

Guía de Seguridad de las TIC CCN-STIC

INSTALACIÓN DESATENDIDA DE SISTEMAS OPERATIVOS Y PRODUCTOS MICROSOFT WINDOWS



NOVIEMBRE 2019

Edita:



© Centro Criptológico Nacional, 2019



2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

Fecha de Edición: noviembre de 2019

Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

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).

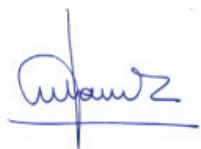
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad 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.

Julio de 2019



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. IMPLEMENTACIÓN DE SEGURIDAD DESATENDIDA EN MS WINDOWS SERVER 2016.....	15
ANEXO A.1. GUÍA PASO A PASO CONTROLADOR DE DOMINIO DE FORMA DESATENDIDA ..	16
ANEXO A.2. GUÍA PASO A PASO SERVIDOR MIEMBRO DE FORMA DESATENDIDA.....	26
1. PREPARACIÓN DEL DOMINIO.....	26
2. DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA	28
ANEXO A.3. GUÍA PASO A PASO SERVIDOR INDEPENDIENTE DE FORMA DESATENDIDA	36
ANEXO B. IMPLEMENTACIÓN DE SEGURIDAD DESATENDIDA EN MS WINDOWS 10	43
ANEXO B.1. GUÍA PASO A PASO WINDOWS 10 MIEMBRO DE DOMINIO DE FORMA DESATENDIDA	44
1. PREPARACIÓN DEL DOMINIO.....	44
2. DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA	45
ANEXO B.2. GUÍA PASO A PASO WINDOWS 10 INDEPENDIENTE DE FORMA DESATENDIDA	54
ANEXO C. IMPLEMENTACIÓN DE SEGURIDAD DESATENDIDA DE PRODUCTOS MICROSOFT EN MS WINDOWS 2016.....	62
ANEXO C.1. GUÍA PASO A PASO INSTALACIÓN PRODUCTOS DE FORMA DESATENDIDA	63
1. PREPARACIÓN DEL DOMINIO.....	63
2. DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA	65

1. INTRODUCCIÓN

Este documento forma parte de la documentación emitida por el Centro Criptológico Nacional cuyo objetivo es el de preservar la seguridad de los sistemas informáticos de la administración pública y de organizaciones dentro del ámbito de los sistemas clasificados.

Para ello, se proporciona un mecanismo de aplicación de medidas de seguridad de forma automatizada y desatendida para facilitar la posibilidad de implementar sistemas informáticos de forma sencilla y ágil.

2. OBJETO

El propósito de este documento consiste en establecer los procedimientos y utilidades necesarias para implementar y garantizar la seguridad en los sistemas operativos Microsoft de manera automatizada. Para ello, se utilizará un procedimiento que minimiza la interacción necesaria por parte del administrador de los sistemas informáticos, proporcionando una homogeneización de los sistemas desplegados, y garantizando unas medidas de seguridad adecuadas.

3. ALCANCE

Este documento establece un procedimiento genérico para realizar el despliegue de forma desatendida de un sistema operativo sobre el que se aplica la configuración de seguridad establecida por las guías CCN-STIC, junto con la instalación de determinado software.

Los apartados y secciones de este documento recogen el proceso de despliegue y configuración de un sistema operativo Microsoft Windows en sus diferentes versiones. A continuación, se muestran las diferentes variantes que se contemplan en esta guía:

a) CCN-STIC-570A

i. CCN-STIC-570A Anexo A ENS:

- Despliegue desatendido de Controlador de Dominio en su Categoría Básica.
- Despliegue desatendido de Controlador de Dominio en su Categoría Media.
- Despliegue desatendido de Controlador de Dominio en su Categoría Alta - DL.
- Despliegue desatendido de Servidor Miembro en su Categoría Básica.
- Despliegue desatendido de Servidor Miembro en su Categoría Media.
- Despliegue desatendido de Servidor Miembro en su Categoría Alta - DL.

ii. CCN-STIC-570A Anexo B Redes Clasificadas:

- Despliegue desatendido de Controlador de Dominio en Redes Clasificadas.
- Despliegue desatendido de Servidor Miembro en Redes Clasificadas.

b) CCN-STIC-570B

i. CCN-STIC-570B Anexo A ENS

- Despliegue desatendido de Servidor Independiente en su Categoría Básica.

- Despliegue desatendido de Servidor Independiente en su Categoría Media.
- Despliegue desatendido de Servidor Independiente en su Categoría Alta - DL.
- ii. CCN-STIC-570B Anexo B Redes Clasificadas
 - Despliegue desatendido de Servidor Independiente en Redes Clasificadas.

Nota: La aplicación de los despliegues desatendidos referenciados en este documento concuerdan con las guías de seguridad codificadas como “CCN-STIC-570A” y “CCN-STIC-570B”. Deberá tomar dichos documentos como referencia para conocer la seguridad establecida en los equipos a los que se les va a aplicar seguridad por el presente documento, así como las tareas adicionales aplicables a los mismos.

Este procedimiento es de aplicabilidad similar sobre otros sistemas operativos Microsoft (Windows 7, Windows 10, etc.) teniendo en consideración que se debe disponer de los recursos adecuados para dichos sistemas operativos, y se debe referir a las guías de seguridad correspondientes a dichos sistemas operativos para la correcta aplicación de este proceso.

Este documento incluye:

- c) Mecanismos para la implementación de la solución. Se incorporan los procedimientos necesarios para la implementación de la solución de forma automatizada.
- d) Mecanismos para la aplicación de configuraciones. Se incorporan los procedimientos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.
- e) Guía paso a paso. Permitirá implementar y establecer las configuraciones necesarias en los sistemas operativos.
- f) Solucionarios y operaciones básicas de administración. Corresponden a procedimientos paso a paso para modificar configuraciones que fueran necesarias en el equipo donde se despliega el sistema operativo y que están extraídos de las guías de seguridad emitidas por el Centro Criptológico Nacional.

Nota: Este procedimiento está pensado para ser utilizado con imágenes de sistema operativo activables con claves de licenciamiento por volumen.

4. ACCIONES PREVIAS

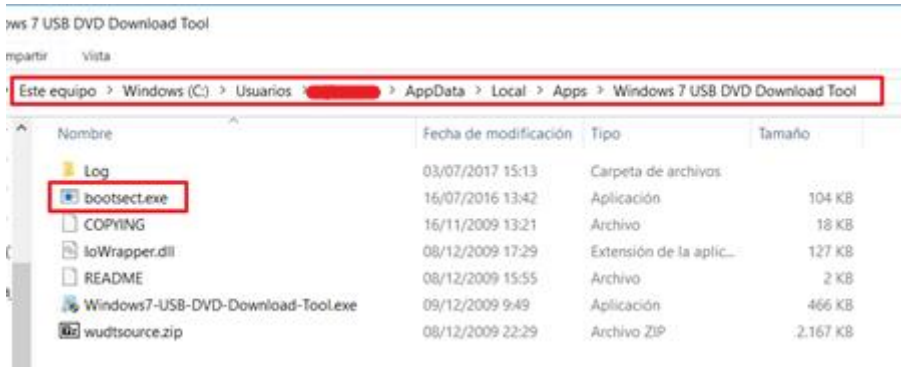
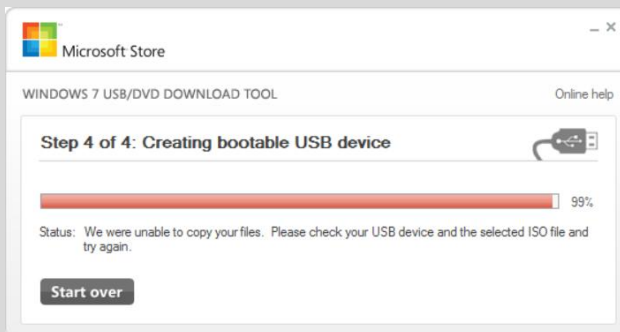
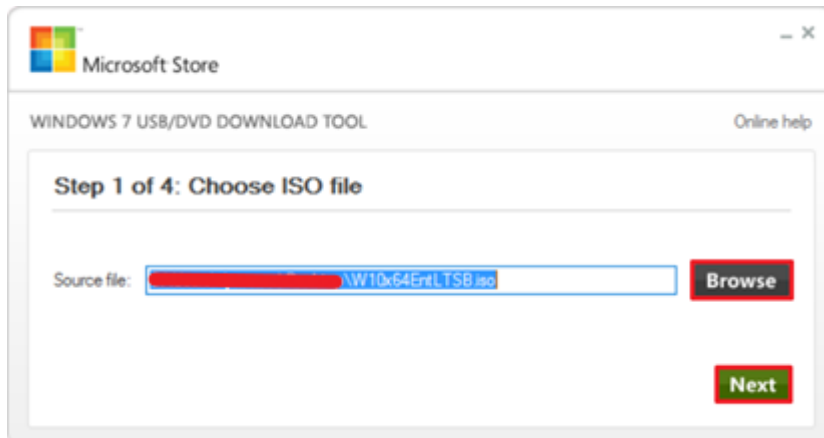
4.1 CREACIÓN DE DISPOSITIVO EXTRAIBLE AUTO-ARRANCABLE

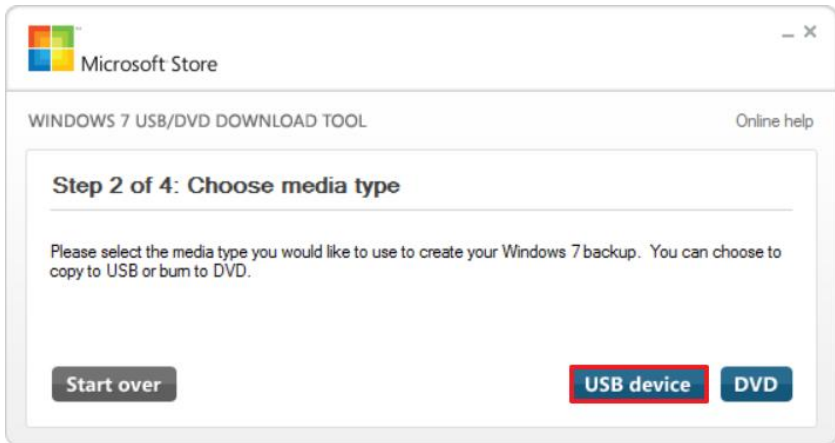
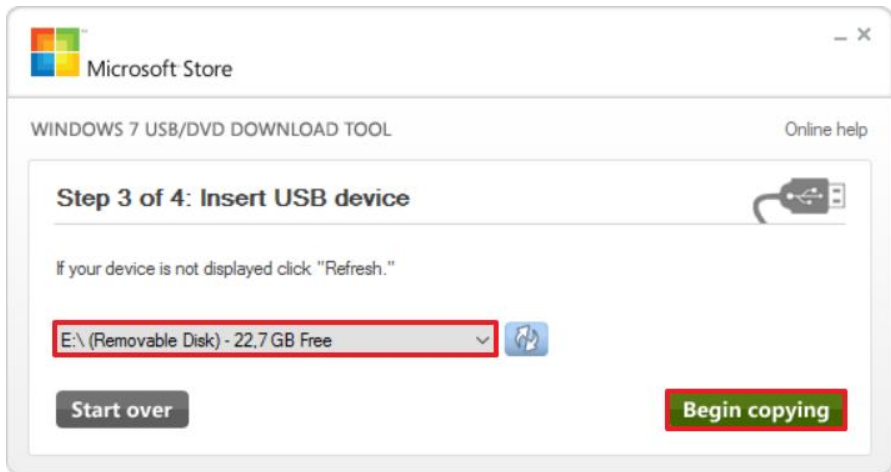
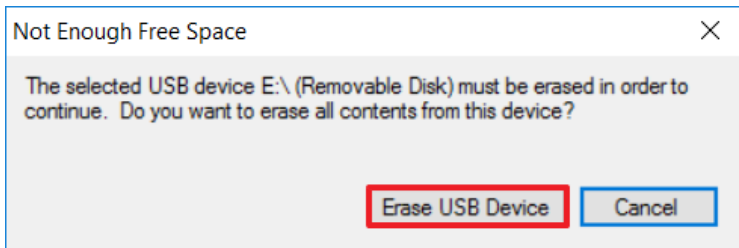
Para la preparación del proceso de despliegue desatendido, será necesario elaborar una unidad “auto-arrancable” que contenga los recursos necesarios para la aplicación de seguridad del sistema.

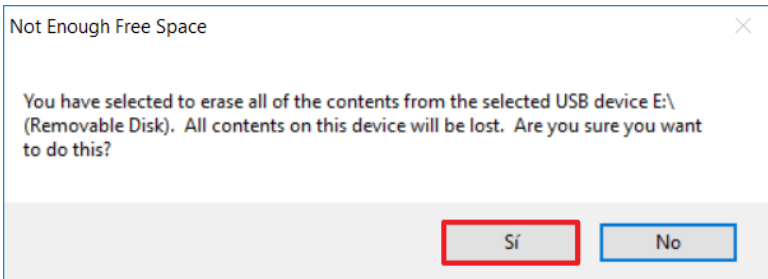
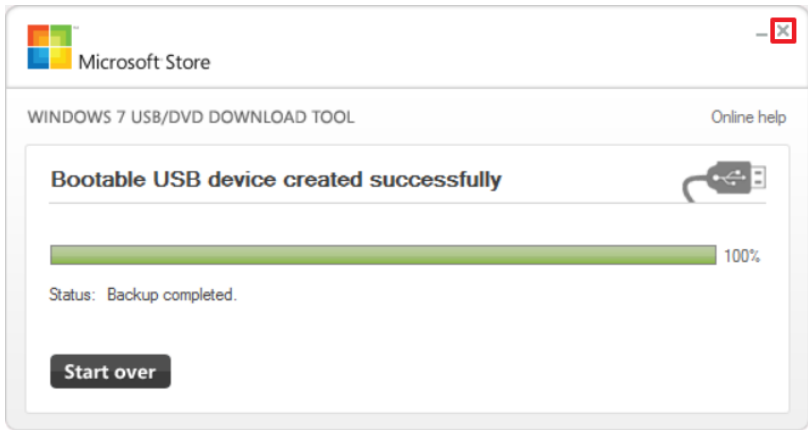
En el siguiente paso a paso se va a utilizar la herramienta “Windows 7 USB DVD Download Tool” la cual es necesaria preparar antes de comenzar el proceso. Puede descargarla a través del siguiente enlace.

<https://www.microsoft.com/es-es/download/windows-usb-dvd-download-tool>

Paso	Descripción
1.	Instale la aplicación “Windows 7 USB DVD Download Tool” siguiendo el asistente de la propia herramienta.

Paso	Descripción
2.	Acceda al directorio “C:\Windows\System32” y copie el fichero denominado “Bootsect.exe”.
3.	Pegue el fichero en el siguiente directorio “C:\Usuarios\<su usuario>\AppData\Local\Apps\Windows 7 USB DVD Download Tool” tal y como se muestra en la imagen.  Nota: Es posible que si no se realiza este paso, cuando se intente crear el medio para arrancar el sistema muestre el siguiente error: 
4.	Ejecute la herramienta “Windows 7 USB DVD Download Tool”.
5.	Pulse sobre el botón “Browse”, seleccione el fichero “.iso” que pertenece al sistema operativo que desea desplegar y pulse el botón “Next”. 

Paso	Descripción
6.	Introduzca el dispositivo extraíble de almacenamiento sobre el que desea desplegar el fichero “.iso” seleccionado en el paso anterior. Nota: Tenga en consideración que la unidad de almacenamiento extraíble se formateará durante el proceso y se perderán todos los datos.
7.	Pulse sobre aquel dispositivo donde desea crear la imagen. En este ejemplo se utilizará la opción “USB device”. 
8.	Seleccione la unidad deseada desde el desplegable de la parte izquierda y pulse sobre el botón “Begin copying”. 
9.	Si el dispositivo no posee espacio suficiente lanzara un mensaje de advertencia. Pulse sobre “Erase USB Device” para formatear el dispositivo.  Nota: El procedimiento borrará el contenido del dispositivo USB. No continúe si no está seguro.

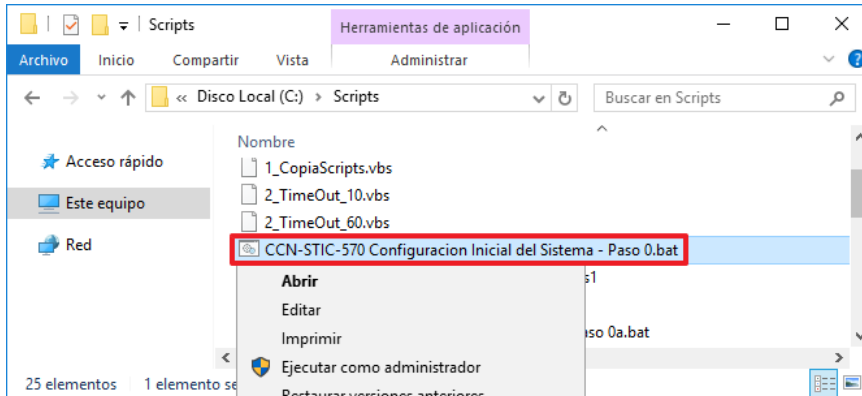
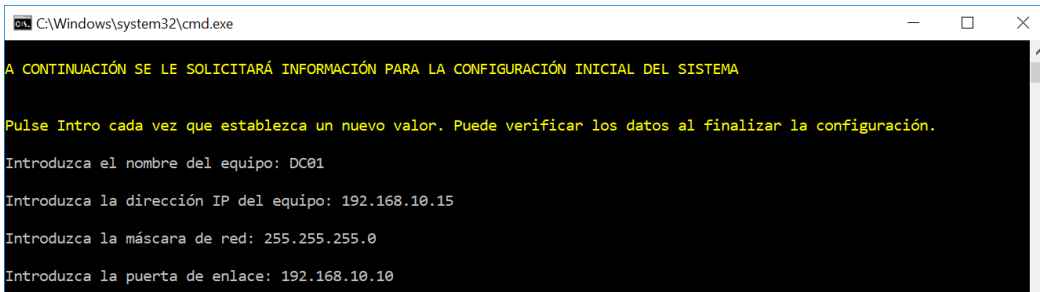
Paso	Descripción
10.	Pulse “Sí” para confirmar el borrado de los datos del dispositivo. 
11.	El proceso dará comienzo. Cierre la herramienta cuando finalice la tarea. 

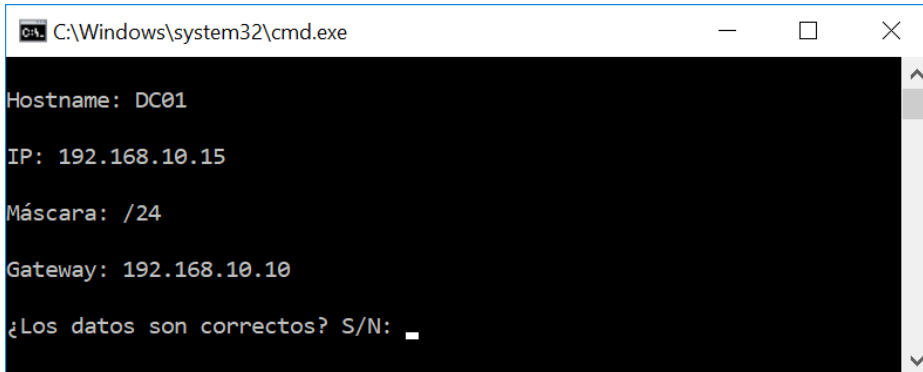
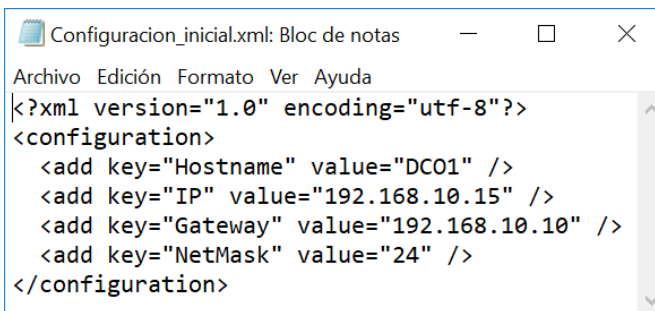
4.2 CONFIGURACIÓN PERSONALIZADA ANTES DE LA INSTALACIÓN DESATENDIDA

Como paso previo al despliegue desatendido de cualquiera de las variantes de seguridad mencionadas en el punto “3. ALCANCE”, será necesaria la configuración de ciertos parámetros como el nombre de equipo, direccionamiento IP o nombre de dominio. Para ello, dentro de la carpeta de recursos “Scripts” se han habilitado ciertos ficheros de configuración que permiten modificar dichos parámetros dependiendo de las necesidades de su organización.

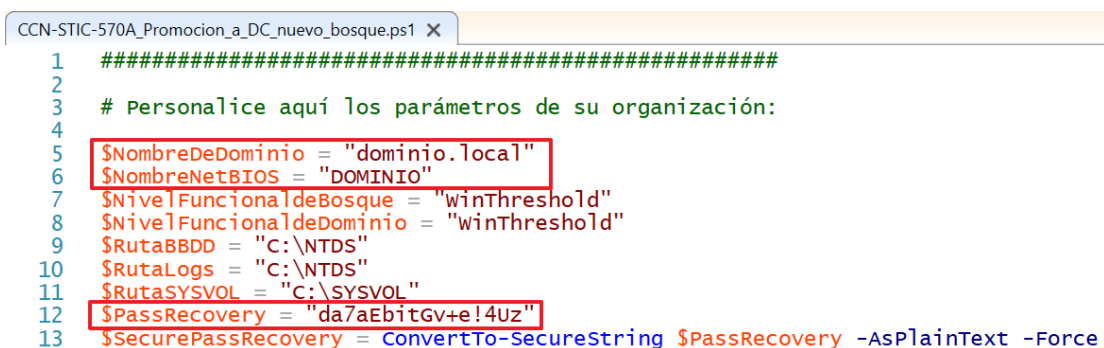
En el siguiente paso a paso se describe como configurar los valores necesarios acorde a su organización, para un correcto despliegue.

Paso	Descripción
12.	De los recursos proporcionados por esta guía, copie la carpeta “Scripts” de aquel despliegue que desea automatizar en su directorio “C:\” de un equipo de trabajo habitual. Nota: La ejecución de los scripts no contempla otra ruta que no sea la mencionada anteriormente, sino es así, la ejecución de los scripts fallará.

Paso	Descripción
13.	Diríjase a la carpeta de recursos “C:\Scripts” y ejecute el script llamado “CCN-STIC-570 Configuración Inicial del Sistema - Paso 0.bat” haciendo clic derecho sobre él y pulsando sobre “Ejecutar como administrador”.  Nota: El nombre del script variará dependiendo del sistema operativo que esté implementando.
14.	Cuando se ejecute el script, se solicitará por pantalla diferentes parámetros de configuración inicial del sistema. Introduzca los parámetros acordes a los criterios de su organización y pulse “Enter” al introducir cada parámetro para continuar con el siguiente. Tome de ejemplo la siguiente imagen.  Nota: El nombre del equipo no debe exceder de los 15 caracteres. Dependiendo del despliegue que haya seleccionado puede variar ciertos parámetros con la imagen mostrada.

Paso	Descripción
15.	Al finalizar, el script mostrara un resumen de los datos introducidos. Verifique que dichos datos son correctos y pulse “S” para terminar y “N” para volver a introducir los datos de nuevo. 
16.	Si lo desea, puede abrir el fichero generado llamado “Configuracion_inicial.xml” donde encontrará los parámetros establecidos en el paso anterior. Asegúrese de no encontrar ningún espacio en los datos introducidos. 
17.	A continuación, dependiendo del sistema operativo o producto que esté implementando deberá realizar configuraciones extras que permitan adaptar el despliegue a las necesidades de su organización. – 4.2.1.CONTROLADOR DE DOMINIO. Deberá seguir dicho apartado en caso de estar implementando un controlador de dominio. – 4.2.3.SERVIDOR MIEMBRO DE DOMINIO. Deberá seguir dicho punto en caso de estar implementando un servidor miembro, cliente miembro o una implementación de cualquier producto. Nota: Si lo que desea es desplegar un equipo independiente, sin hacer distinción al grado de clasificación, diríjase al anexo correspondiente al despliegue desatendido que desee implantar.

4.2.1 CONTROLADOR DE DOMINIO

Paso	Descripción
18.	Si desea desplegar un controlador de dominio, ubíquese en la carpeta “C:\Scripts” y edite el script “CCN-STIC-570A_Promocion_a_DC_nuevo_bosque.ps1” y modifique las siguientes variables. Tome de ejemplo la siguiente imagen. – \$NombreDeDominio: Establezca el nombre del dominio que desea crear. – \$NombreNetBIOS: Establezca el nombre NetBIOS. No debe exceder los 15 caracteres. – PassRecovery: Establezca la contraseña de recuperación. Una vez guardado el script, la contraseña será encriptada. Cuando haya finalizado, pulse “Archivo → Guardar” para aplicar los cambios al archivo de configuración.  <pre> 1 ##### 2 3 # Personalice aquí los parámetros de su organización: 4 5 \$NombreDeDominio = "dominio.local" 6 \$NombreNetBIOS = "DOMINIO" 7 \$NivelFuncionaldeBosque = "winThreshold" 8 \$NivelFuncionaldeDominio = "winThreshold" 9 \$RutaBBDD = "C:\NTDS" 10 \$RutaLogs = "C:\NTDS" 11 \$RutaSYSVOL = "C:\SYSVOL" 12 \$PassRecovery = "da7aEbitGv+e!4Uz" 13 \$SecurePassRecovery = ConvertTo-SecureString \$PassRecovery -AsPlainText -Force </pre> Nota: Tenga en consideración que si desea modificar la ruta de instalación de los componentes del directorio activo puede estar afectando al correcto funcionamiento del despliegue desatendido. La letra de la unidad de instalación de los componenetes variara en función del grado de clasificación que haya elegido.
19.	A continuación, tras modificar los diferentes archivos atendiendo a las necesidades de su organización continúe con el siguiente punto en el caso de implementar un controlador de dominio para una red clasificada (CCN-STIC-570A – Anexo B). En caso contrario diríjase al anexo que corresponda para comenzar el despliegue.

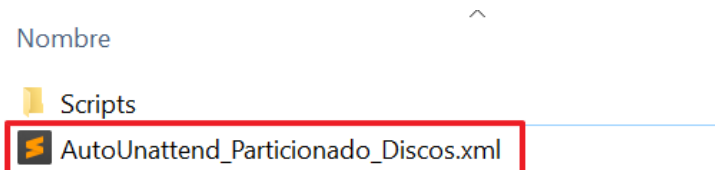
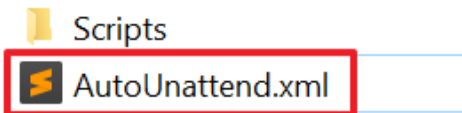
4.2.2 CONFIGURACIÓN PRELIMINAR DE PARTICIONADO DE DISCOS

Debido a las directrices de seguridad marcadas por las guías CCN-STIC, dependiendo del grado de clasificación, se debe realizar un particionado del disco como medida de seguridad. Este es el caso de Windows Server 2016 como controlador de dominio, el cual, por las medidas de seguridad estipuladas por la guía 570A Anexo B, requiere el uso de tres (3) discos o en su defecto de tres (3) particiones para realizar una correcta instalación del sistema y así cumplir con lo establecido en dicho documento.

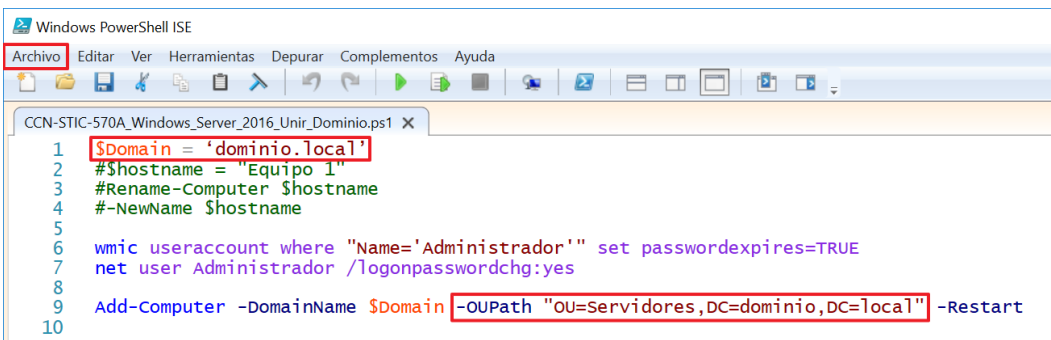
En el proceso del despliegue desatendido del punto “**ANEXO A.1. GUÍA PASO A PASO CONTROLADOR DE DOMINIO DE FORMA DESATENDIDA**” se contempla una instalación donde el equipo tenga 3 discos duros físicos para realizar una correcta instalación. Sino es así, y en su sistema no puede contemplar el uso de tres (3) discos duros físicos, siga el siguiente paso a paso

para crear tres (3) particiones de forma desatendida durante la instalación sobre un disco duro con una capacidad mínima de 300 GB.

Nota: El disco sobre el que se realizará el particionado durante la instalación desatendida debe estar debidamente formateado en una partición primaria que ocupe todo el espacio del disco. Puede cambiar el tamaño de particionado según las necesidades y capacidades del disco que disponga. Tenga en consideración no alterar cualquier otro valor ya que podría modificar el despliegue.

Paso	Descripción
20.	De los recursos proporcionados por esta guía referentes al apartado mencionado anteriormente, elimine el fichero llamado “AutoUnattend.xml” de tal forma que solo disponga de un único archivo en la carpeta “Scripts” denominado “AutoUnattend_Particionado_Discos.xml” que realizará las funciones de particionado del disco además del resto de configuraciones necesarias. 
21.	Renombre dicho fichero “.xml”, para ello haga clic derecho sobre él y pinche “Cambiar Nombre” y establezca el nombre de “AutoUnattend.xml”. 
22.	Cuando finalice podrá dirijase al Anexo mencionado anteriormente para proceder al despliegue desatendido. Nota: Tenga en consideración que las tres particiones que se creará en el proceso de despliegue tendrán una capacidad de 100GB cada una.

4.2.3 SERVIDOR MIEMBRO DE DOMINIO

Paso	Descripción
23.	Si desea desplegar un servidor miembro o un cliente miembro como Windows 10, diríjase a la carpeta “C:\Scripts” edite el script correspondiente a su despliegue y modifique las siguientes variables. Siga el siguiente ejemplo. – \$Domain: Escriba el nombre de dominio de su organización. – OUPath: Escriba el dominio al que pertenecerá tomando de ejemplo la siguiente imagen. Cuando haya finalizado, pulse “Archivo → Guardar” para aplicar los cambios al script de configuración.  <pre> 1 \$Domain = 'dominio.local' 2 \$hostname = "Equipo 1" 3 #Rename-Computer \$hostname 4 #-NewName \$hostname 5 6 wmic useraccount where "Name='Administrador'" set passwordexpires=TRUE 7 net user Administrador /logonpasswordchg:yes 8 9 Add-Computer -DomainName \$Domain -OUPath "OU=Servidores,DC=dominio,DC=local" -Restart 10 </pre> - CCN-STIC-570A_Windows_Server_2016_Unir_Dominio.ps1: corresponde con la aplicación de la guía 570A Anexo A como servidores miembros y guías como 572 Anexo A servidores de impresión y 573 Anexo A servidores de ficheros. - CCN-STIC-599A18_Windows_10_Ent_2016LTSB_Unir_Dominio.ps1: corresponde con la aplicación de la guía 599A18 como cliente miembro.
24.	Tras finalizar, diríjase al anexo correspondiente al despliegue desatendido que desee implantar.

ANEXO A. IMPLEMENTACIÓN DE SEGURIDAD DESATENDIDA EN MS WINDOWS SERVER 2016

Este anexo ha sido diseñado para ayudar a los operadores a desplegar distintas configuraciones de seguridad de forma desatendida. A continuación, se describe, paso a paso, como implementar las diferentes configuraciones de seguridad atendiendo al Esquema Nacional de Seguridad y a entornos clasificados.

Esta guía incorpora todos los ficheros y scripts de configuración para poder realizar un despliegue automatizado atendiendo a los estándares de seguridad definidos en las diferentes categorías del ENS así como en las guías orientadas a redes clasificadas.

ANEXO A.1. GUÍA PASO A PASO CONTROLADOR DE DOMINIO DE FORMA DESATENDIDA

Este apartado recoge el procedimiento para automatizar la instalación y aplicación de seguridad sobre Windows Server 2016 con la función de nuevo controlador de dominio en un nuevo bosque.

Esta guía incorpora todos archivos de automatización necesarios para cumplir con las directrices de seguridad marcadas en la guía CCN-STIC-570A.

El proceso de despliegue, en el caso de un entorno de red clasificada, contempla que el equipo donde se vaya a desplegar el sistema operativo cuenta con **tres discos duros** para realizar la instalación desatendida cumpliendo con la guía CCN-STIC-570B Anexo B, sino es así, realice los cambios oportunos descritos en el apartado “4.2.2 CONFIGURACIÓN PRELIMINAR DE PARTICIONADO DE DISCOS”.

Nota: La configuración de particiones solo es aplicable en el caso de implementar un controlador de dominio para una red clasificada.

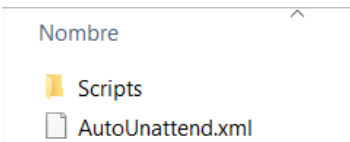
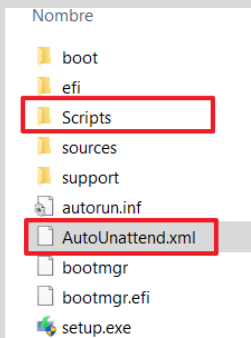
Una vez generado el dispositivo extraíble “auto-arrancable”, deberá seguir los siguientes pasos para desplegar el sistema operativo correspondiente a la imagen seleccionada en el equipo deseado. Este proceso eliminará el contenido del disco duro del equipo.

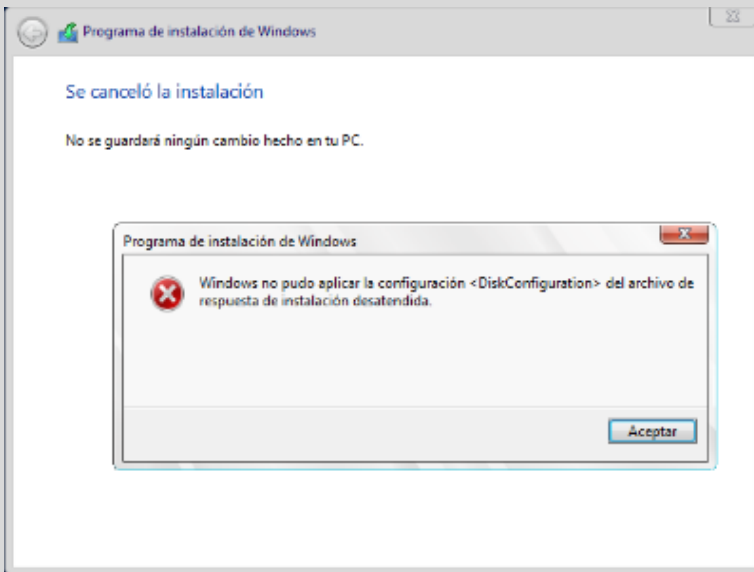
Adicionalmente deberá tener conectado un USB o un CD-ROM el cual posea en su directorio raíz los ficheros que se adjuntan a esta guía.

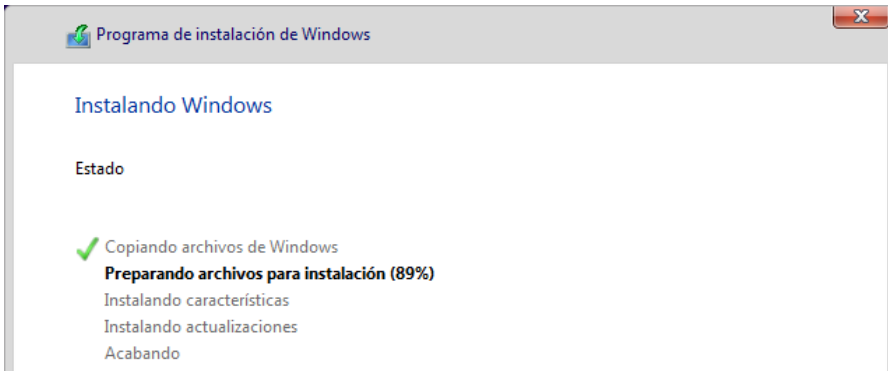
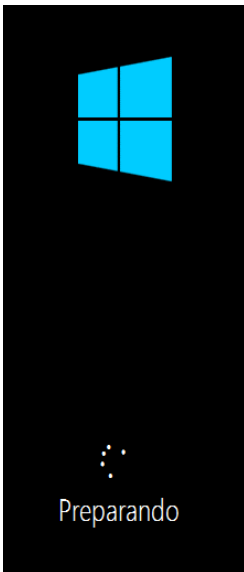
Antes de realizar el despliegue de la imagen del sistema operativo, se recomienda configurar la BIOS del sistema para deshabilitar los dispositivos conectados que no sean necesarios con el fin de prevenir la instalación de los drivers de dichos dispositivos en el sistema operativo durante el proceso de despliegue.

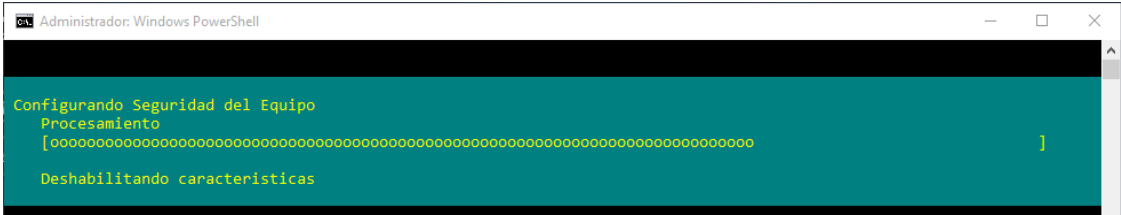
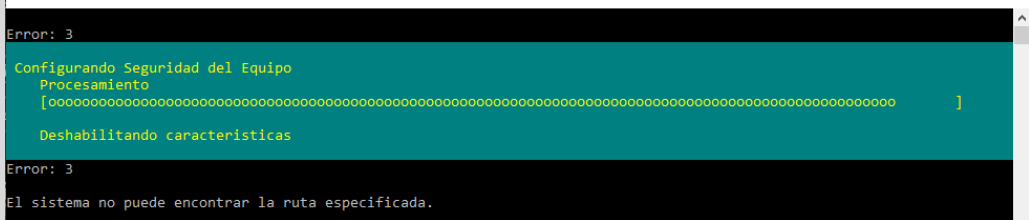
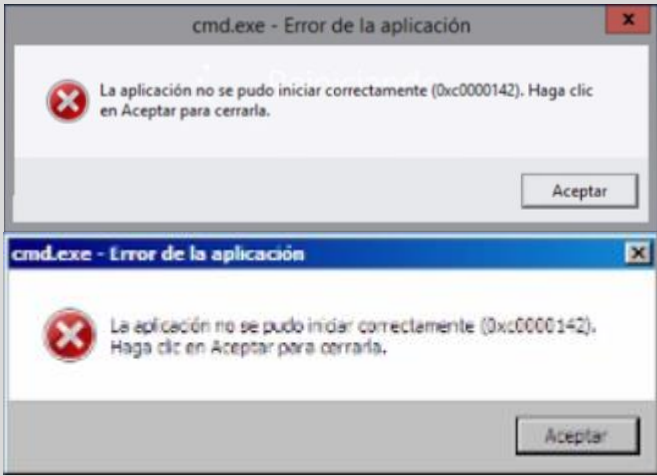
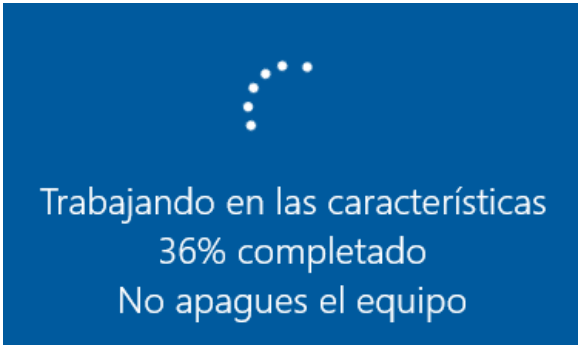
Nota: Tenga en consideración que el presente despliegue está pensado para un sistema operativo con instalación en castellano, por lo que, si la imagen ISO utilizada para este despliegue no posee dicho idioma, la aplicación del procedimiento de bastionado del sistema no se realizará adecuadamente.

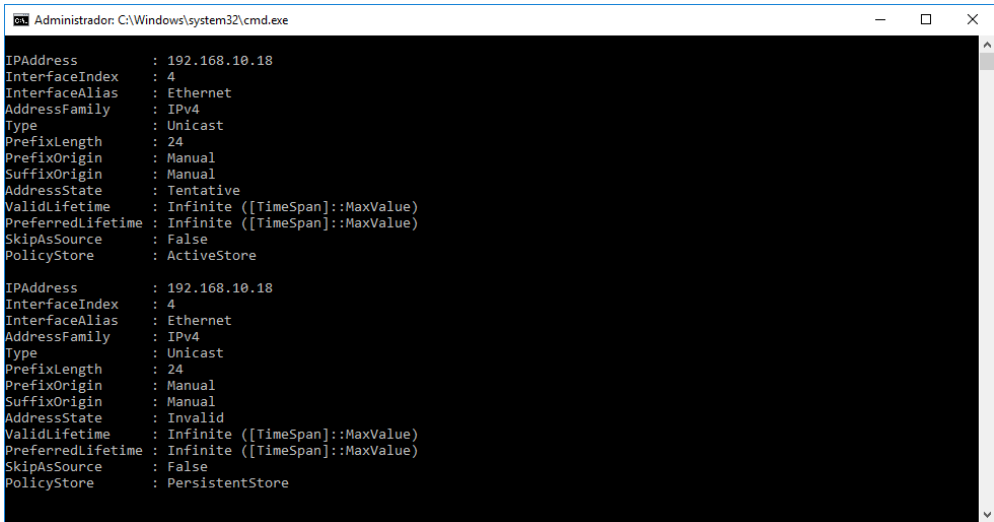
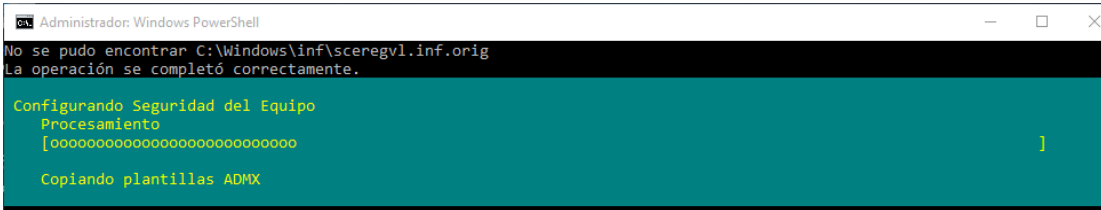
Paso	Descripción
1.	Introduzca el USB de instalación que ha creado en el apartado “4.1.CREACIÓN DE DISPOSITIVO EXTRAIBLE AUTO-ARRANCABLE” en el equipo en el que desee desplegar la imagen del sistema operativo y arranque el equipo. Nota: Deberá tener en consideración la configuración de la BIOS del equipo para que el proceso de arranque comience desde el USB de instalación. Para ello deberá: - Configurar la BIOS con la opción “Legacy” para que permita el arranque mediante dispositivos USB. Esta opción es posible que sea necesario cambiarla más adelante. - Modificar el orden de arranque para que el sistema inicie desde el dispositivo USB. Tenga en consideración que tras el primer reinicio del sistema éste deberá arrancar el sistema desde el disco duro. Por lo tanto, es probable que necesite configurar de nuevo la BIOS para que el sistema no proceda a instalar de nuevo el sistema operativo. Es necesario que no se retiren los elementos de instalación hasta que se indique lo contrario en este manual. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.

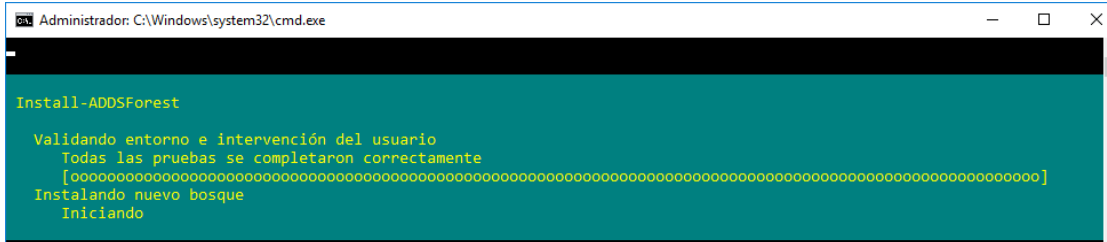
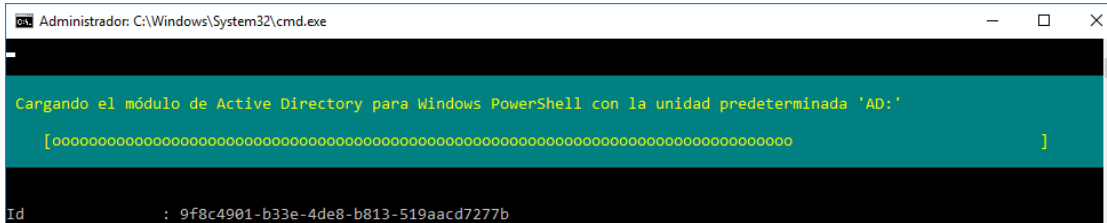
Paso	Descripción
2.	Asegúrese, antes de iniciar el equipo, que tiene todos los dispositivos conectados y configurados de manera adecuada: – Dispositivo auto-arrancable con el sistema operativo deseado (realizado en el punto anterior). – USB o CD-ROM con los ficheros que se adjuntan a esta guía en el directorio raíz.
3.	En la siguiente imagen podrá observar cómo deben estar dispuestos los ficheros que se adjuntan a esta guía dentro del directorio raíz del dispositivo.  Nota: Tenga en consideración que estos ficheros pueden ser copiados en el directorio raíz del dispositivo autoarrancable generado con la ISO del Sistema Operativo lo que supone que solo sería necesario un único dispositivo USB. El dispositivo autoarrancable junto con los ficheros que se adjuntan a este manual tendrían un aspecto similar al siguiente. 

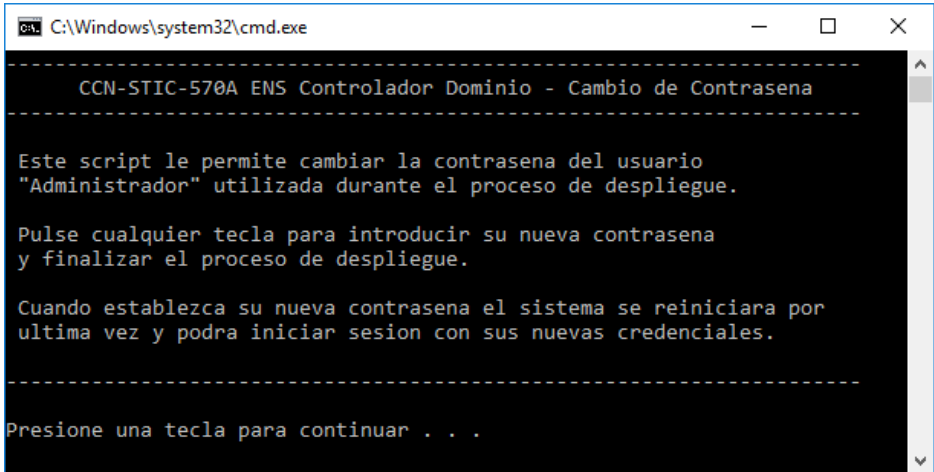
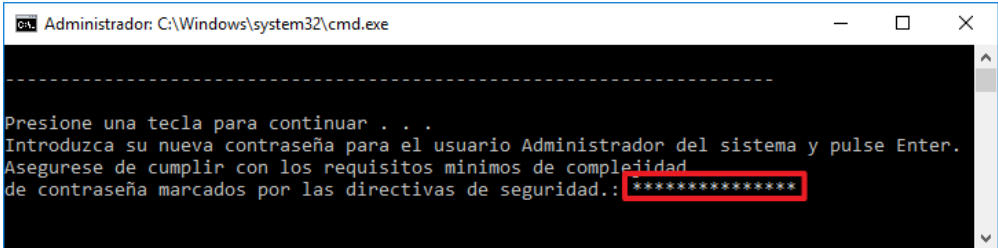
Paso	Descripción
4.	El sistema arrancará desde la unidad auto-arrancable. En primer lugar, deberá aceptar el EULA del fabricante. Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  Nota: Tenga en consideración que este procedimiento realiza un borrado del disco por lo que antes de comenzar la instalación haga una copia de seguridad de los archivos necesarios. Apague el equipo en este punto si fuera necesario. Si el sistema no dispone de tres discos duros para el despliegue desatendido, observará el siguiente error. Realice los cambios oportunos descritos en el apartado “4.2.2 CONFIGURACIÓN PRELIMINAR DE PARTICIONADO DE DISCOS”. Solo será aplicable este punto en el caso de un controlador de dominio para una red clasificada. 

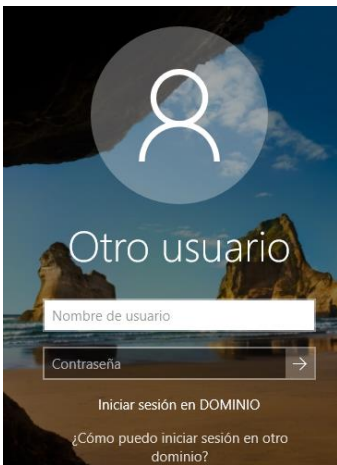
Paso	Descripción
5.	A continuación, el proceso de instalación desatendida comenzará. 
6.	El equipo se reiniciará varias veces durante la instalación. Recuerde no extraer ninguno de los dispositivos conectados a éste, ya que si lo hace antes de que se indique en este manual la aplicación de seguridad del sistema no se completará. Deberá configurar la BIOS, si es necesario, para que el arranque después del primer reinicio se realice desde el disco duro del equipo. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
7.	Durante la instalación aparecerán diferentes pantallas que estarán personalizando y aplicando seguridad en el equipo. No pulse ninguna tecla durante todo el proceso, de lo contrario podría interrumpir el proceso y será necesario empezar de nuevo. 
8.	El equipo iniciará sesión una primera vez de forma automática y continuará implantando la seguridad en el equipo. Nota: Dependiendo de la velocidad del equipo es posible que el tiempo de configuración del equipo varíe. Si está implementando un controlador de dominio para una red clasificada continúe con el siguiente paso. En caso contrario vaya al paso “11”.

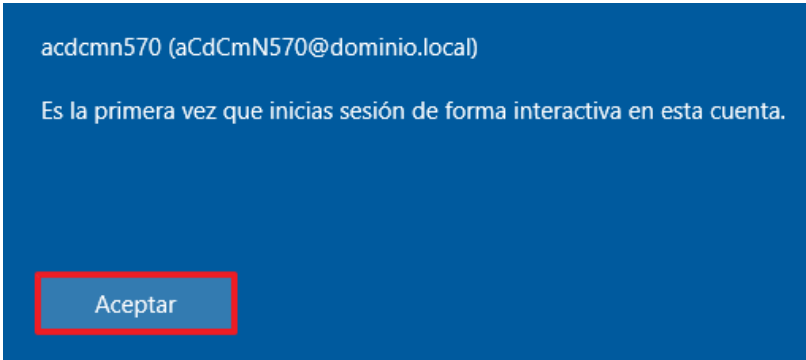
Paso	Descripción
9.	La primera vez que se muestra el escritorio aparecerá una consola que muestra el progreso de la aplicación de seguridad del sistema.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. En caso de aparecer el mensaje “Error 3: El sistema no puede encontrar la ruta especificada.”, ignórelo y no cancele el proceso del script.  Adicionalmente si apareciese el siguiente error durante el despliegue en alguno de los sistemas, ignórelo y continúe. 
10.	El equipo se reiniciará de nuevo y continuará con la implementación de seguridad en el sistema. 

Paso	Descripción
11.	A continuación, aparecerá una consola que configurará el nombre y el direccionamiento IP del equipo. Cuando termine el equipo se reiniciará de nuevo automáticamente. 
12.	Se iniciará de nuevo sesión en el sistema de manera automática y continuará el proceso.  Nota: El número de reinicios dependerá del sistema operativo instalado y las necesidades de éste. En cualquiera de las casuísticas, cuando la aplicación de seguridad del equipo haya finalizado se pedirá al usuario que inicie sesión y no antes de que el proceso finalice.
13.	Tras el reinicio, se mostrará de nuevo una ventana en la que se muestra el progreso de implantación de seguridad.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. Ignore el mensaje “No se puede encontrar C:\Windows\inf\sceregvl.inf.orig” en caso de que apareciese.

Paso	Descripción
14.	Posteriormente, se procederá a la instalación del rol de directorio activo y a su promoción como controlador de dominio. El proceso puede tardar varios minutos. 
15.	Cuando finalice la instalación del rol de directorio activo, se reiniciará para aplicar la correcta configuración en el sistema. 
16.	Una vez el equipo haya promocionado a controlador de dominio, comenzará con la importación de las medidas de seguridad y la aplicación de las GPO en las Unidades Organizativas correspondientes. 
17.	Si está implementado la categoría alta – DL del ENS o bien un controlador de dominio en una red clasificada continúe con el siguiente paso, en caso contrario salte al paso “20”.

Paso	Descripción
18.	Como último paso, y para finalizar el despliegue desatendido en el caso de la categoría alta – DL o una red clasificada, deberá establecer una nueva contraseña para el usuario “Administrador” del sistema, el cual ha sido utilizado durante el proceso de despliegue para realizar las labores de implantación de seguridad. Debido a ello, será necesario que establezca una nueva contraseña para el usuario “Administrador”. Pulse una tecla para continuar.  Nota: A causa de las medidas de seguridad implantadas en el sistema, y a diferencia de otros despliegues desatendidos, no se realiza un cambio de contraseña en la pantalla de bloqueo debido a que las políticas de seguridad recién importadas no aceptan MD5 como cifrado seguro para el protocolo Kerberos, con lo que impide cambiar las credenciales en la pantalla de bloqueo tras importar la configuración de seguridad y en el primer inicio de sesión.
19.	En la siguiente pantalla, introduzca sus nuevas credenciales para el usuario “Administrador”. 
20.	Cuando finalice el proceso, el equipo se reiniciará por última vez. Inicie sesión y continúe con el siguiente paso.

Paso	Descripción
21.	Introduzca las credenciales del usuario predefinido para este proceso e inicie sesión. Las credenciales para iniciar sesión son: – Usuario: Administrador – Contraseña: Password_1234  Nota: En el caso de sistemas operativos servidor el usuario con el que se debe iniciar sesión es el “Administrador”. Para la categoría alta – DL o una red clasificada deberá introducir las credenciales ya definidas en el paso “19”. El usuario puede haber sido renombrado por la aplicación de seguridad en el equipo y definido por el nombre de la guía que se le aplica. Por ejemplo, en el caso de Windows Server 2016 el usuario “Administrador” se renombra como “aCdCmN570”.
22.	Debido a que se trata del primer inicio de sesión que no es desatendido, deberá establecer las credenciales para el usuario. Pulse “Aceptar” para comenzar el proceso.  Nota: Este paso y el siguiente no será necesario en el caso de un equipo que le sea de aplicación la categoría alta – DL del ENS o pertenezca a la configuración de una red clasificada.

Paso	Descripción
23.	Introduzca las nuevas credenciales y pulse “→”.  Nota: Recuerde que la nueva contraseña debe cumplir con los requisitos de longitud y complejidad establecidos.
24.	Debido a que se trata del primer inicio de sesión no desatendido con la configuración de seguridad ya aplicada, es necesario pulsar “Aceptar” en el siguiente mensaje de inicio de sesión y comenzar con el siguiente punto.  Nota: Este mensaje solo aparecerá en el caso de haber configurado un controlador de dominio para un entorno de red clasificada.
25.	Adicionalmente, revise el documento de seguridad codificado como “CCN-STIC-570A” que hace referencia al sistema operativo que está instalando para verificar la configuración aplicada y realizar aquellas acciones manuales que no pueden ser automatizadas.

ANEXO A.2. GUÍA PASO A PASO SERVIDOR MIEMBRO DE FORMA DESATENDIDA

Este punto se recoge el procedimiento para automatizar la instalación y aplicación de seguridad en Windows Server 2016 con la función de servidor miembro para todos los diferentes grados de clasificación de la guía CCN-STIC-570A.

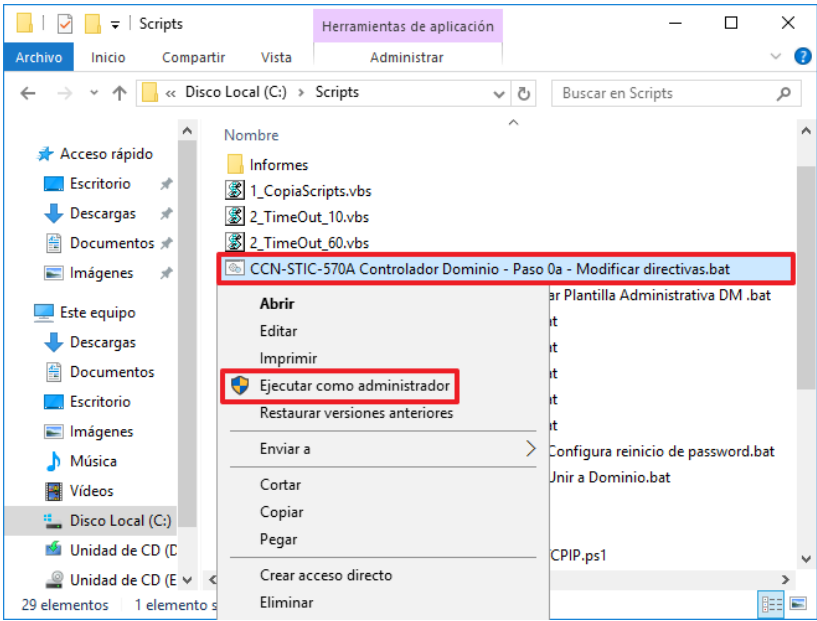
Esta guía incorpora todos archivos de automatización necesarios para cumplir con las directrices de seguridad marcadas en la guía CCN-STIC-570A.

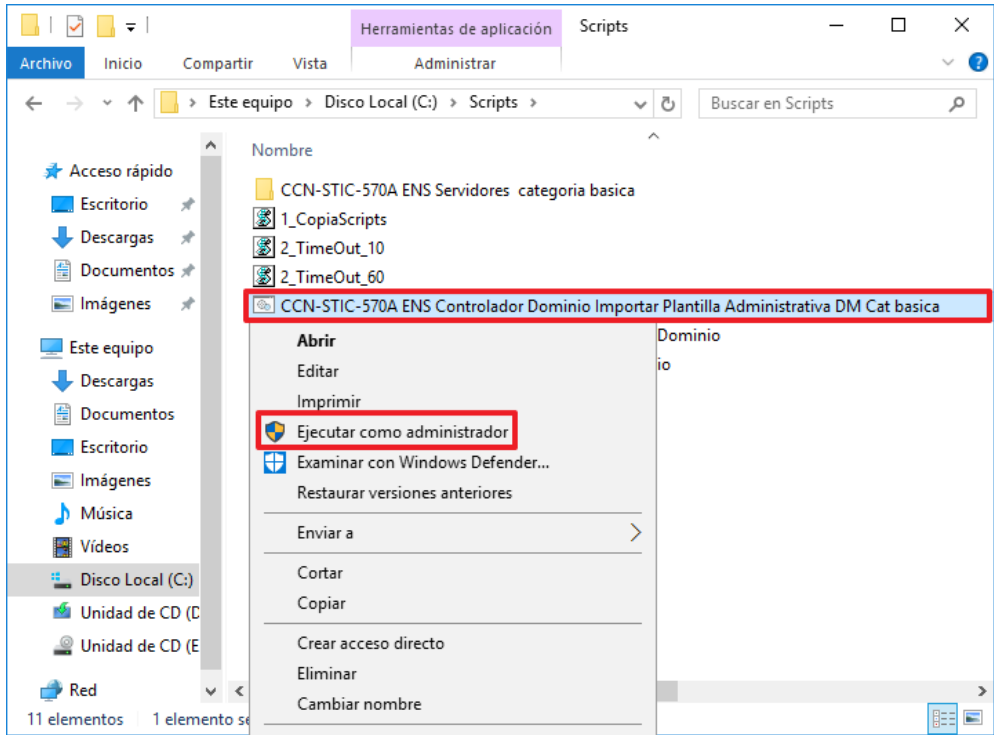
1. PREPARACIÓN DEL DOMINIO

Antes del despliegue desatendido del servidor miembro, es necesario la creación de la unidad organizativa donde se aplicará la seguridad del servidor miembro en el controlador de dominio al que vaya a permanecer dicho equipo.

Siga el siguiente paso a paso para la creación de las directivas de seguridad (GPO) de forma automatizada en el controlador de dominio.

Nota: Si previamente ya ha configurado las directivas de seguridad correspondientes a un servidor miembro siguiendo la guía CCN-STIC 570A, puede saltar al punto **2.DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA**.

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad.
2.	Copie los recursos de dicha guía en la ruta "C:\\".
3.	Diríjase a la carpeta de recursos "Scripts" y ejecute con privilegios de administrador el script "CCN-STIC-570A Controlador Dominio - Paso 0a - Modificar directivas.bat".  Nota: Solo deberá ejecutar este paso en el caso de que esté implementando un servidor miembro orientado a una red clasificada (CCN-STIC-570A - Anexo B). De no ser así vaya al paso siguiente.

Paso	Descripción
4.	Diríjase a la carpeta de recursos “Scripts” y ejecute con privilegios de administrador el script “CCN-STIC-570A ENS Controlador Dominio Importar Plantilla Administrativa DM Cat [su_categoria].bat”.  Nota: Al ejecutar el script se creará la unidad organizativa “Servidores” con sus respectivas directivas de seguridad. Si ya están creadas, la ejecución del script fallará, con lo que podrá continuar con el siguiente punto de la guía. El nombre del fichero variará dependiendo de la categoría a implementar pudiendo existir las siguientes variantes: - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM Cat básica: corresponde con la aplicación de la categoría básica según las especificaciones del ENS. - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM Cat media: corresponde con la aplicación de la categoría media según las especificaciones del ENS. - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM Cat alta – DL: corresponde con la aplicación de la categoría alta/difusión limitada según las especificaciones del ENS. - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM: corresponde con la aplicación de las medidas de seguridad de un servidor miembro dedicado a una red clasificada.
5.	Finalmente, compruebe que se ha creado correctamente la unidad organizativa “Servidores” y su GPO correspondiente en el “Administrador de directivas de grupo”. Así mismo configure el objeto GPO para que la aplicación del mismo se realice sobre los servidores deseados.

2. DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA

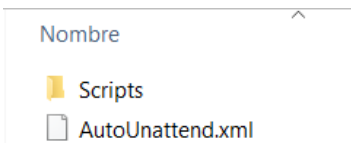
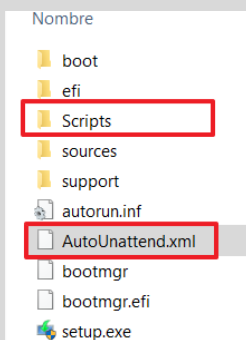
Una vez generado el dispositivo extraíble auto-arrancable, deberá seguir los siguientes pasos para desplegar el sistema operativo correspondiente a la imagen seleccionada en el equipo deseado. Este proceso eliminará el contenido del disco duro del equipo.

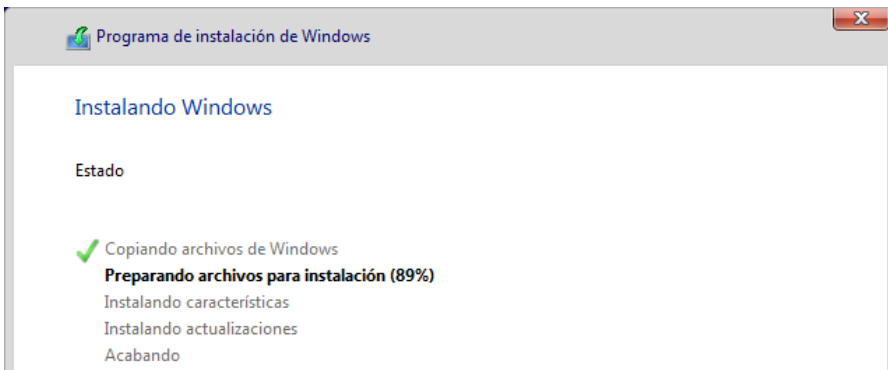
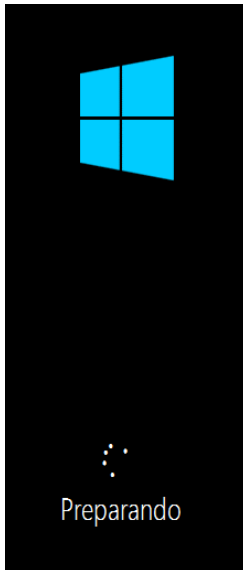
Adicionalmente deberá tener conectado un USB o un CD-ROM el cual posea en su directorio raíz los ficheros que se adjuntan a esta guía.

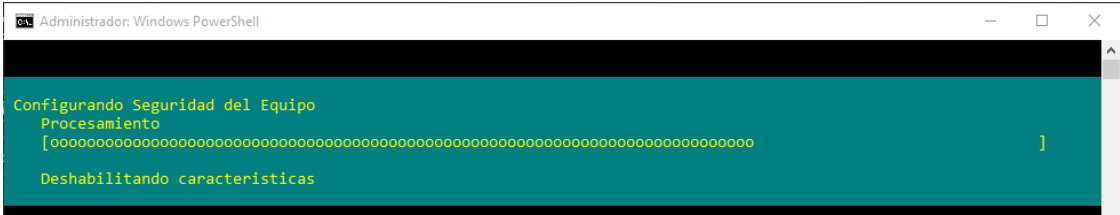
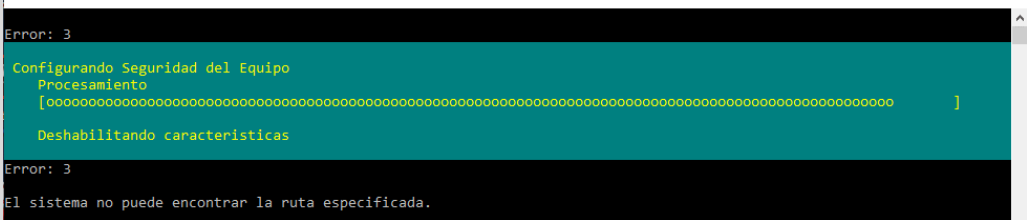
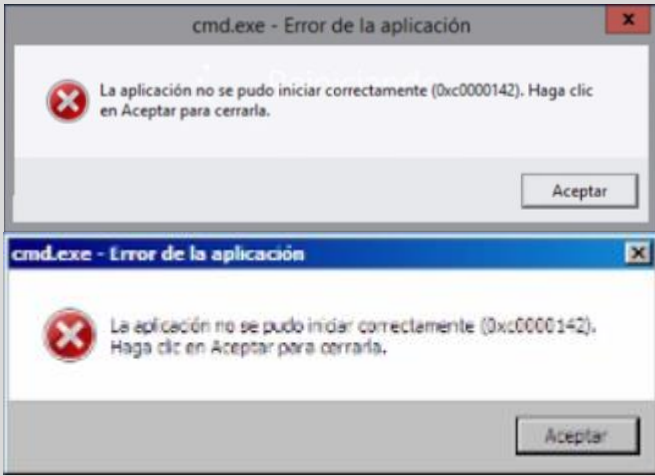
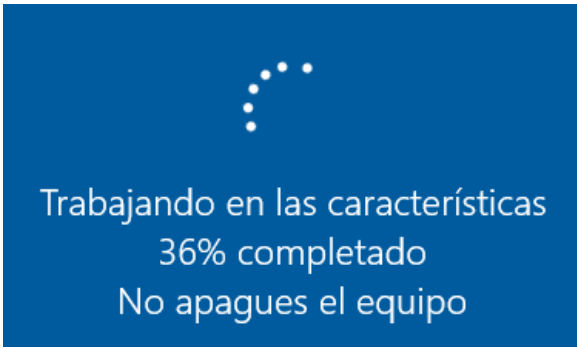
Antes de realizar el despliegue de la imagen del sistema operativo, se recomienda configurar la BIOS del sistema para deshabilitar los dispositivos conectados que no sean necesarios con el fin de prevenir la instalación de los drivers de dichos dispositivos en el sistema operativo durante el proceso de despliegue.

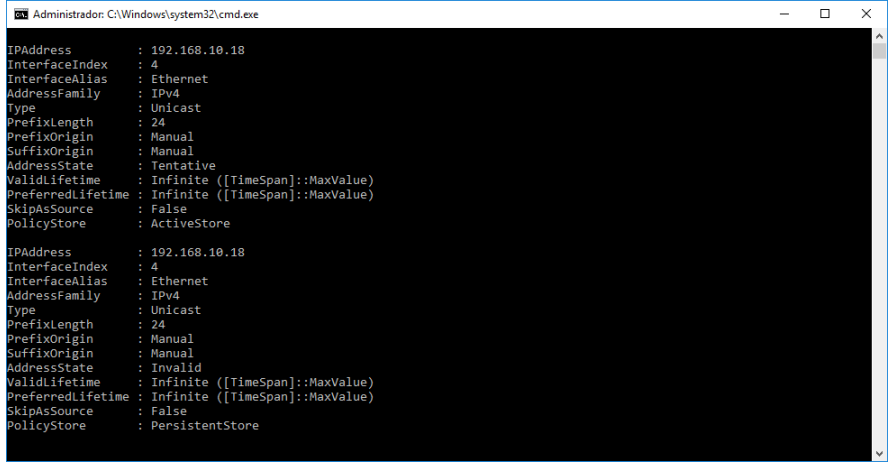
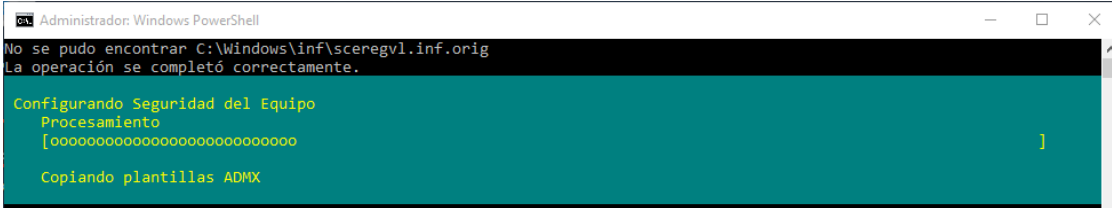
Nota: Tenga en consideración que el presente despliegue está pensado para un sistema operativo con instalación en castellano, por lo que, si la imagen ISO utilizada para este despliegue no posee dicho idioma, la aplicación del procedimiento de bastionado del sistema no se realizará adecuadamente.

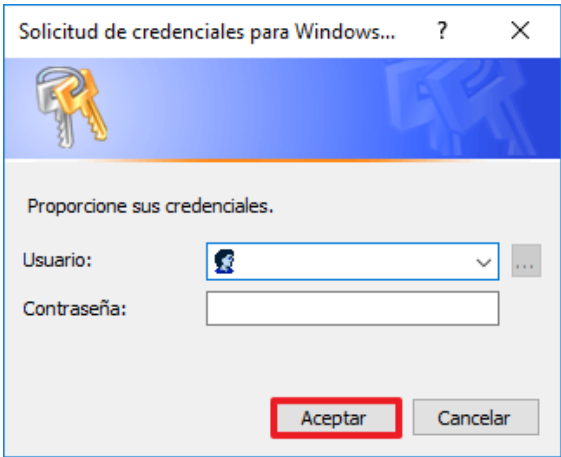
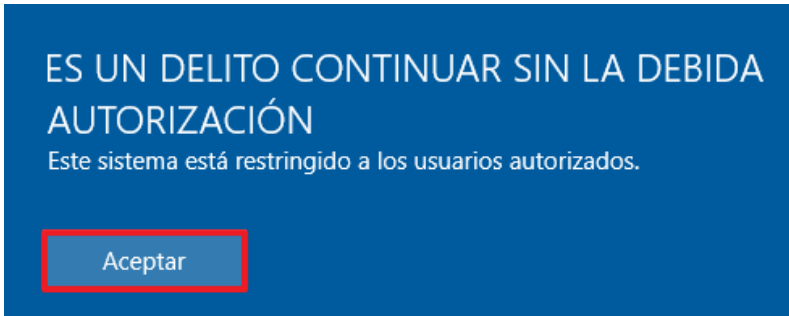
Paso	Descripción
6.	Introduzca el USB de instalación que ha creado en el apartado “4.1.CREACIÓN DE DISPOSITIVO EXTRAIBLE AUTO-ARRANCABLE” en el equipo en el que desee desplegar la imagen del sistema operativo y arranque el equipo. Nota: Deberá tener en consideración la configuración de la BIOS del equipo para que el proceso de arranque comience desde el USB de instalación. Para ello deberá: - Configurar la BIOS con la opción “Legacy” para que permita el arranque mediante dispositivos USB. Esta opción es posible que sea necesario cambiarla más adelante. - Modificar el orden de arranque para que el sistema arranque desde el dispositivo USB. Tenga en consideración que tras el primer reinicio del sistema éste deberá arrancar el sistema desde el disco duro. Por lo tanto, es probable que necesite configurar de nuevo la BIOS para que el sistema no proceda a instalar de nuevo el sistema operativo. Es necesario que no se retiren los elementos de instalación hasta que se indique lo contrario en este manual. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
7.	Asegúrese, antes de iniciar el equipo, que tiene todos los dispositivos conectados y configurados de manera adecuada: – Dispositivo auto-arrancable con el sistema operativo deseado (realizado en el punto anterior). – USB o CD-ROM con los ficheros que se adjuntan a esta guía en el directorio raíz.

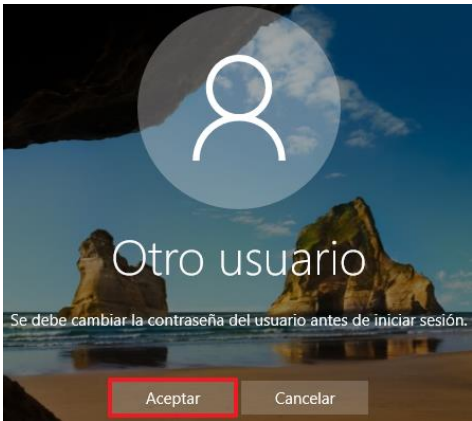
Paso	Descripción
8.	En la siguiente imagen podrá observar cómo deben estar dispuestos los ficheros que se adjuntan a esta guía dentro del directorio raíz del dispositivo.  Nota: Tenga en consideración que estos ficheros pueden ser copiados en el directorio raíz del dispositivo autoarrancable generado con la ISO del Sistema Operativo lo que supone que solo sería necesario un único dispositivo USB. El dispositivo autoarrancable junto con los ficheros que se adjuntan a este manual tendrían un aspecto similar al siguiente. 
9.	El sistema arrancará desde la unidad auto-arrancable. En primer lugar, deberá aceptar el EULA del fabricante. Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  Nota: Tenga en consideración que este procedimiento realiza un borrado del disco por lo que antes de comenzar la instalación haga una copia de seguridad de los archivos necesarios. Apague el equipo en este punto si fuera necesario.

Paso	Descripción
10.	A continuación, el proceso de instalación desatendida comenzará. 
11.	El equipo se reiniciará varias veces durante la instalación. Recuerde no extraer ninguno de los dispositivos conectados a éste, ya que si lo hace antes de que se indique en este manual la aplicación de seguridad del sistema no se completará. Deberá configurar la BIOS, si es necesario, para que el arranque después del primer reinicio se realice desde el disco duro del equipo. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
12.	Durante la instalación aparecerán diferentes pantallas que estarán personalizando y aplicando seguridad en el equipo. No pulse ninguna tecla durante todo el proceso, de lo contrario podría interrumpir el proceso y será necesario empezar de nuevo. 
13.	El equipo iniciará sesión una primera vez de forma automática y continuará importando la seguridad al equipo. Nota: Dependiendo de la velocidad del equipo es posible que el tiempo de configuración del equipo varíe. Si está implementando un servidor miembro de dominio para una red clasificada continúe con el siguiente paso. En caso contrario vaya al paso “16”.

Paso	Descripción
14.	La primera vez que se muestra el escritorio aparecerá una consola que muestra el progreso de la importación de seguridad en el sistema.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. En caso de aparecer el mensaje “Error 3: El sistema no puede encontrar la ruta especificada.”, ignórela y no cancele la aplicación de seguridad en el equipo.  Adicionalmente si apareciese el siguiente error durante el despliegue en alguno de los sistemas, ignórela y continúe. 
15.	El equipo reiniciará de nuevo y continuará con la aplicación de seguridad en el sistema. 

Paso	Descripción
16.	A continuación, aparecerá una consola que configurará el nombre y el direccionamiento IP del equipo. Cuando termine el equipo se reiniciará de nuevo automáticamente. 
17.	Tras el reinicio, se mostrará de nuevo una ventana en la que se muestra el progreso de aplicación de seguridad en el sistema. Este proceso solo será necesario en el caso de un servidor que pertenezca a una red clasificada. Si no es su situación continúe con el siguiente paso.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. Ignore el mensaje “No se pudo encontrar C:\Windows\inf\sceregvl.inf.orig” en caso de que apareciese.

Paso	Descripción
18.	Posteriormente, se procederá a la unión del servidor al dominio. Para ello, introduzca las credenciales de un usuario de dominio con privilegios para unir equipos a dominio y pulse “Aceptar”.  Nota: Si introduce las credenciales de forma errónea, copie la carpeta de recursos “Scripts” a “C:\” y ejecute el script “CCN-STIC-570A Servidor Miembro - Paso 1 - Unir a Dominio.bat” para unir el equipo al dominio.
19.	Para finalizar, el equipo se reiniciará para su posterior unión a dominio aplicándose las diferentes directivas de seguridad al sistema. 
20.	Cuando el sistema se inicie, pulse “Aceptar” en el siguiente mensaje.  Nota: Este mensaje solo aparecerá en el caso de haber configurado un servidor miembro para un entorno de red clasificada.

Paso	Descripción
21.	Introduzca las credenciales del usuario predefinido para este proceso e inicie sesión. Las credenciales para iniciar sesión localmente son: – Usuario: Administrador – Contraseña: Password_1234 
	Nota: En el caso de sistemas operativos servidor el usuario con el que se debe iniciar sesión es el “Administrador”. El usuario puede haber sido renombrado por la aplicación de seguridad en el equipo y definido por el nombre de la guía que se le aplica. Por ejemplo, en el caso de Windows Server 2016 el usuario “Administrador” se renombra como “aCdCmN570”.
22.	Debido a que se trata del primer inicio de sesión que no es desatendido, deberá establecer las credenciales para el usuario. Pulse “Aceptar” para comenzar el proceso. 

Paso	Descripción
23.	Introduzca sus nuevas credenciales y pulse “→”.  Nota: Recuerde que la nueva contraseña debe cumplir con los requisitos de longitud y complejidad establecidos.
24.	Una vez cambiada la contraseña de administrador local, puede iniciar sesión con una cuenta de dominio.
25.	Adicionalmente, revise el documento de seguridad codificado como “CCN-STIC-570A” que hace referencia al sistema operativo que está instalando para verificar la configuración aplicada y realizar aquellas acciones manuales que no pueden ser automatizadas como, por ejemplo, la configuración de las tarjetas de red del dispositivo.

ANEXO A.3. GUÍA PASO A PASO SERVIDOR INDEPENDIENTE DE FORMA DESATENDIDA

Este punto se recoge el procedimiento para automatizar la instalación y aplicación de seguridad en Windows Server 2016 con la función de servidor independiente para todos los diferentes grados de clasificación de la guía CCN-STIC-570B.

Esta guía incorpora todos archivos de automatización necesarios para cumplir con las directrices de seguridad marcadas en la guía CCN-STIC-570B.

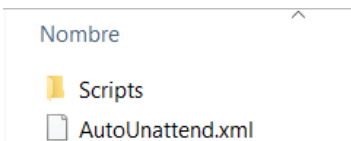
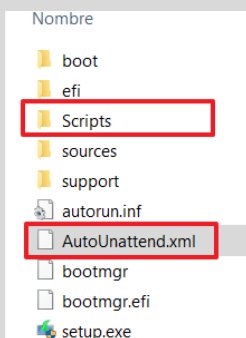
Una vez generado el dispositivo extraíble auto-arrancable, deberá seguir los siguientes pasos para desplegar el sistema operativo correspondiente a la imagen seleccionada en el equipo deseado. Este proceso eliminará el contenido del disco duro del equipo.

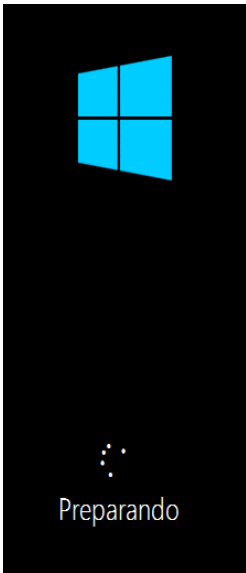
Adicionalmente deberá tener conectado un USB o un CD-ROM el cual posea en su directorio raíz los ficheros que se adjuntan a esta guía.

Antes de realizar el despliegue de la imagen del sistema operativo, se recomienda configurar la BIOS del sistema para deshabilitar los dispositivos conectados que no sean necesarios con el fin de prevenir la instalación de los drivers de dichos dispositivos en el sistema operativo durante el proceso de despliegue.

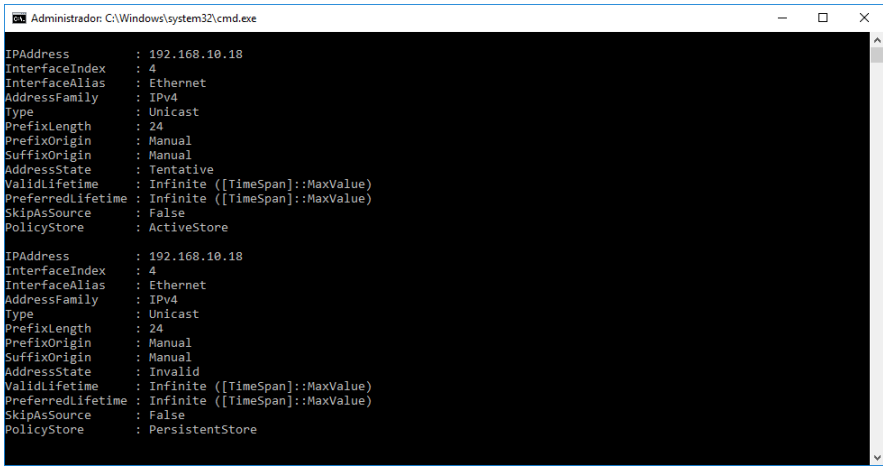
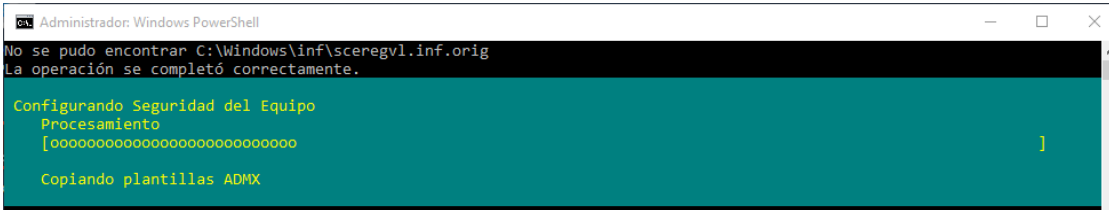
Nota: Tenga en consideración que el presente despliegue está pensado para un sistema operativo con instalación en castellano, por lo que, si la imagen ISO utilizada para este despliegue no posee dicho idioma, la aplicación del procedimiento de bastionado del sistema no se realizará adecuadamente.

Paso	Descripción
1.	Introduzca el USB de instalación que ha creado en el apartado “4.1.CREACIÓN DE DISPOSITIVO EXTRAIBLE AUTO-ARRANCABLE” en el equipo en el que desee desplegar la imagen del sistema operativo y arranque el equipo. Nota: Deberá tener en consideración la configuración de la BIOS del equipo para que el proceso de arranque comience desde el USB de instalación. Para ello deberá: - Configurar la BIOS con la opción “Legacy” para que permita el arranque mediante dispositivos USB. Esta opción es posible que sea necesario cambiarla más adelante. - Modificar el orden de arranque para que el sistema arranque desde el dispositivo USB. Tenga en consideración que tras el primer reinicio del sistema éste deberá arrancar el sistema desde el disco duro. Por lo tanto, es probable que necesite configurar de nuevo la BIOS para que el sistema no proceda a instalar de nuevo el sistema operativo. Es necesario que no se retiren los elementos de instalación hasta que se indique lo contrario en este manual. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
2.	Asegúrese, antes de iniciar el equipo, que tiene todos los dispositivos conectados y configurados de manera adecuada: – Dispositivo auto-arrancable con el sistema operativo deseado (realizado en el punto anterior). – USB o CD-ROM con los ficheros que se adjuntan a esta guía en el directorio raíz.

Paso	Descripción
3.	En la siguiente imagen podrá observar cómo deben estar dispuestos los ficheros que se adjuntan a esta guía dentro del directorio raíz del dispositivo.  Nota: Tenga en consideración que estos ficheros pueden ser copiados en el directorio raíz del dispositivo autoarrancable generado con la ISO del Sistema Operativo lo que supone que solo sería necesario un único dispositivo USB. El dispositivo autoarrancable junto con los ficheros que se adjuntan a este manual tendrían un aspecto similar al siguiente. 
4.	El sistema arrancará desde la unidad auto-arrancable. En primer lugar, deberá aceptar el EULA del fabricante. Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  Nota: Tenga en consideración que este procedimiento realiza un borrado del disco por lo que antes de comenzar la instalación haga una copia de seguridad de los archivos necesarios. Apague el equipo en este punto si fuera necesario.

Paso	Descripción
5.	A continuación, el proceso de instalación desatendida comenzará. 
6.	El equipo se reiniciará varias veces durante la instalación. Recuerde no extraer ninguno de los dispositivos conectados a éste, ya que si lo hace antes de que se indique en este manual la aplicación de seguridad del sistema no se completará. Deberá configurar la BIOS, si es necesario, para que el arranque después del primer reinicio se realice desde el disco duro del equipo. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
7.	Durante la instalación aparecerán diferentes pantallas que estarán personalizando y aplicando seguridad en el equipo. No pulse ninguna tecla durante todo el proceso, de lo contrario podría interrumpir el proceso y será necesario empezar de nuevo. 
8.	El equipo iniciará sesión una primera vez de forma automática y continuará importando la seguridad al equipo. Nota: Dependiendo de la velocidad del equipo es posible que el tiempo de configuración del equipo varíe. Si está implementando servidor independiente para una red clasificada continúe con el siguiente paso. En caso contrario vaya al paso “10”.

Paso	Descripción
9.	La primera vez que se muestra el escritorio aparecerá una consola que muestra el progreso de la aplicación de seguridad del sistema. Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. En caso de aparecer el mensaje “Error 3: El sistema no puede encontrar la ruta especificada.”, ignórelo y no cancele la aplicación de seguridad del equipo. Adicionalmente si apareciese el siguiente error durante el despliegue en alguno de los sistemas, ignórelo y continúe.
10.	El equipo reiniciará de nuevo y continuará con la aplicación de seguridad del sistema.

Paso	Descripción
11.	A continuación, aparecerá una consola que configurará el nombre y el direccionamiento IP del equipo. Cuando termine el equipo se reiniciará de nuevo automáticamente. 
12.	Tras el reinicio, se mostrará de nuevo una ventana en la que se muestra el progreso de configuración de seguridad. Este proceso solo será necesario en el caso de un servidor independiente que pertenezca a una red clasificada. Si no es su situación continúe con el siguiente paso.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. Ignore el mensaje “No se pudo encontrar C:\Windows\inf\sceregvl.inf.orig” en caso de que apareciese.
13.	Para finalizar, el equipo se reiniciará y continuarán aplicándose las diferentes directivas de seguridad al sistema. 

Paso	Descripción
14.	Cuando finalice el proceso, el equipo se reiniciará por última vez. Inicie sesión ahora sí en el equipo ya configurado. Pulse “Aceptar” para continuar.  Nota: Este mensaje solo aparecerá en el caso de haber configurado un servidor independiente para un entorno de red clasificada.
15.	Introduzca las credenciales del usuario predefinido para este proceso e inicie sesión. Las credenciales para iniciar sesión localmente son: – Usuario: Administrador – Contraseña: Password_1234  Nota: En el caso de sistemas operativos servidor el usuario con el que se debe iniciar sesión es el “Administrador”. El usuario puede haber sido renombrado por la aplicación de seguridad en el equipo y definido por el nombre de la guía que se le aplica. Por ejemplo, en el caso de Windows Server 2016 el usuario “Administrador” se renombra como “aCdCmN570”.

Paso	Descripción
16.	Debido a que se trata del primer inicio de sesión que no es desatendido, deberá establecer las credenciales para el usuario. Pulse “Aceptar” para comenzar el proceso. 
17.	Introduzca las nuevas credenciales y pulse “→”.  Nota: Recuerde que la nueva contraseña debe cumplir con los requisitos de longitud y complejidad establecidos.
18.	Una vez cambiada la contraseña de administrador local, puede iniciar sesión con la misma.
19.	Adicionalmente, revise el documento de seguridad codificado como “CCN-STIC-570B” que hace referencia al sistema operativo que está instalando para verificar la configuración aplicada y realizar aquellas acciones manuales que no pueden ser automatizadas como, por ejemplo, la configuración de las tarjetas de red del dispositivo.

ANEXO B. IMPLEMENTACIÓN DE SEGURIDAD DESATENDIDA EN MS WINDOWS 10

Este anexo ha sido diseñado para ayudar a los operadores a desplegar distintas configuraciones de seguridad de forma desatendida. A continuación, se describe, paso a paso, como implementar las diferentes configuraciones de seguridad atendiendo al Esquema Nacional de Seguridad y a entornos clasificados.

Esta guía incorpora todos los ficheros y scripts de configuración para poder realizar un despliegue automatizado atendiendo a los estándares de seguridad definidos en las diferentes categorías del ENS así como en las guías orientadas a redes clasificadas.

ANEXO B.1. GUÍA PASO A PASO WINDOWS 10 MIEMBRO DE DOMINIO DE FORMA DESATENDIDA

Este punto se recoge el procedimiento para automatizar la instalación y aplicación de seguridad en Windows 10 miembro de dominio para todos los diferentes grados de clasificación de la guía CCN-STIC-599A18.

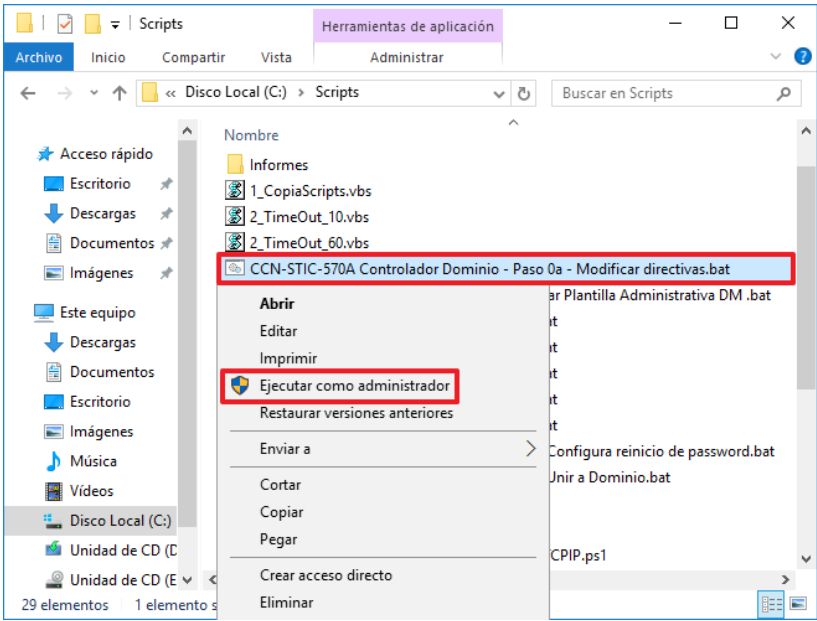
Esta guía incorpora todos archivos de automatización necesarios para cumplir con las directrices de seguridad marcadas en la guía CCN-STIC-599A18.

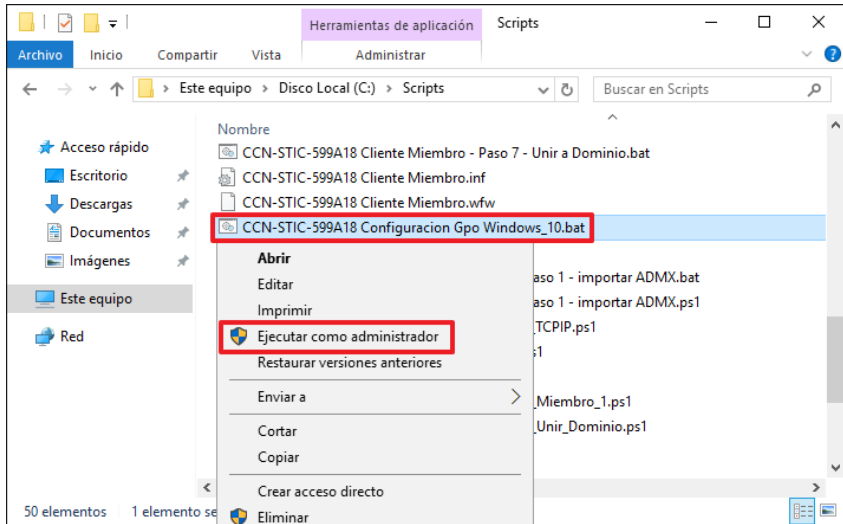
1. PREPARACIÓN DEL DOMINIO

Antes del despliegue desatendido del servidor miembro, es necesario la creación de la unidad organizativa donde se aplicará la seguridad del servidor miembro en el controlador de dominio al que vaya a permanecer dicho equipo.

Siga el siguiente paso a paso para la creación de las directivas de seguridad (GPO) de forma automatizada en el controlador de dominio.

Nota: Si previamente ya ha configurado las directivas de seguridad correspondientes a Windows 10 siguiendo la guía CCN-STIC 599A18, puede saltar al punto **2.DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA**.

Paso	Descripción
20.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad.
21.	Copie los recursos de dicha guía en la ruta "C:\\".
22.	Diríjase a la carpeta de recursos "Scripts" y ejecute con privilegios de administrador el script "CCN-STIC-570A Controlador Dominio - Paso 0a - Modificar directivas.bat".  Nota: Solo deberá ejecutar este paso en el caso de que esté implementando un Windows 10 miembro del dominio orientado a una red clasificada (CCN-STIC-599A18 - Anexo B). De no ser así vaya al paso siguiente.

Paso	Descripción
23.	Diríjase a la carpeta de recursos “Scripts” y ejecute con privilegios de administrador el script “CCN-STIC-599A18 Configuración Gpo Windows 10 Categoría [su_categoria].bat”.  Nota: Al ejecutar el script se creará la unidad organizativa “Servidores” con sus respectivas directivas de seguridad. Si ya están creadas, la ejecución del script fallará, con lo que podrá continuar con el siguiente punto de la guía. El nombre del fichero variará dependiendo de la categoría a implementar pudiendo existir las siguientes variantes: - CCN-STIC-599A18_Configuración Gpo Windows 10 ENS Categoría Básica: corresponde con la aplicación de la categoría básica según las especificaciones del ENS. - CCN-STIC-599A18_Configuración Gpo Windows 10 ENS Categoría Media: corresponde con la aplicación de la categoría media según las especificaciones del ENS. - CCN-STIC-599A18_Configuración Gpo Windows 10 ENS Categoría alta – DL: corresponde con la aplicación de la categoría alta/difusión limitada según las especificaciones del ENS. - CCN-STIC-599A18 Configuración Gpo Windows 10: corresponde con la aplicación de las medidas de seguridad de un Windows 10 miembro del dominio dedicado a una red clasificada.
24.	Finalmente, compruebe que se ha creado correctamente la unidad organizativa “Servidores” y su GPO correspondiente en el “Administrador de directivas de grupo”. Así mismo configure el objeto GPO para que la aplicación del mismo se realice sobre los servidores deseados.

2. DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA

Una vez generado el dispositivo extraíble auto-arrancable, deberá seguir los siguientes pasos para desplegar el sistema operativo correspondiente a la imagen seleccionada en el equipo deseado. Este proceso eliminará el contenido del disco duro del equipo.

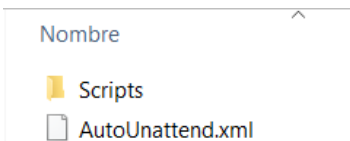
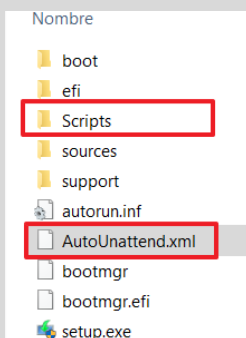
Adicionalmente deberá tener conectado un USB o un CD-ROM el cual posea en su directorio raíz los ficheros que se adjuntan a esta guía.

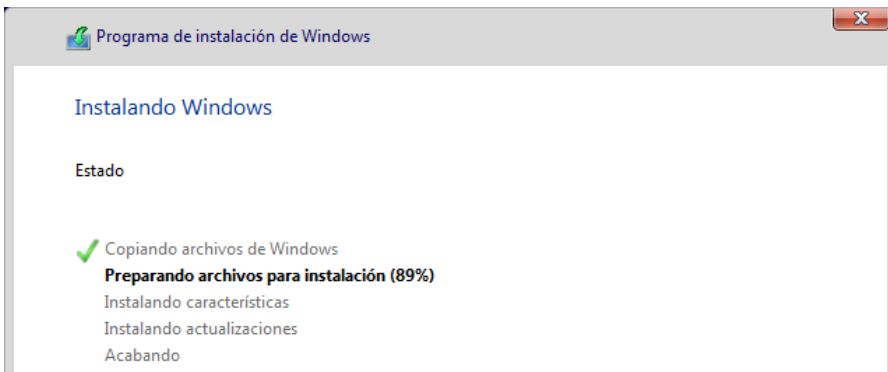
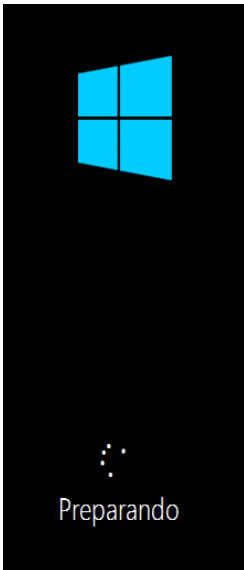
Antes de realizar el despliegue de la imagen del sistema operativo, se recomienda configurar la BIOS del sistema para deshabilitar los dispositivos conectados que no sean necesarios con el

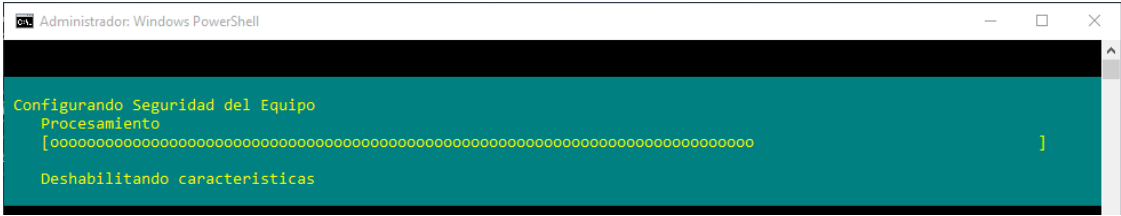
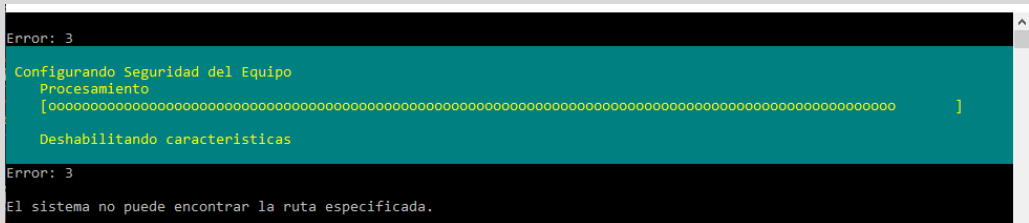
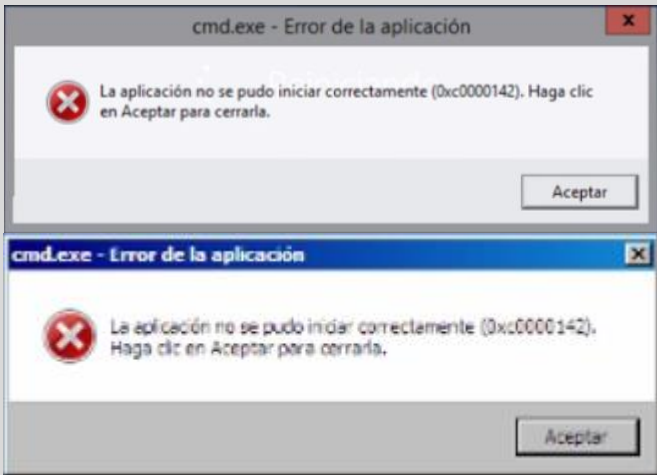
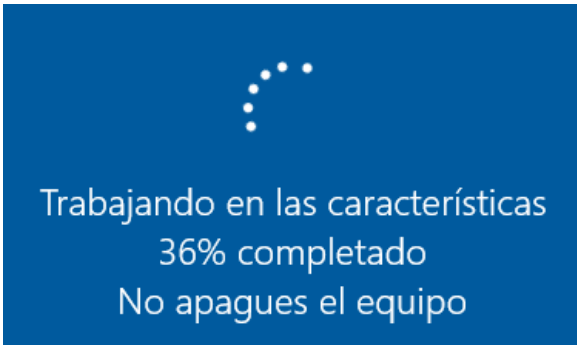
fin de prevenir la instalación de los drivers de dichos dispositivos en el sistema operativo durante el proceso de despliegue.

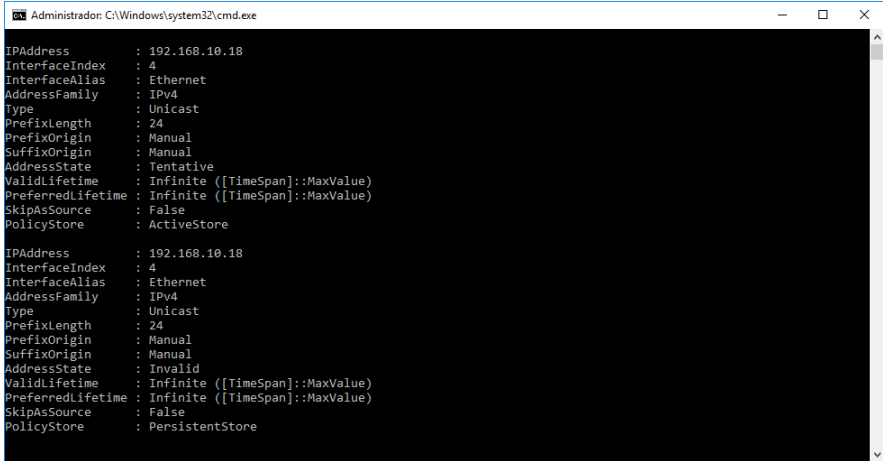
Nota: Tenga en consideración que el presente despliegue está pensado para un sistema operativo con instalación en castellano, por lo que, si la imagen ISO utilizada para este despliegue no posee dicho idioma, la aplicación del procedimiento de bastionado del sistema no se realizará adecuadamente.

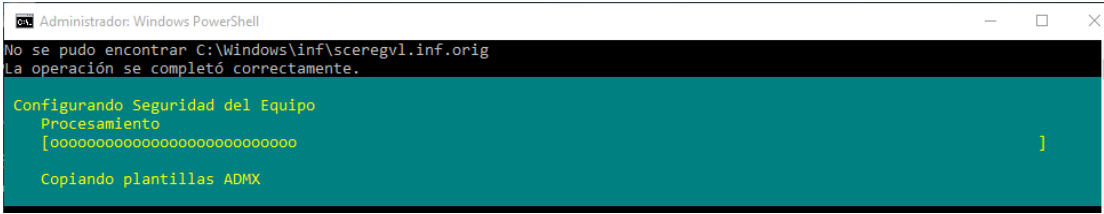
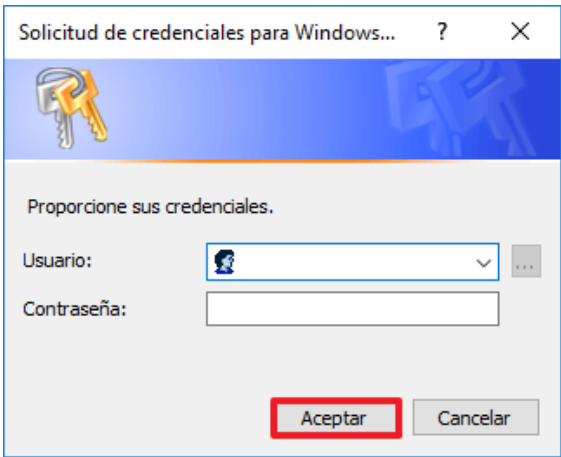
Paso	Descripción
1.	Introduzca el USB de instalación que ha creado en el apartado “4.1.CREACIÓN DE DISPOSITIVO EXTRAIBLE AUTO-ARRANCABLE” en el equipo en el que desee desplegar la imagen del sistema operativo y arranque el equipo. Nota: Deberá tener en consideración la configuración de la BIOS del equipo para que el proceso de arranque comience desde el USB de instalación. Para ello deberá: - Configurar la BIOS con la opción “Legacy” para que permita el arranque mediante dispositivos USB. Esta opción es posible que sea necesario cambiarla más adelante. - Modificar el orden de arranque para que el sistema arranque desde el dispositivo USB. Tenga en consideración que tras el primer reinicio del sistema éste deberá arrancar el sistema desde el disco duro. Por lo tanto, es probable que necesite configurar de nuevo la BIOS para que el sistema no proceda a instalar de nuevo el sistema operativo. Es necesario que no se retiren los elementos de instalación hasta que se indique lo contrario en este manual. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
2.	Asegúrese, antes de iniciar el equipo, que tiene todos los dispositivos conectados y configurados de manera adecuada: – Dispositivo auto-arrancable con el sistema operativo deseado (realizado en el punto anterior). – USB o CD-ROM con los ficheros que se adjuntan a esta guía en el directorio raíz.

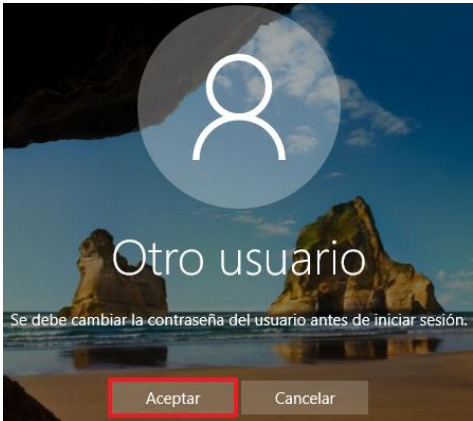
Paso	Descripción
3.	En la siguiente imagen podrá observar cómo deben estar dispuestos los ficheros que se adjuntan a esta guía dentro del directorio raíz del dispositivo.  Nota: Tenga en consideración que estos ficheros pueden ser copiados en el directorio raíz del dispositivo autoarrancable generado con la ISO del Sistema Operativo lo que supone que solo sería necesario un único dispositivo USB. El dispositivo autoarrancable junto con los ficheros que se adjuntan a este manual tendrían un aspecto similar al siguiente. 
4.	El sistema arrancará desde la unidad auto-arrancable. En primer lugar, deberá aceptar el EULA del fabricante. Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  Nota: Tenga en consideración que este procedimiento realiza un borrado del disco por lo que antes de comenzar la instalación haga una copia de seguridad de los archivos necesarios. Apague el equipo en este punto si fuera necesario.

Paso	Descripción
5.	A continuación, el proceso de instalación desatendida comenzará. 
6.	El equipo se reiniciará varias veces durante la instalación. Recuerde no extraer ninguno de los dispositivos conectados a éste, ya que si lo hace antes de que se indique en este manual la aplicación de seguridad del sistema no se completará. Deberá configurar la BIOS, si es necesario, para que el arranque después del primer reinicio se realice desde el disco duro del equipo. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
7.	Durante la instalación aparecerán diferentes pantallas que estarán personalizando y aplicando seguridad en el equipo. No pulse ninguna tecla durante todo el proceso, de lo contrario podría interrumpir el proceso y será necesario empezar de nuevo. 
8.	El equipo iniciará sesión una primera vez de forma automática y continuará importando la seguridad al equipo. Nota: Dependiendo de la velocidad del equipo es posible que el tiempo de configuración del equipo varíe. Si está implementando un controlador de dominio para una red clasificada continúe con el siguiente paso. En caso contrario vaya al paso “14”.

Paso	Descripción
9.	La primera vez que se muestra el escritorio aparecerá una consola que muestra el progreso de la importación de seguridad en el sistema.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. En caso de aparecer el mensaje “Error 3: El sistema no puede encontrar la ruta especificada.”, ignórela y no cancele la aplicación de seguridad en el equipo.  Adicionalmente si apareciese el siguiente error durante el despliegue en alguno de los sistemas, ignórela y continúe. 
10.	El equipo reiniciará de nuevo y continuará con la aplicación de seguridad en el sistema. 

Paso	Descripción
11.	A continuación, aparecerá una consola que configurará el nombre y el direccionamiento IP del equipo. Cuando termine el equipo se reiniciará de nuevo automáticamente. 
12.	Se iniciará de nuevo sesión en el sistema de manera automática y continuará el proceso.  Nota: El número de reinicios dependerá del sistema operativo instalado y las necesidades de éste. En cualquiera de las casuísticas, cuando la aplicación de seguridad del equipo haya finalizado se pedirá al usuario que inicie sesión y no antes de que el proceso finalice.

Paso	Descripción
13.	Tras el reinicio, se mostrará de nuevo una ventana en la que se muestra el progreso de aplicación de seguridad en el sistema. Este proceso solo será necesario en el caso de un servidor que pertenezca a una red clasificada. Si no es su situación continúe con el siguiente paso.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. Ignore el mensaje “No se pudo encontrar C:\Windows\inf\sceregvl.inf.orig” en caso de que apareciese.
14.	A continuación, se procederá a la unión del servidor al dominio. Para ello, introduzca las credenciales de un usuario de dominio con privilegios para unir equipos a dominio y pulse “Aceptar”.  Nota: Si introduce las credenciales de forma errónea, copie la carpeta de recursos “Scripts” a “C:\” y ejecute el script “CCN-STIC-599A18_Windows_10_Ent_2016LTSB_Unir_Dominio.ps1” para unir el equipo al dominio.
15.	Para finalizar, el equipo se reiniciará para su posterior unión a dominio aplicándose las diferentes directivas de seguridad al sistema. 

Paso	Descripción
16.	Cuando el sistema se inicie, pulse “Aceptar” en el siguiente mensaje.  Nota: Este mensaje solo aparecerá en el caso de haber configurado un cliente miembro para un entorno de red clasificada.
17.	Introduzca las credenciales del usuario predefinido para este proceso e inicie sesión. Las credenciales para iniciar sesión localmente son: Usuario: Despliegue Contraseña: Password_1234 
18.	Debido a que se trata del primer inicio de sesión que no es desatendido, deberá establecer las credenciales para el usuario. Pulse “Aceptar” para comenzar el proceso. 

Paso	Descripción
19.	Introduzca sus nuevas credenciales y pulse “→”.  Nota: Recuerde que la nueva contraseña debe cumplir con los requisitos de longitud y complejidad establecidos.
20.	Una vez cambiada la contraseña de administrador local, puede iniciar sesión con una cuenta de dominio.
21.	Adicionalmente, revise el documento de seguridad codificado como “CCN-STIC-599A18” que hace referencia al sistema operativo que está instalando para verificar la configuración aplicada y realizar aquellas acciones manuales que no pueden ser automatizadas como, por ejemplo, la configuración de las tarjetas de red del dispositivo.

ANEXO B.2. GUÍA PASO A PASO WINDOWS 10 INDEPENDIENTE DE FORMA DESATENDIDA

Este punto se recoge el procedimiento para automatizar la instalación y aplicación de seguridad en Windows 10 independiente para todos los diferentes grados de clasificación de la guía CCN-STIC-599B18.

Esta guía incorpora todos archivos de automatización necesarios para cumplir con las directrices de seguridad marcadas en la guía CCN-STIC-599B18.

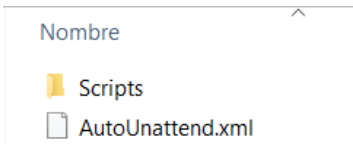
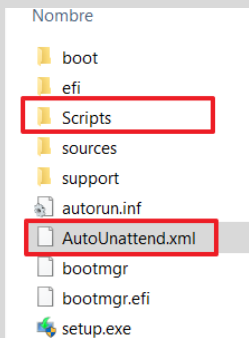
Una vez generado el dispositivo extraíble auto-arrancable, deberá seguir los siguientes pasos para desplegar el sistema operativo correspondiente a la imagen seleccionada en el equipo deseado. Este proceso eliminará el contenido del disco duro del equipo.

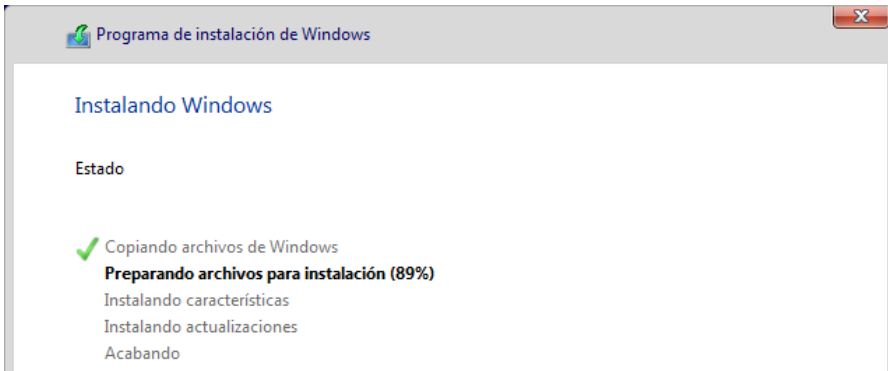
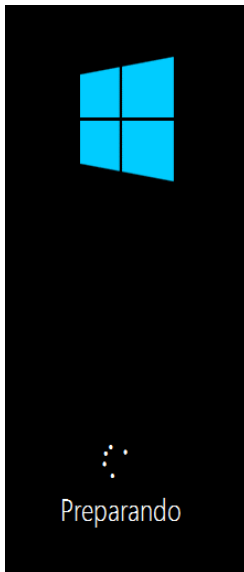
Adicionalmente deberá tener conectado un USB o un CD-ROM el cual posea en su directorio raíz los ficheros que se adjuntan a esta guía.

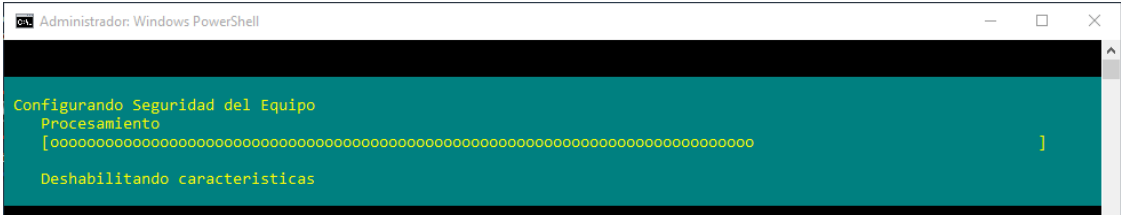
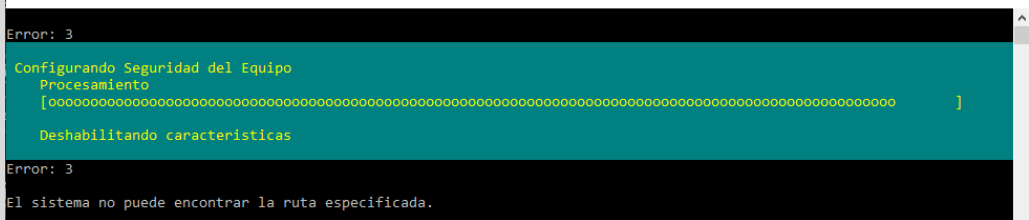
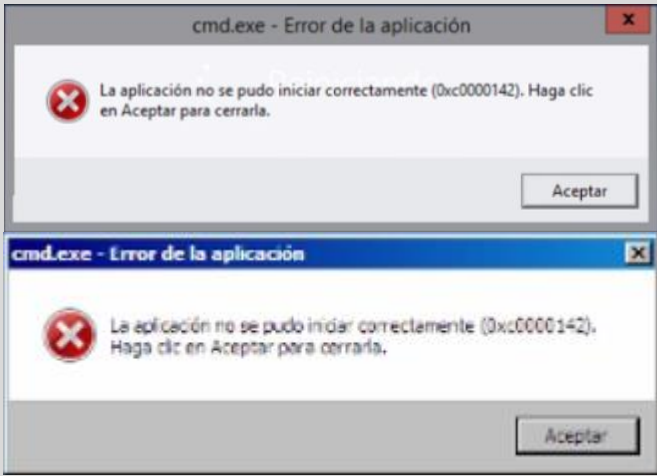
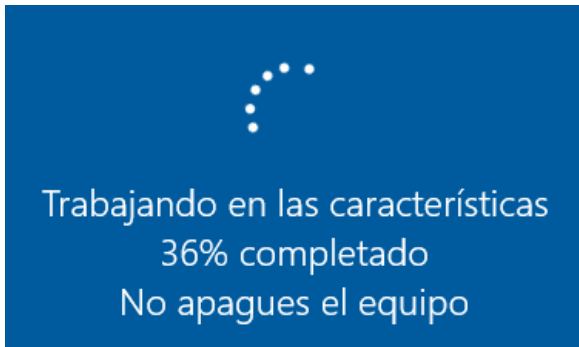
Antes de realizar el despliegue de la imagen del sistema operativo, se recomienda configurar la BIOS del sistema para deshabilitar los dispositivos conectados que no sean necesarios con el fin de prevenir la instalación de los drivers de dichos dispositivos en el sistema operativo durante el proceso de despliegue.

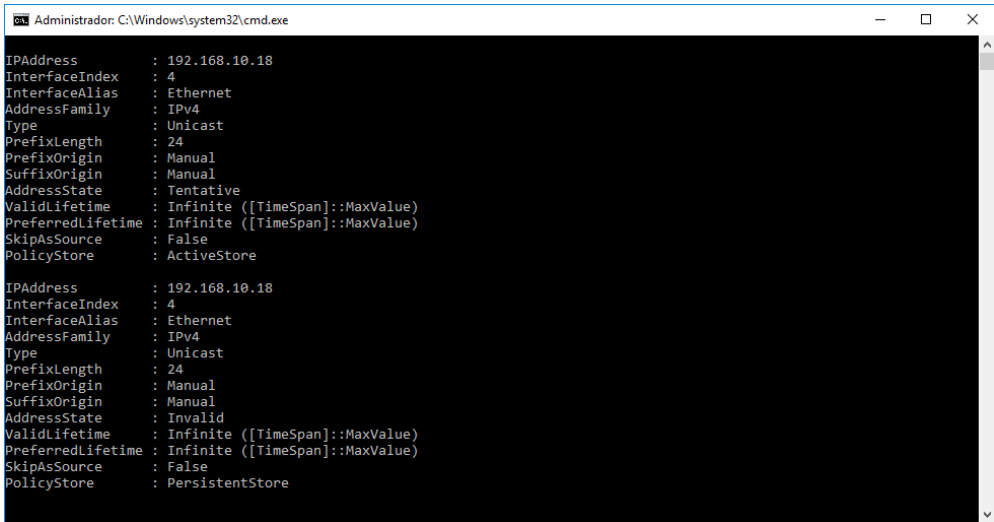
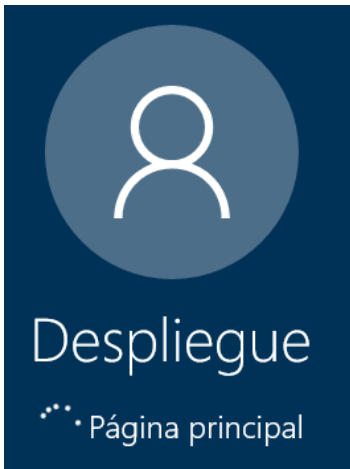
Nota: Tenga en consideración que el presente despliegue está pensado para un sistema operativo con instalación en castellano, por lo que, si la imagen ISO utilizada para este despliegue no posee dicho idioma, la aplicación del procedimiento de bastionado del sistema no se realizará adecuadamente.

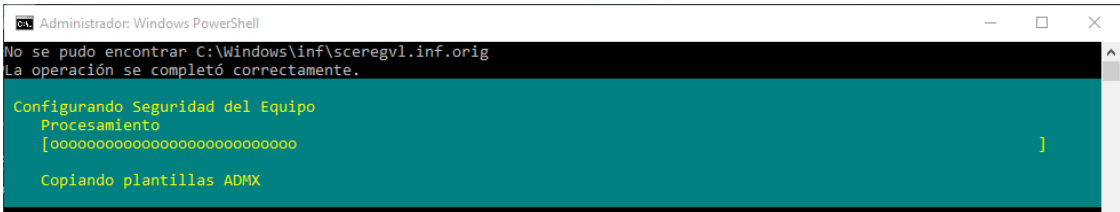
Paso	Descripción
1.	Introduzca el USB de instalación que ha creado en el apartado “4.1.CREACIÓN DE DISPOSITIVO EXTRAIBLE AUTO-ARRANCABLE” en el equipo en el que desee desplegar la imagen del sistema operativo y arranque el equipo. Nota: Deberá tener en consideración la configuración de la BIOS del equipo para que el proceso de arranque comience desde el USB de instalación. Para ello deberá: - Configurar la BIOS con la opción “Legacy” para que permita el arranque mediante dispositivos USB. Esta opción es posible que sea necesario cambiarla más adelante. - Modificar el orden de arranque para que el sistema inicie desde el dispositivo USB. Tenga en consideración que tras el primer reinicio del sistema éste deberá arrancar el sistema desde el disco duro. Por lo tanto, es probable que necesite configurar de nuevo la BIOS para que el sistema no proceda a instalar de nuevo el sistema operativo. Es necesario que no se retiren los elementos de instalación hasta que se indique lo contrario en este manual. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
2.	Asegúrese, antes de iniciar el equipo, que tiene todos los dispositivos conectados y configurados de manera adecuada: – Dispositivo auto-arrancable con el sistema operativo deseado (realizado en el punto anterior). – USB o CD-ROM con los ficheros que se adjuntan a esta guía en el directorio raíz.

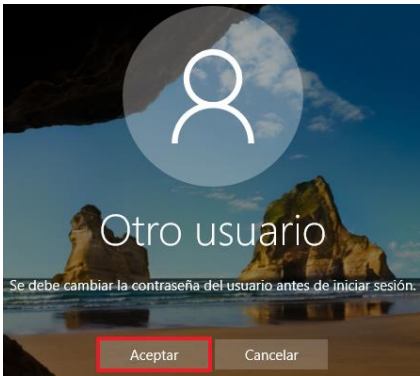
Paso	Descripción
3.	En la siguiente imagen podrá observar cómo deben estar dispuestos los ficheros que se adjuntan a esta guía dentro del directorio raíz del dispositivo.  Nota: Tenga en consideración que estos ficheros pueden ser copiados en el directorio raíz del dispositivo autoarrancable generado con la ISO del Sistema Operativo lo que supone que solo sería necesario un único dispositivo USB. El dispositivo autoarrancable junto con los ficheros que se adjuntan a este manual tendrían un aspecto similar al siguiente. 
4.	El sistema arrancará desde la unidad auto-arrancable. En primer lugar, deberá aceptar el EULA del fabricante. Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  Nota: Tenga en consideración que este procedimiento realiza un borrado del disco por lo que antes de comenzar la instalación haga una copia de seguridad de los archivos necesarios. Apague el equipo en este punto si fuera necesario.

Paso	Descripción
5.	A continuación, el proceso de instalación desatendida comenzará. 
6.	El equipo se reiniciará varias veces durante la instalación. Recuerde no extraer ninguno de los dispositivos conectados a éste, ya que si lo hace antes de que se indique en este manual la aplicación de seguridad del sistema no se completará. Deberá configurar la BIOS, si es necesario, para que el arranque después del primer reinicio se realice desde el disco duro del equipo. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
7.	Durante la instalación aparecerán diferentes pantallas que estarán personalizando y aplicando seguridad en el equipo. No pulse ninguna tecla durante todo el proceso, de lo contrario podría interrumpir el proceso y será necesario empezar de nuevo. 
8.	El equipo iniciará sesión una primera vez de forma automática y continuará implantando la seguridad en el equipo. Nota: Dependiendo de la velocidad del equipo es posible que el tiempo de configuración del equipo varíe. Si está implementando un Windows 10 para una red clasificada continúe con el siguiente paso. En caso contrario vaya al paso “11”.

Paso	Descripción
9.	La primera vez que se muestra el escritorio aparecerá una consola que muestra el progreso de la aplicación de seguridad del sistema.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. En caso de aparecer el mensaje “Error 3: El sistema no puede encontrar la ruta especificada.”, ignórela y no cancele el proceso del script.  Adicionalmente si apareciese el siguiente error durante el despliegue en alguno de los sistemas, ignórela y continúe. 
10.	El equipo se reiniciará de nuevo y continuará con la implementación de seguridad en el sistema. 

Paso	Descripción
11.	A continuación, aparecerá una consola que configurará el nombre y el direccionamiento IP del equipo. Cuando termine el equipo se reiniciará de nuevo automáticamente. 
12.	Se iniciará de nuevo sesión en el sistema de manera automática y continuará el proceso.  Nota: El número de reinicios dependerá del sistema operativo instalado y las necesidades de éste. En cualquiera de las casuísticas, cuando la aplicación de seguridad del equipo haya finalizado se pedirá al usuario que inicie sesión y no antes de que el proceso finalice.

Paso	Descripción
13.	Tras el reinicio, se mostrará de nuevo una ventana en la que se muestra el progreso de implantación de seguridad.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. Ignore el mensaje “No se puede encontrar C:\Windows\inf\sceregvl.inf.orig” en caso de que apareciese.
14.	Cuando el sistema se inicie, pulse “Aceptar” en el siguiente mensaje.  Nota: Este mensaje solo aparecerá en el caso de haber configurado un Windows 10 para un entorno de red clasificada.
15.	Introduzca las credenciales del usuario predefinido para este proceso e inicie sesión. Las credenciales para iniciar sesión son: – Usuario: Despliegue – Contraseña: Password_1234 

Paso	Descripción
16.	Debido a que se trata del primer inicio de sesión que no es desatendido, deberá establecer las credenciales para el usuario. Pulse “Aceptar” para comenzar el proceso. 
17.	Introduzca las nuevas credenciales y pulse “→”.  Nota: Recuerde que la nueva contraseña debe cumplir con los requisitos de longitud y complejidad establecidos.

Paso	Descripción
18.	Debido a que se trata del primer inicio de sesión no desatendido con la configuración de seguridad ya aplicada, es necesario pulsar “Aceptar” en el siguiente mensaje de inicio de sesión y comenzar con el siguiente punto. Despliegue (WCL10\Despliegue) Es la primera vez que inicias sesión de forma interactiva en esta cuenta. Aceptar Nota: Este mensaje solo aparecerá en el caso de haber configurado un Windows 10 para un entorno de red clasificada.
19.	Adicionalmente, revise el documento de seguridad codificado como “CCN-STIC-599B18” que hace referencia al sistema operativo que está instalando para verificar la configuración aplicada y realizar aquellas acciones manuales que no pueden ser automatizadas.

ANEXO C. IMPLEMENTACIÓN DE SEGURIDAD DESATENDIDA DE PRODUCTOS MICROSOFT EN MS WINDOWS 2016

Este anexo ha sido diseñado para ayudar a los operadores a desplegar distintas configuraciones de seguridad de forma desatendida. A continuación, se describe, paso a paso, como implementar las diferentes configuraciones de seguridad atendiendo al Esquema Nacional de Seguridad y a entornos clasificados.

Esta guía incorpora todos los ficheros y scripts de configuración para poder realizar un despliegue automatizado atendiendo a los estándares de seguridad definidos en las diferentes categorías del ENS así como en las guías orientadas a redes clasificadas.

ANEXO C.1. GUÍA PASO A PASO INSTALACIÓN PRODUCTOS DE FORMA DESATENDIDA

Este apartado recoge el procedimiento para automatizar la instalación y aplicación de seguridad sobre Windows Server 2016 como servidor miembro junto a la función de servidor de impresión o servidor de ficheros.

Esta guía incorpora todos archivos de automatización necesarios para cumplir con las directrices de seguridad marcadas en la guía de servidor de impresión CCN-STIC-572 y en la guía servidor de ficheros CCN-STIC-573.

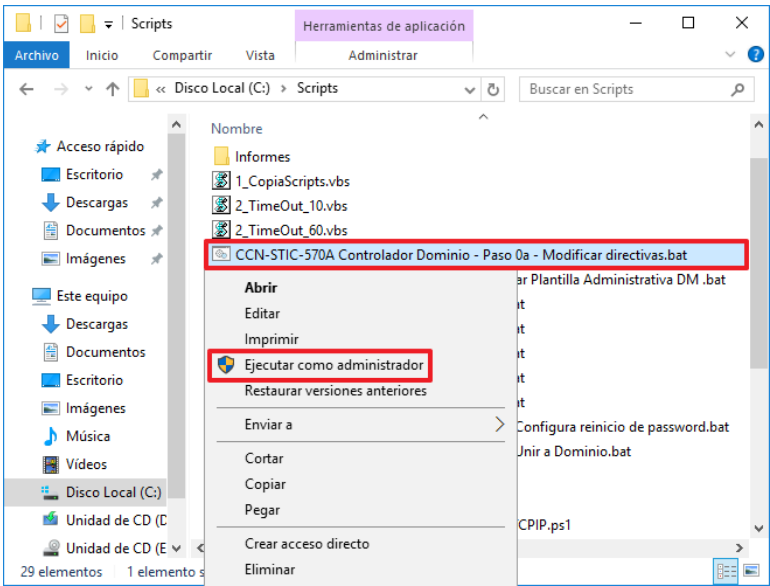
1. PREPARACIÓN DEL DOMINIO

Antes del despliegue desatendido del servidor miembro como rol, es necesario la creación de la unidad organizativa donde se aplicará la seguridad del servidor miembro en el controlador de dominio al que vaya a permanecer dicho equipo.

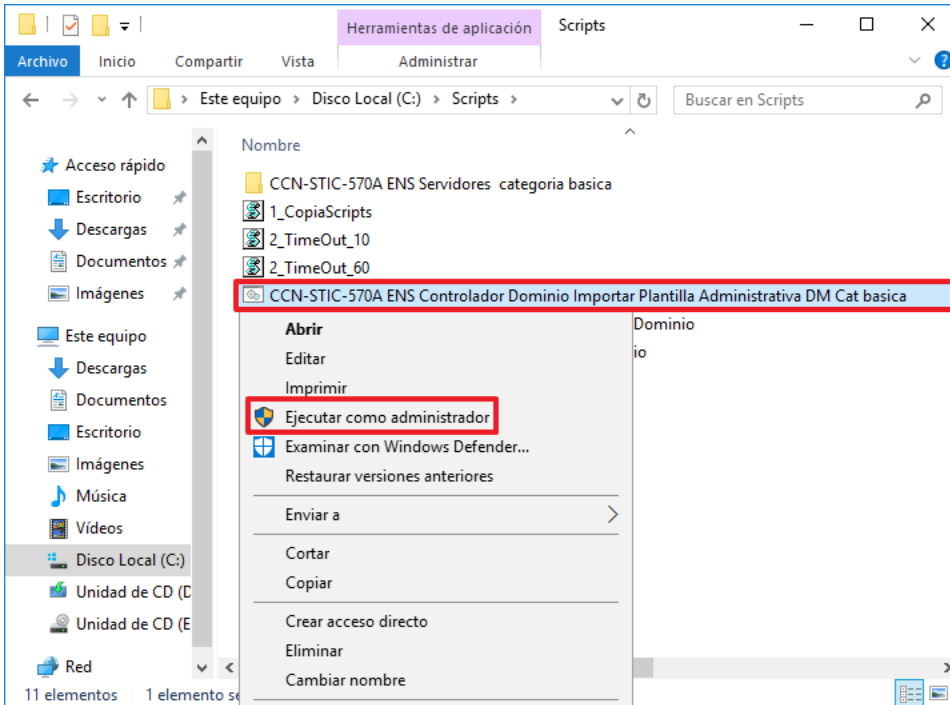
Siga el siguiente paso a paso para la creación de las directivas de seguridad (GPO) de forma automatizada en el controlador de dominio.

Nota: Si previamente ya ha configurado las directivas de seguridad correspondientes a un servidor miembro siguiendo la guía CCN-STIC 570A, puede saltar al punto 2.DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA.

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad.
2.	Copie los recursos de dicha guía en la ruta "C:\\".
3.	Diríjase a la carpeta de recursos "Scripts" y ejecute con privilegios de administrador el script "CCN-STIC-570A Controlador Dominio - Paso 0a - Modificar directivas.bat".



Nota: Solo deberá ejecutar este paso en el caso de que esté implementando un servidor miembro orientado a una red clasificada (CCN-STIC-570A - Anexo B). De no ser así vaya al paso siguiente.

Paso	Descripción
4.	Diríjase a la carpeta de recursos “Scripts” y ejecute con privilegios de administrador el script “CCN-STIC-570A ENS Controlador Dominio Importar Plantilla Administrativa DM Cat [su_categoria].bat”.  Nota: Al ejecutar el script se creará la unidad organizativa “Servidores” con sus respectivas directivas de seguridad. Si ya están creadas, la ejecución del script fallará, con lo que podrá continuar con el siguiente punto de la guía. El nombre del fichero variará dependiendo de la categoría y rol a implementar pudiendo existir las siguientes variantes: - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM Cat básica: corresponde con la aplicación de la categoría básica según las especificaciones del ENS. - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM Cat media: corresponde con la aplicación de la categoría media según las especificaciones del ENS. - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM Cat alta – DL: corresponde con la aplicación de la categoría alta/difusión limitada según las especificaciones del ENS. - CCN-STIC-570A Controlador Dominio Importar Plantilla Administrativa DM: corresponde con la aplicación de las medidas de seguridad de un servidor miembro dedicado a una red clasificada.
5.	Finalmente, compruebe que se ha creado correctamente la unidad organizativa “Servidores” y su GPO correspondiente en el “Administrador de directivas de grupo”. Así mismo configure el objeto GPO para que la aplicación del mismo se realice sobre los servidores deseados.

2. DESPLIEGUE DE LA CONFIGURACIÓN DE SEGURIDAD DESATENDIDA

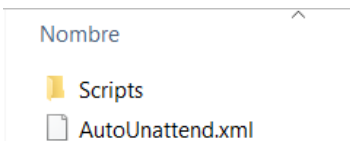
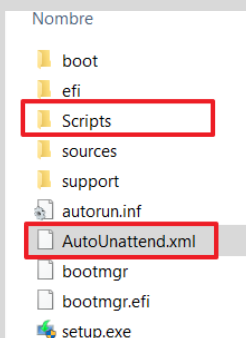
Una vez generado el dispositivo extraíble auto-arrancable, deberá seguir los siguientes pasos para desplegar el sistema operativo correspondiente a la imagen seleccionada en el equipo deseado. Este proceso eliminará el contenido del disco duro del equipo.

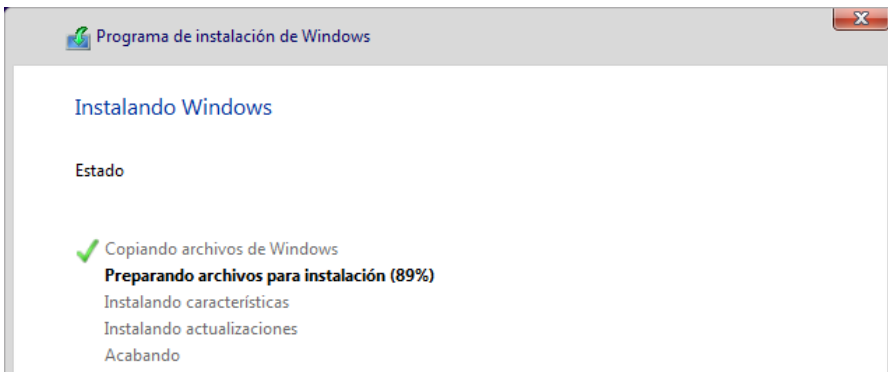
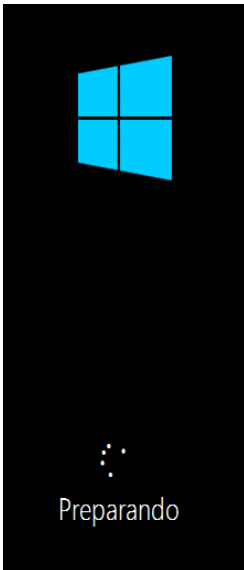
Adicionalmente deberá tener conectado un USB o un CD-ROM el cual posea en su directorio raíz los ficheros que se adjuntan a esta guía.

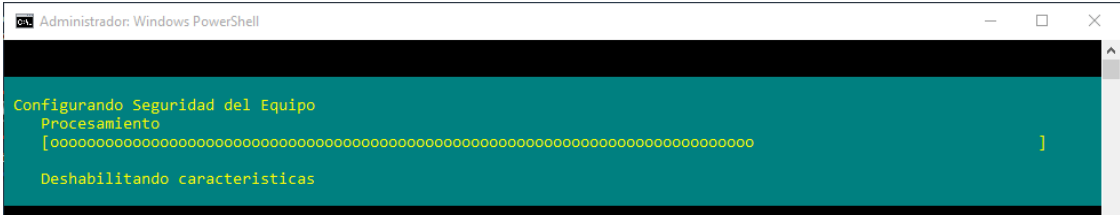
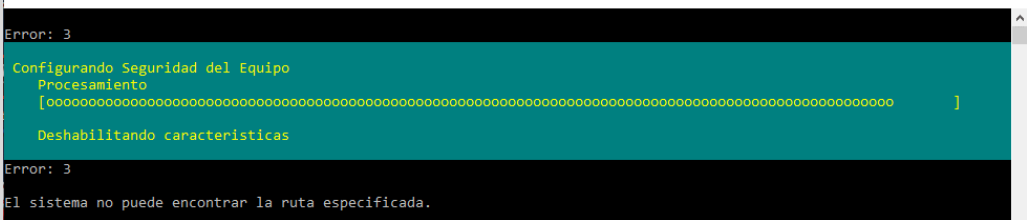
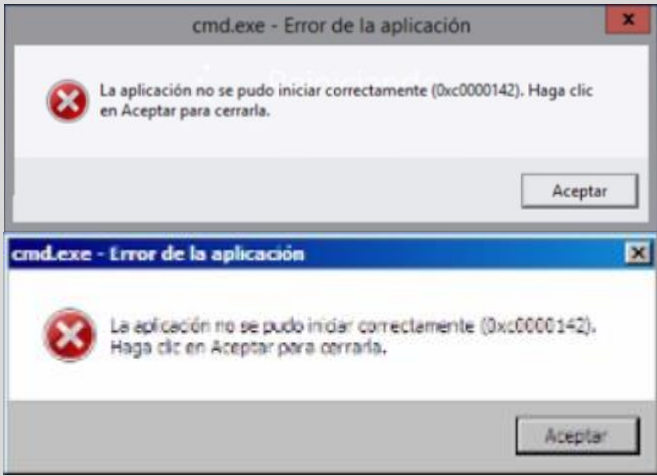
Antes de realizar el despliegue de la imagen del sistema operativo, se recomienda configurar la BIOS del sistema para deshabilitar los dispositivos conectados que no sean necesarios con el fin de prevenir la instalación de los drivers de dichos dispositivos en el sistema operativo durante el proceso de despliegue.

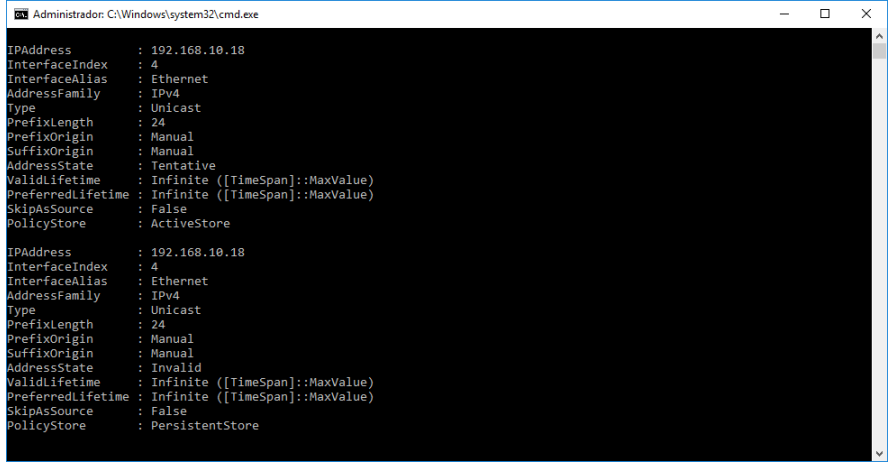
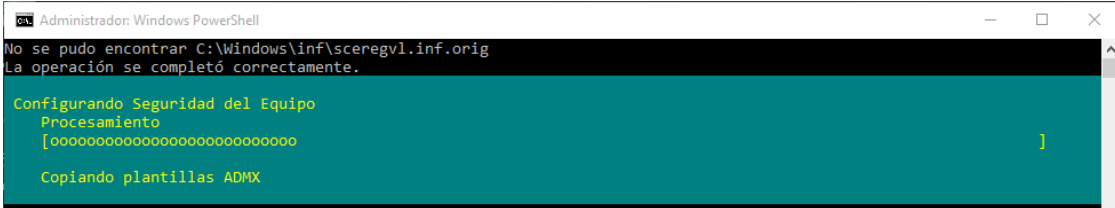
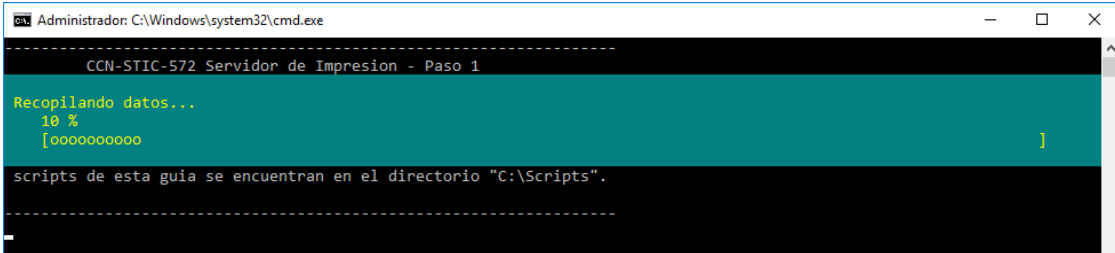
Nota: Tenga en consideración que el presente despliegue está pensado para un sistema operativo con instalación en castellano, por lo que, si la imagen ISO utilizada para este despliegue no posee dicho idioma, la aplicación del procedimiento de bastionado del sistema no se realizará adecuadamente.

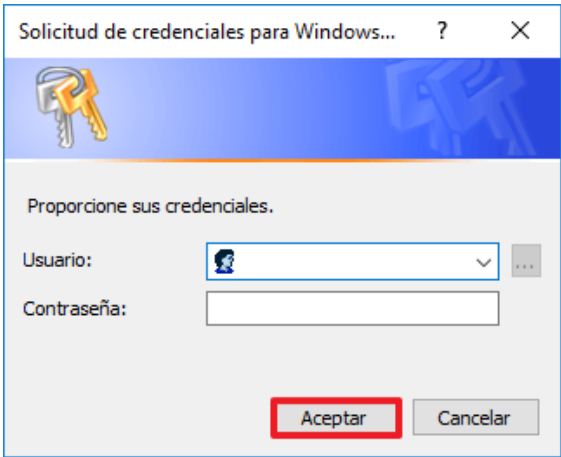
Paso	Descripción
6.	Introduzca el USB de instalación que ha creado en el apartado “4.1.CREACIÓN DE DISPOSITIVO EXTRAIBLE AUTO-ARRANCABLE” en el equipo en el que desee desplegar la imagen del sistema operativo y arranque el equipo. Nota: Deberá tener en consideración la configuración de la BIOS del equipo para que el proceso de arranque comience desde el USB de instalación. Para ello deberá: - Configurar la BIOS con la opción “Legacy” para que permita el arranque mediante dispositivos USB. Esta opción es posible que sea necesario cambiarla más adelante. - Modificar el orden de arranque para que el sistema arranque desde el dispositivo USB. Tenga en consideración que tras el primer reinicio del sistema éste deberá arrancar el sistema desde el disco duro. Por lo tanto, es probable que necesite configurar de nuevo la BIOS para que el sistema no proceda a instalar de nuevo el sistema operativo. Es necesario que no se retiren los elementos de instalación hasta que se indique lo contrario en este manual. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
7.	Asegúrese, antes de iniciar el equipo, que tiene todos los dispositivos conectados y configurados de manera adecuada: – Dispositivo auto-arrancable con el sistema operativo deseado (realizado en el punto anterior). – USB o CD-ROM con los ficheros que se adjuntan a esta guía en el directorio raíz.

Paso	Descripción
8.	En la siguiente imagen podrá observar cómo deben estar dispuestos los ficheros que se adjuntan a esta guía dentro del directorio raíz del dispositivo.  Nota: Tenga en consideración que estos ficheros pueden ser copiados en el directorio raíz del dispositivo autoarrancable generado con la ISO del Sistema Operativo lo que supone que solo sería necesario un único dispositivo USB. El dispositivo autoarrancable junto con los ficheros que se adjuntan a este manual tendrían un aspecto similar al siguiente. 
9.	El sistema arrancará desde la unidad auto-arrancable. En primer lugar, deberá aceptar el EULA del fabricante. Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  Nota: Tenga en consideración que este procedimiento realiza un borrado del disco por lo que antes de comenzar la instalación haga una copia de seguridad de los archivos necesarios. Apague el equipo en este punto si fuera necesario.

Paso	Descripción
10.	A continuación, el proceso de instalación desatendida comenzará. 
11.	El equipo se reiniciará varias veces durante la instalación. Recuerde no extraer ninguno de los dispositivos conectados a éste, ya que si lo hace antes de que se indique en este manual la aplicación de seguridad del sistema no se completará. Deberá configurar la BIOS, si es necesario, para que el arranque después del primer reinicio se realice desde el disco duro del equipo. De lo contrario, la configuración y aplicación de seguridad del sistema no se realizará de forma adecuada.
12.	Durante la instalación aparecerán diferentes pantallas que estarán personalizando y aplicando seguridad en el equipo. No pulse ninguna tecla durante todo el proceso, de lo contrario podría interrumpir el proceso y será necesario empezar de nuevo. 
13.	El equipo iniciará sesión una primera vez de forma automática y continuará importando la seguridad al equipo. Nota: Dependiendo de la velocidad del equipo es posible que el tiempo de configuración del equipo varíe. Si está implementando un servidor miembro con un rol para una red clasificada continúe con el siguiente paso. En caso contrario vaya al paso “18”.

Paso	Descripción
14.	La primera vez que se muestra el escritorio aparecerá una consola que muestra el progreso de la importación de seguridad en el sistema.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. En caso de aparecer el mensaje “Error 3: El sistema no puede encontrar la ruta especificada.”, ignórela y no cancele la aplicación de seguridad en el equipo.  Adicionalmente si apareciese el siguiente error durante el despliegue en alguno de los sistemas, ignórela y continúe. 
15.	El equipo reiniciará de nuevo y continuará con la aplicación de seguridad en el sistema.  Trabajando en las características 36% completado No apagues el equipo

Paso	Descripción
16.	A continuación, aparecerá una consola que configurará el nombre y el direccionamiento IP del equipo. Cuando termine el equipo se reiniciará de nuevo automáticamente. 
17.	Tras el reinicio, se mostrará de nuevo una ventana en la que se muestra el progreso de aplicación de seguridad en el sistema. Este proceso solo será necesario en el caso de un servidor que pertenezca a una red clasificada. Si no es su situación continúe con el siguiente paso.  Nota: No realice todavía ninguna acción sobre el equipo ya que esto podría provocar la configuración inadecuada del sistema. Ignore el mensaje “No se pudo encontrar C:\Windows\inf\sceregvl.inf.orig” en caso de que apareciese.
18.	Por último, se mostrará la instalación del rol de manera desatendida.  Nota: La imagen cambiara en función del rol que haya elegido desplegar.

Paso	Descripción
19.	Posteriormente, se procederá a la unión del servidor al dominio. Para ello, introduzca las credenciales de un usuario de dominio con privilegios para unir equipos a dominio y pulse “Aceptar”.  Nota: Si introduce las credenciales de forma errónea, copie la carpeta de recursos “Scripts” a “C:\” y ejecute el script “CCN-STIC-570A_Windows_Server_2016_Unir_Dominio.ps1” para unir el equipo al dominio.
20.	Para finalizar, el equipo se reiniciará para su posterior unión a dominio aplicándose las diferentes directivas de seguridad al sistema. 
21.	Cuando el sistema se inicie, pulse “Aceptar” en el siguiente mensaje.  Nota: Este mensaje solo aparecerá en el caso de haber configurado un servidor miembro para un entorno de red clasificada.

Paso	Descripción
22.	Introduzca las credenciales del usuario predefinido para este proceso e inicie sesión. Las credenciales para iniciar sesión localmente son: – Usuario: Administrador – Contraseña: Password_1234 
23.	Debido a que se trata del primer inicio de sesión que no es desatendido, deberá establecer las credenciales para el usuario. Pulse “Aceptar” para comenzar el proceso. 

Paso	Descripción
24.	Introduzca sus nuevas credenciales y pulse “→”.  Nota: Recuerde que la nueva contraseña debe cumplir con los requisitos de longitud y complejidad establecidos.
25.	Una vez cambiada la contraseña de administrador local, puede iniciar sesión con una cuenta de dominio.
26.	Adicionalmente, revise los documentos de seguridad codificados como “CCN-STIC-572” y “CCN-STIC-573” que hace referencia al producto en el sistema operativo que está instalando para verificar la configuración aplicada y realizar aquellas acciones manuales que no pueden ser automatizadas como, por ejemplo, la configuración de las tarjetas de red del dispositivo.