica no recopila información personal de forma intencionada, puede ser que parte del contenido que se envía incluya elementos marcados como errores gramaticales u ortográficos con información sensible. Todos los números se convierten en ceros al recopilarse los datos.

Si se adhiere a CEIP está configuración quedará habilitada de forma predeterminada.

En entornos de alta seguridad, se debería deshabilitar esta opción o al menos se debe evaluar la posibilidad.

9.7.5 OTRAS OPCIONES DE PRIVACIDAD

Adicionalmente a las opciones de privacidad citadas anteriormente, Office 2016 proporciona otros mecanismos para entornos de seguridad restringidos:

a) Proteger los metadatos del documento para archivos protegidos por contraseña. Esta opción determina si los metadatos se cifran cuando se usa la característica de cifrar con contraseña. En entornos de alta protección, es una opción recomendable para evitar filtrar datos tales como el autor del documento.

b) Proteger metadatos del documento para los archivos Office Open XML con derechos administrados. Esta configuración determina si los metadatos se cifran cuando usa la característica Restringir permisos por personas.

c) Advertir antes de imprimir, guardar o enviar un archivo que contenga marcas de control de cambios o comentarios. Esta configuración determina si los usuarios son advertidos sobre las marcas de revisión o comentarios cuando se realicen acciones sobre el documento: imprimir, guardar o enviar.

d) Mostrar la revisión oculta. Esta configuración determina si el control de cambios será visible cuando se abre el documento.

e) Evitar que se ejecuten los inspectores de documentos. Esta configuración deshabilita los módulos del Inspector de documentos que permite a los usuarios la eliminación de la información confidencial que puede revelar información sensible, por ejemplo, los metadatos, pies de página, encabezados, etc.

En entornos de alta seguridad, se deberían evaluar cada uno de los puntos anteriores con detenimiento.

9.8 CONFIGURACIÓN DE CRIPTOGRAFÍA Y CIFRADO PARA OFFICE 2016

MS Office 2016 contiene opciones de configuración para establecer la forma en la que se cifran y protegen los ficheros a utilizar en las aplicaciones MS Word, MS Excel, MS PowerPoint, MS Access, MS OneNote y MS Project.

Los algoritmos de cifrado disponibles en MS Office 2016 dependen de los algoritmos a los se pueda tener acceso a través de las interfaces de programación de aplicaciones (API, por *Application Programming Interface*) del propio sistema operativo. Además de mantener la compatibilidad con la API de criptografía (CryptoAPI), MS Office 2016 es compatible con CNG (CryptoAPI Next Generation), disponible desde el lanzamiento de Microsoft Office System 2007 con Service Pack 2.

El sistema CNG agiliza el cifrado permitiendo especificar diversos algoritmos de hash y cifrado que estén disponibles en el sistema operativo para proteger los documentos.

CNG permite utilizar módulos de cifrado de terceros.

Si se utiliza CrytoAPI, los algoritmos de cifrado dependen de los que se encuentren disponibles en un proveedor de servicios de cifrado (CSP, por *Cryptographic Service Provider*) que forma parte del sistema operativo. Puede ver la lista en la siguiente clave de registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Defaults/Provider

Por defecto, los siguientes algoritmos de cifrado CNG se pueden utilizar con Office 2016:

a) AES
b) DES
c) DESX
d) 3DES
e) 3DES_112
f) RC2

Con MS Office 2016, se puede utilizar cualquier extensión de cifrado CNG instalada en el sistema o los siguientes algoritmos de hash que se encuentran incluidos en el mismo:

a) SHA512
b) SHA384
c) SHA256
d) SHA-1
e) RIPEMD-160
f) RIPEMD-128
g) MD5
h) MD4
i) MD2

De forma predeterminada, cuando se cifran ficheros con formato Office Open XML (por ejemplo, .docx o .xslx), los valores predeterminados son AES, con longitud de clave de 128 bits, SHA1 y CBC (Encadenamiento de bloques de cifrado, en inglés *cipher-block chaining*).

El cifrado AES proporciona una protección suficientemente fuerte para la mayor parte de organismos. Por ejemplo, AES de 256 bits podría utilizarse para un nivel de alto secreto.

En la tabla siguiente, se enumeran las opciones de configuración de algoritmos de cifrado que se pueden usar con las versiones de Office con acceso a CryptoAPI, como Office 2016:

Configuración	Descripción
Tipo de cifrado para archivos Office Open XML protegidos con contraseña	Esta configuración le permite especificar el tipo de cifrado para archivos XML abiertos de los proveedores de servicios de criptográficos disponibles (CSP). Esta configuración es obligatoria si usa un complemento de cifrado COM personalizado.
Tipo de cifrado para archivos de Office 97-2003 protegidos con contraseña	Esta configuración le permite especificar un tipo de cifrado para archivos de Office 97-2003 (binarios) de los proveedores de servicios criptográficos disponibles (CSP). El único algoritmo de cifrado admitido con esta configuración es RC4, que no recomienda Microsoft.

Existe la posibilidad de establecer opciones de configuración para cambiar los algoritmos de cifrado cuando se hace uso de MS Office 2016. La siguiente tabla presenta las disponibles:

Opción	Descripción
Establecer algoritmo de cifrado CNG	Esta opción de configuración permite configurar el algoritmo de cifrado CNG que se debe usar. El valor predeterminado es "AES".
Configurar modo de encadenamiento de cifrado CNG	Esta opción de configuración permite configurar el modo de encadenamiento de cifrado que se debe usar. El valor predeterminado es "Encadenamiento de bloques de cifrado (CBC)".
Establecer longitud de la clave de cifrado CNG	Esta opción de configuración permite configurar el número de bits que se deben usar al crear la clave de cifrado. El valor predeterminado es 128 bits.
Especificar compatibilidad de cifrado	Esta opción de configuración permite especificar el formato de compatibilidad. El valor predeterminado es "Usar formato de última generación".
Establecer parámetros para el contexto de CNG	Esta opción de configuración permite especificar los parámetros de cifrado que se deben usar para el contexto de CNG. Para hace uso de esta opción, primero se deberá crear un contexto de CNG mediante CryptoAPI: Next Generation (CNG).
Especificar algoritmo hash CNG	Esta opción de configuración permite especificar el algoritmo hash que se debe usar. El valor predeterminado es "SHA1".
Establecer número de recombinaciones de contraseña de CNG	Esta opción de configuración permite especificar el número de veces que se genera (recombina) el comprobador de contraseñas. El valor predeterminado es 100.000.
Especificar algoritmo de generador de números aleatorios de CNG	Esta opción de configuración permite configurar el generador de números aleatorios de CNG que se va a usar. El valor predeterminado es "RNG (Generador de números aleatorios)".
Especificar longitud de contraseña CNG con sal	Esta opción de configuración permite especificar el número de bytes de sal que se debe usar. El valor predeterminado es 16.

Adicionalmente, para MS Word, MS Excel y MS PowerPoint, existe la posibilidad de forzar el uso de una nueva clave al cambiar la contraseña. La opción predeterminada es **No usar una nueva clave en los cambios de contraseña**.

En el caso de emplear documentos de versiones con formato de Office 97 a 2003 (.doc o .xls, por ejemplo) debe tener en cuenta que el cifrado utilizado usa el algoritmo RC4, muy inseguro comparado con el predeterminado AES para el formato Office Open XML y, por tanto, no recomendado.

Nota: Puesto que el algoritmo RC4 es considerado en la actualidad como inseguro, se desaconseja guardar documentos que vayan a ser cifrados en el formato tipo de las versiones previas (.doc, .xls, .ppt). Se deberán guardar los ficheros con formato Office Open XML para hacer uso de algoritmos de cifrado seguros.

En el caso de que la organización cuente con equipos con versiones anteriores a MS Office 2007, las aplicaciones no podrán abrir los ficheros con formato Office Open XML. Para hacerlo, deberá instalarse el paquete de compatibilidad de Office Open XML:

https://www.microsoft.com/es-es/download/office.aspx

Office 2016 incluye una nueva funcionalidad que permite a los administradores desbloquear archivos de Office protegidos con contraseña; por ejemplo, el propietario del archivo olvida la contraseña o deja la organización. Mediante una nueva herramienta de administración de claves de cifrado, el personal de TI puede asignar fácilmente una nueva contraseña al archivo, o ninguna contraseña, y guardar el archivo en la misma ubicación o en una nueva. Puede descargar la herramienta de administración de claves de cifrado desde el sitio de Microsoft.

9.9 CONFIGURACIÓN DE FIRMA DIGITAL PARA OFFICE 2016

Las firmas digitales ayudan a establecer las siguientes medidas de autenticación:

a) **Autenticidad:** Identifica de forma inequívoca al firmante evitando la suplantación de identidad.

b) **Integridad:** Asegura que el contenido no ha sido alterado desde la firma.

c) **No rechazo:** Un firmante no puede rechazar la firma de un documento sin rechazar su clave digital y, por lo tanto, otros documentos firmados con esa clave.

En MS Office 2016, se pueden firmar digitalmente documentos a través de las aplicaciones MS Word, MS Excel y MS PowerPoint. También puede establecerse una línea de firma o una marca de firma con MS Word, MS Excel y MS InfoPath. MS Office 2016 es compatible con XAdES, firma electrónica avanzada con un conjunto de extensiones para el estándar XML-DSig.

Si no se crea una línea de firma o una marca de firma, el documento quedará firmado digitalmente de forma "invisible".

Los documentos de Office 2016 con firma XAdES permiten a los suscriptores agregar sus direcciones y sus cargos y describir la intención de las firmas. Office también evalúa firmas -XL mediante certificados y cualquier dato de revocación que incluya el archivo.

Los usuarios pueden "firmar" digitalmente archivos de Open Document Format (ODF v1.2) aplicando una firma digital invisible. Además, Office comprobará las firmas en archivos ODF que se crearon con otras aplicaciones.

La firma digital se utiliza para autenticar la identidad del creador de un documento mediante el empleo de certificados digitales.

Para que una firma digital pueda ser utilizada en documentos de Office deberán cumplirse los siguientes criterios:

a) La firma digital es válida. Una CA de confianza para el sistema operativo debe firmar el certificado digital en el cual se basa la firma digital.

b) El certificado asociado con la firma digital no caducó o contiene una marca de tiempo que indica que el certificado era válido en el momento de la firma.

c) El certificado asociado con la firma digital no está revocado.

d) La persona u organización que firma (conocida como publicador) es de confianza para el destinatario.

MS Word, MS Excel y MS PowerPoint identifican estos criterios y advierten al usuario si existe un problema con la firma digital.

MS Office 2016 usa el formato XML-DSig y compatibilidad con XAdES. Este es un conjunto de extensiones en niveles XML-DSig, en él cada nivel se basa en el nivel anterior para proporcionar firmas digitales más confiables. Estas firmas no son compatibles con las versiones anteriores a MS Office 2007 de tal forma que, si un documento se abre con una aplicación previa haciendo uso del paquete de compatibilidad instalado, el usuario recibe un mensaje indicando que el documento se firmó con una versión de MS Office más reciente y la firma digital se perderá.

En el caso de compatibilidad con Office 2007, hay que tener presente que, si se hace uso de XAdES para la firma digital, no existirá compatibilidad a menos que la opción de configuración "no incluir objeto de referencia XAdES en el manifiesto" se establezca en deshabilitado.

De forma predeterminada, Office 2016 crea firmas digitales XAdES, independientemente de que se use un certificado con firma personal o un certificado firmado por una entidad de certificación durante la creación de la firma digital.

En la siguiente tabla se enumeran los niveles de firma digital XAdES disponibles en MS Office 2016.

Nivel de firma	Descripción
XAdES-EPES (base)	Agrega información sobre el certificado de firma a la firma XML DSig. Es el valor predeterminado de las firmas de Office 2016.
XAdES-T (marca de tiempo)	Agrega una marca de tiempo a las secciones XML-DSig y XAdES-EPES de la firma, lo que proporciona protección contra la caducidad del certificado.
XAdES-C (completo)	Agrega referencias a la cadena de certificación e información del estado de revocación.
XAdES-X (extendido)	Agrega una marca de tiempo para el elemento XML-DSig SignatureValue y las secciones -T y - C de la firma. La marca de tiempo adicional protege los datos adicionales de rechazo.
XAdES-X-L (periodo de tiempo largo y extendido)	Almacena la información de revocación de certificados y del certificado real además de la firma. Eso permite la validación de certificados incluso si los servidores de certificados ya no están disponibles.

Las firmas digitales con marca de tiempo tienen la capacidad de ampliar la vida útil de una firma digital. Si un certificado ha caducado y este fue utilizado previamente para creación de una firma digital que contiene una marca de tiempo de un servidor de marca de tipo de confianza, la firma digital puede ser considerada válida, aunque el certificado haya caducado. Para usar esta funcionalidad se deber realizar lo siguiente:

a) Configure un servidor de marca de tiempo que cumpla con RFC 3161

b) Use la opción de Directiva de grupo, **Especificar el nombre de servidor **, para especificar la ubicación del servidor de marca de tiempo en la red.

Pueden, también, establecerse parámetros adicionales de marca de tiempo como son la configuración del algoritmo de hash y el tiempo de espera del servidor de marca tiempo. El valor hash predeterminado es SHA1 y el tiempo de espera de MS Office 2016 para que el servidor de marca de tiempo responda a una solicitud es de 5 segundos.

Además de las opciones relacionadas con la marca de tiempo, existen otras opciones de configuración de las directivas de grupo para determinar la forma de configurar y controlar las firmas digitales a nivel corporativo. Estas opciones se enumeran en la siguiente tabla:

Configuración de directiva de grupo	Descripción
Requerir OCSP al generarse las firmas	Esta configuración de directiva permite determinar si Office 2016 requiere datos de revocación de OCSP (Protocolo de estado de certificado en línea) para todos los certificados digitales de una cadena cuando se generan firmas digitales.
Especificar el nivel mínimo de XAdES para la generación de firmas digitales	Esta configuración de directiva permite especificar un nivel mínimo de XAdES que las aplicaciones de Office 2016 deben alcanzar para crear una firma digital XAdES. Si las aplicaciones de Office 2016 son no puede alcanzar el nivel mínimo de XAdES, la aplicación de Office no crea la firma.
Comprobar las partes XAdES de una firma digital	Esta configuración de directiva permite especificar si Office 2016 comprueba las partes XAdES de una firma digital al validar una firma digital para un documento.
No permitir certificados caducados al validar firmas	Esta configuración de directiva permite que configurar si las aplicaciones de Office 2016 aceptan certificados digitales expirados al comprobar las firmas digitales.
No incluir objeto de referencia XAdES en el manifiesto	Esta configuración de directiva permite determinar si un objeto de referencia XAdES aparecerá en el manifiesto. Debe configurar este parámetro en habilitado si desea que el sistema de Office 2007 que puedan leer las firmas de 2016 de Office que contengan contenido XAdES. De lo contrario, el sistema de Office 2007 tendrá en cuenta las firmas que contengan contenido XAdES no válido.
Seleccionar algoritmo hash de firma digital	Esta configuración de directiva permite configurar el algoritmo hash que las aplicaciones de Office 2016 usan para confirmar las firmas digitales.
Establecer nivel de comprobación de firmas	Esta configuración de directiva permite establecer el nivel de comprobación que se usa en las aplicaciones de Office 2016 al validar una firma digital.
Nivel de XAdES requerido para la generación de firmas	Esta opción de directiva permite especificar un nivel de XAdES requerido o deseado en la creación de una firma digital.