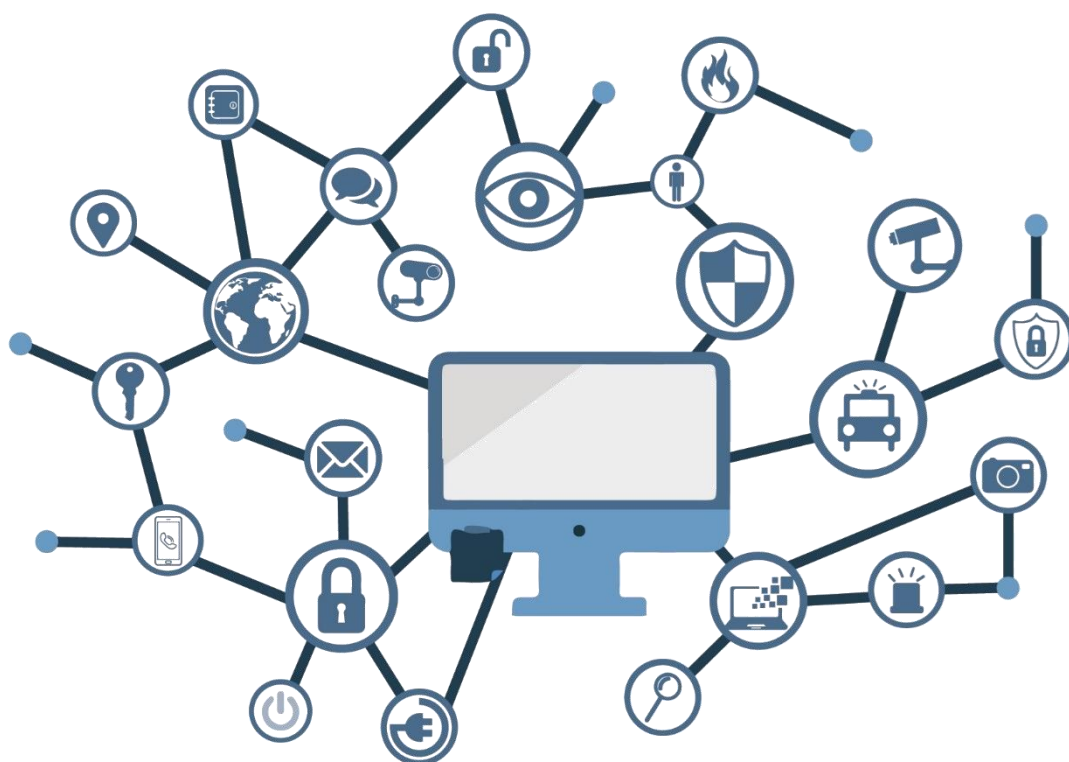


GUÍA DE APLICACIÓN DE PERFILADO DE SEGURIDAD PARA WINDOWS SERVER 2019 (CONTROLADOR DE DOMINIO O SERVIDOR MIEMBRO)





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

Edita:



P.º de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022

NIPO: 083-21-164-9

Fecha de Edición: abril de 2022

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.

cpage.mpr.gob.es

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

abril de 2022



Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN	5
2. OBJETO	5
3. ALCANCE	6
4. DESCRIPCIÓN DEL USO DE ESTA GUÍA	7
5. DECLARACIÓN DE RIESGOS	9
5.1 RIESGOS ASOCIADOS A UN SERIDOR WINDOWS SERVER 2019	10
5.2 CUANTIFICACIÓN DE PROBABILIDAD DE CADA RIESGO	11
5.3 CUANTIFICACIÓN DE IMPACTO DE CADA RIESGO	11
5.4 CUANTIFICACIÓN DE SUPERFICIE DE EXPOSICIÓN DEL SISTEMA	12
6. IDENTIFICACIÓN DE LOS VALORES DE RIESGO RESULTANTES.....	13
7. PERFILADO PARA LA APLICABILIDAD DE MEDIDAS	14
ANEXO A. PASO A PASO CONFIGURACIÓN BASE DE SEGURIDAD SOBRE WINDOWS SERVER 2019	20
ANEXO A.1. PREPARACIÓN DEL DOMINIO	20
ANEXO A.2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD	35
ANEXO A.3. CONFIGURACIONES ADICIONALES	39

1. INTRODUCCIÓN

Esta guía forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en las tecnologías y sistemas operativos de Microsoft (CCN-STIC 500), siendo de aplicación en el cumplimiento del Esquema Nacional de Seguridad (ENS) y para los sistemas que manejen información clasificada.

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

2. OBJETO

El propósito de esta guía es proporcionar los procedimientos para aplicar un perfilado de seguridad en base a un análisis de riesgos preceptivo, en sistemas que implementen servidores Windows Server 2019 y que actúen bien como servidor controlador de dominio o bien como servidor miembro de un dominio.

La configuración que se aplica a través de la presente guía se ha diseñado para adaptarse a las características específicas de cada entorno, en función de los resultados obtenidos del análisis de riesgos preceptivo. Se trata de la aproximación del MARCO MODERNO DE SEGURIDAD que desde el Centro Criptológico Nacional se persigue para una adaptación adecuada al ecosistema en cuestión, el cual basa sus pilares fundamentales en los siguientes objetivos:

- a) Las medidas a adoptar estarán condicionadas por el análisis de riesgos preceptivo de cada escenario, la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.
- b) Se tendrán en cuenta los avances tecnológicos y el estado de arte más reciente en ciberseguridad.
- c) Será adaptable en la aplicación de medidas, evitando una aplicación monolítica y estanca utilizando la Declaración de Aplicabilidad como elemento fundamental sobre el que vertebrar la seguridad en base a responsabilidad compartida.
- d) La Declaración de Aplicabilidad (conjunto de medidas a implementar) utilizarán de base los niveles del Esquema Nacional de Seguridad validados por el análisis de riesgos preceptivo utilizando de base una categorización de ENS MEDIO.
- e) Las medidas de seguridad se podrán aplicar a sistemas ya implementados o nuevos sistemas, minimizando el impacto en el entorno de producción.
- f) Las guías se revisarán y se actualizarán según las nuevas amenazas y estado de arte tecnológico en ciberseguridad.

Este marco de aplicación basado en un perfilado de seguridad tiene en consideración la diversidad de escenarios que se pueden dar, con sus particularidades, riesgos y amenazas, por lo que será cada organización que implementa las medidas de seguridad la que deba determinar qué medidas serán de aplicación, compensadas o complementadas, en función de sus condiciones específicas asumiendo una responsabilidad compartida en la puesta en operación del sistema.

Para ayudar a las organizaciones a implementar las medidas de seguridad, se ha considerado la necesidad de crear tres (3) alcances de implementación:

- a) Alcance BÁSICO.
- b) Alcance INTERMEDIO.
- c) Alcance AVANZADO.

Para la elaboración de esta guía, se ha hecho un esfuerzo de revisión exhaustiva de las distintas configuraciones de seguridad disponibles en Windows Server 2019, alineándolas y clasificándolas en función de los riesgos que cada una de ellas mitigan o abordan individualmente.

De esta forma, se pretende dar mayor coherencia a conjunto de medidas resultantes o perfilado de seguridad, siendo necesario aplicar únicamente aquellas medidas que realmente atienden a un riesgo declarado en función de los niveles de alcance señalados anteriormente.

Se trata de implementar medidas con un criterio claro, conociendo los riesgos, el contexto de la amenaza y la superficie de exposición de cada sistema en particular, y adaptando las medidas de seguridad a aplicar en función de ello.

3. ALCANCE

Para ayudar a las organizaciones a identificar los riesgos de seguridad y por lo tanto realizar el perfilado correspondiente para cada uno de sus sistemas, se ha incorporado a esta guía un apartado denominado declaración de riesgos donde se identifican y se explican los principales riesgos del producto o tecnología de que trata la guía.

Esta guía se ha elaborado con el objetivo de proporcionar información específica sobre los riesgos y las medidas de mitigación recomendadas para los escenarios planteados. En particular, se incluirá la configuración para aplicar un perfilado de seguridad de un servidor con “Windows Server 2019”, instalado en español con la versión completa del producto, bien actuando con el rol de controlador de dominio o bien como servidor miembro de un dominio.

Para garantizar la seguridad de los clientes y servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Microsoft Update. Las actualizaciones, por lo general, se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento.

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

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

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

Esta guía incluye:

- a) Descripción de uso de esta guía. Breve explicación acerca de los pasos a seguir para identificar, seleccionar y aplicar las medidas de seguridad recomendadas.
- b) Declaración de riesgos. En esta sección se identifican los principales riesgos asociados al producto o tecnología del que trata la guía CCN-STIC. Por ejemplo, un servicio web puede tener riesgos relacionados con el acceso remoto, mientras que un controlador de dominio puede tener riesgos relacionados con los procesos de autenticación. La organización podrá hacer uso de los riesgos identificados en este punto y añadir los que considere necesarios para su escenario en particular.
- c) Identificación de valor de riesgo. En esta sección se muestran una serie de tablas o mapas de calor, con tres (3) niveles de superficie de exposición y los valores de riesgo resultantes de la intersección de los niveles de impacto y probabilidad. Se trata de una muestra de cómo alterando alguna de estas variables (superficie de exposición, impacto y probabilidad), los resultados del riesgo se adecúan a cada realidad.
- d) Perfilado de seguridad. En este punto se establecen las medidas de seguridad que se deberán aplicar al producto o tecnología del que trata de guía. Su clasificación se realiza en tres (3) niveles, cada uno de ellos asociado a un conjunto de niveles de riesgos.

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

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

- a) **Identificación de riesgos del producto o tecnología.** Se recomienda realizar un inventario de riesgos que puedan existir por la propia naturaleza del producto o tecnología, como por la funcionalidad prevista por la organización. Para ello, se han identificado una serie de riesgos inherentes al producto o tecnología, los cuales deberán ser completados con los riesgos particulares del sistema que se vaya a implementar.

Para la identificación inicial de riesgos, se ha empleado la metodología MAGERIT y la herramienta PILAR, sobre un escenario basado en un sistema operativo Windows Server 2019 en las modalidades de uso como controlador de dominio y como servidor miembro.

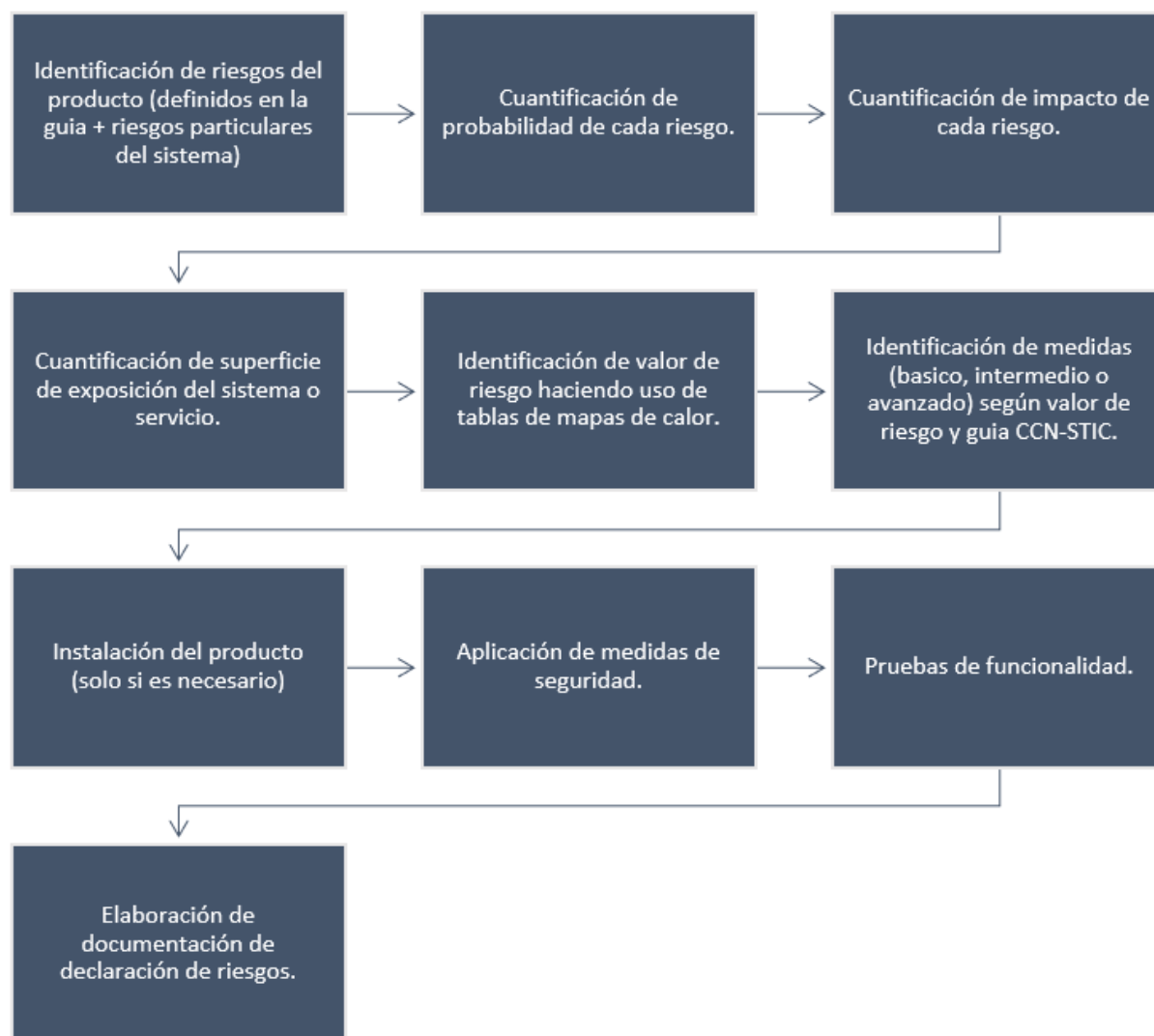
- b) **Cuantificación de probabilidad de cada riesgo.** Se deberá cuantificar la probabilidad de ocurrencia de cada riesgo en función de las condiciones particulares que cada organización conoce de sus sistemas.
- c) **Cuantificación de impacto de cada riesgo.** Se deberá cuantificar el impacto en las operaciones y en el negocio, en función de las condiciones particulares que cada organización conoce de sus sistemas.
- d) **Cuantificación de superficie de exposición del sistema o servicio.** La organización deberá determinar el nivel de superficie de exposición que tendrá el activo (servicio que presta o información que maneja).
- e) **Identificación de valor de riesgo haciendo uso de tablas de mapas de calor.** Para cada guía se han desarrollado una serie de tablas de mapas de calor, permitiendo calcular e identificar donde se sitúa cada uno de los riesgos identificados en los primeros pasos. Una

vez identificado el nivel de riesgo, en el siguiente paso se procederá a aplicar la medida correspondiente para mitigar dicho nivel de riesgo.

- f) **Identificación de medidas (BÁSICO, INTERMEDIO o AVANZADO) según valor de riesgo y guía CCN-STIC.** La lista de medidas de seguridad está agrupada en categorías y ordenada según el nivel de riesgo resultado de los cálculos anteriores. Es importante señalar que cada categoría puede conllevar la necesidad de aplicar una o varias medidas de seguridad, que a su vez se pueden traducir en distintas configuraciones, directivas de seguridad o la instalación de software de protección.

Cada organización deberá determinar cómo configurar el sistema para el cumplimiento de la medida correspondiente. De esta forma, se ofrece un mayor grado de adaptación al entorno a la hora de proteger el sistema, necesario sobre todo en sistemas que ya están en funcionamiento o en producción. Es decir, en esta guía de seguridad se identifican qué medidas de seguridad serán necesarias aplicar, pero el cómo aplicarlas se deja a responsabilidad de las propias organizaciones.

- g) **Instalación del producto (en nuevas instalaciones).** Una vez conocidos los riesgos y las medidas de mitigación de éstos, se procederá con la instalación del sistema operativo, en el caso de nuevas implementaciones. Si su sistema ya está instalado, se puede saltar este paso.
- h) **Aplicación de medidas de seguridad.** En este paso se aplicarán las medidas de seguridad recomendadas según el nivel de riesgo resultante para hacer efectiva la mitigación, reducción o eliminación del riesgo. Es lo que se denomina el perfilado de seguridad. Cada organización puede tener un perfilado distinto y como se ha indicado anteriormente, se deberán aplicar las medidas de seguridad en función de dicho perfilado.
- i) **Pruebas de funcionalidad.** Se recomienda diseñar y ejecutar un plan de pruebas de funcionalidad posterior a la aplicación de medidas, dado que alguna de ellas puede haber deshabilitado o bloqueado funcionalidades que requiere la organización. En ese caso se podrán establecer directivas de excepción para revertir los cambios, asumiendo el riesgo que ello conlleva.
- j) **Elaboración de documentación de declaración de riesgos.** Se recomienda elaborar un documento de declaración de riesgos donde se establezca claramente cada uno de los riesgos identificados y las medidas de seguridad aplicadas.



5. DECLARACIÓN DE RIESGOS

Se trata del primer paso a realizar para la aplicación de las medidas de seguridad acordes a la realidad y condiciones donde estará operando el sistema.

Con motivo de la aparición de nuevas versiones y cambios en el software de base como los sistemas operativos, es altamente recomendable contar con unas medidas de seguridad y de evaluación constantes que puedan detectar de forma proactiva y previa a su implementación cualquier vulnerabilidad, amenaza o riesgo.

El análisis de riesgos permitirá elaborar un perfilado para la aplicabilidad de medidas acorde a los resultados obtenidos, minimizando los vectores de ataque, brechas o malas configuraciones de seguridad sobre los activos, e intentando también que estas medidas no afecten a la funcionalidad o usabilidad del sistema y sus objetivos.

Esta guía de seguridad tiene como uno de sus objetivos, ayudar a la implementación de las medidas de seguridad, por lo tanto, para la elaboración de la propia guía se ha realizado un análisis de riesgos específico para un sistema basado en Windows Server 2019.

Para la ejecución del presente Análisis de Riesgos se han definido dos (2) escenarios base, los cuales se consideran esenciales y estándar de uso del sistema operativo:

- a) El primer escenario será un sistema aislado en red, quiere decir que estará conectando a elementos de red internos dentro de una organización o entidad, pero no realizará conexiones externas hacia redes no seguras como Internet.
- b) El segundo escenario será un sistema conectado a redes no seguras como puede ser Internet, quiere decir que tendría la capacidad de establecer conexiones con elementos de red externos de una organización o entidad.

5.1 RIESGOS ASOCIADOS A UN SERIDOR WINDOWS SERVER 2019

A continuación, se identifican los resultados de este análisis, los cuales forman parte de la declaración de riesgos y constituye, como ya se ha indicado, el primer paso a realizar en la implementación de esta guía de seguridad. Estos riesgos se deberán tener en consideración cuando la organización diseñe y elabore su propio análisis de riesgos.

Para facilitar la tarea de identificar, cuantificar y valorar cada uno de los riesgos, se ha elaborado la siguiente tabla de control, donde se podrá ir registrando en cada caso los niveles de probabilidad e impacto asociados a cada riesgo para un equipo en concreto.

EXP	NOMBRE DEL EQUIPO			
	SISTEMA OPERATIVO		BUILD	
	FUNCION PRINCIPAL		FECHA DE AA.RR.	
NUM	RIESGOS	APLICA (S/N)	PROBABILIDAD [1...5]	IMPACTO [1...5]
1.	[A.3] Manipulación de los registros de actividad.			
2.	[A.4] Manipulación de los ficheros de configuración.			
3.	[A.5] Suplantación de la identidad.			
4.	[A.6] Abuso de privilegios de acceso.			
5.	[A.8] Difusión de software dañino.			
6.	[A.11] Acceso no autorizado.			
7.	[A.15] Modificación de la información.			
8.	[A.19] Revelación de información.			
9.	[A.22] Manipulación de programas.			
10.	[A.23] Manipulación del hardware.			
11.	[A.24] Denegación de servicio.			
12.	[A.25] Robo de equipos.			
13.	[A.29] Extorsión.			
14.	[A.30] Ingeniería social.			
15.	[E.25] Pérdida de equipos.			

5.2 CUANTIFICACIÓN DE PROBABILIDAD DE CADA RIESGO

El siguiente paso, será cuantificar la probabilidad de cada uno de los riesgos. Los valores de probabilidad podrán ir desde el valor uno (1) hasta el valor cinco (5), siendo uno (1) muy poco probable y cinco (5) muy probable.

- a) **Probabilidad 1:** es muy poco probable que se materialice el riesgo, ya sea por las condiciones específicas del sistema en la organización o porque existan salvaguardas ya implementadas que hagan que el riesgo prácticamente desaparezca.
- b) **Probabilidad 2:** es poco probable que se materialice el riesgo, aunque se puede materializar.
- c) **Probabilidad 3:** es probable que se materialice el riesgo dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.
- d) **Probabilidad 4:** es bastante probable que se materialice el riesgo, dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.
- e) **Probabilidad 5:** es muy probable que se materialice el riesgo, dadas las condiciones específicas del sistema en la organización o porque no existen salvaguardas que reduzcan la probabilidad de materialización del riesgo. Las medidas de seguridad a aplicar cuando se da este nivel pueden ser más estrictas que en niveles inferiores.

5.3 CUANTIFICACIÓN DE IMPACTO DE CADA RIESGO

Al igual que sucede con la cuantificación de la probabilidad, se deberá cuantificar el grado de impacto en el servicio o negocio en el supuesto caso de que el riesgo se materialice. Los valores de impacto podrán ir desde el valor 1 hasta el valor 5, siendo 1 cuando no tiene un impacto conocido o es muy pequeño y 5 cuando el impacto es muy importante.

- a) **Impacto 1:** el riesgo, en el caso de que se materialice, no tiene un impacto conocido o es muy pequeño, prácticamente despreciable. Los datos y el servicio no se ven comprometidos y el sistema funciona correctamente. Este nivel de impacto puede requerir la aplicación de medidas de prevención.
- b) **Impacto 2:** el riesgo, en el caso de que se materialice, tiene un impacto pequeño. No se han comprometidos los datos ni el servicio, sin embargo, es posible que, si no se corrige, el sistema se vuelva inestable o pueda existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención.
- c) **Impacto 3:** el impacto en el sistema es preocupante. No se han comprometido los datos, sin embargo, el servicio puede continuar de forma limitada y a corto plazo podría haber una degradación de la seguridad del sistema. Si no se aplican las medidas necesarias puede existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención, pero también medidas de corrección.

- d) **Impacto 4:** el impacto en el sistema es importante. Es posible que algunos datos hayan sido comprometidos y los servicios se hayan visto afectados. También es posible que el sistema se haya vuelto inestable o comience a ser vulnerable. Se debe actuar lo antes posible para restablecer el correcto funcionamiento.
- e) **Impacto 5:** el impacto en el sistema es muy importante. Afecta directamente a la disponibilidad del servicio, imposibilitando el acceso a la información. El sistema ha sido comprometido, y algunos o todos los datos han sido comprometidos. Un atacante externo puede haber obtenido acceso privilegiado y puede estar controlando el sistema. Se deben aplicar medidas de recuperación de forma inmediata.

5.4 CUANTIFICACIÓN DE SUPERFICIE DE EXPOSICIÓN DEL SISTEMA

Por último, se deberá tener en cuenta el nivel o grado de exposición del sistema a las amenazas y riesgos externos. Este valor actuará como modulador a la hora de calcular el valor final de cada uno de los riesgos.

Por ejemplo, ante un riesgo cuyo impacto y probabilidad son altos o muy altos, si el sistema se encuentra en un nivel de superficie de exposición bajo, es lógico pensar que el valor final del riesgo se vea atenuado en parte por las condiciones de exposición en las que se encuentra el sistema. Por el contrario, si un riesgo tiene unos niveles de impacto y probabilidad bajos, ante un nivel de superficie de exposición alto, es lógico pensar que el valor final del riesgo se vea incrementado por este mismo motivo.

Es evidente que pueden existir multitud de escenarios y configuraciones de red, siendo prácticamente imposible poder reflejar todas ellas en una sola guía de seguridad. Sin embargo, para una mejor comprensión y simplificación de las medidas que se deberán adoptar, se han agrupado en tres (3) niveles las distintas opciones de superficie de exposición.

- a) **Nivel de superficie de exposición 1:** representa aquellos sistemas que no están expuestos a riesgos externos, procedentes de redes interconectadas o redes no confiables como Internet. En este nivel se encuentran los sistemas aislados, sin ningún tipo de comunicación con otras redes.
- b) **Nivel de superficie de exposición 2:** representa aquellos sistemas que tienen algún tipo de conexión de red local o de interconexión con otras redes. Estos sistemas se conectan únicamente con redes confiables. En este nivel se encuentran los sistemas compuestos por más de un equipo conectado a través de una red local (LAN) o varios sistemas que están interconectados entre sí a través de otros medios, pero que no son accesibles desde Internet o redes no confiables.
- c) **Nivel de superficie de exposición 3:** representa aquellos sistemas accesibles desde o con conexión directa o indirecta con Internet y otras redes. Dado que Internet se considera una red no confiable, el riesgo de explotación de vulnerabilidades de ejecución remota es mucho mayor que en los niveles inferiores. En este nivel se encuentra la mayoría de los sistemas en producción de las organizaciones.

6. IDENTIFICACIÓN DE LOS VALORES DE RIESGO RESULTANTES

Una vez identificados los distintos riesgos inherentes al sistema y después de calcular los valores de probabilidad, impacto y superficie de exposición de cada uno de ellos, el siguiente paso será determinar el valor final de cada riesgo. Tal y como ya se ha indicado, este valor variará en función de cada una de las tres (3) variables que se han tenido en cuenta.

Para facilitar su cálculo, se han elaborado las siguientes tablas con un diseño de mapas de calor, que varían según la superficie de exposición que tendrá el sistema. Cada una de ellas servirá como referencia para determinar el valor final del riesgo, el cual se podrá anexar a la tabla de riesgos del punto “5.1 RIESGOS ASOCIADOS A UN SERIDOR WINDOWS SERVER 2019”.

SUPERFICIE DE EXPOSICIÓN		1			
PROBABILIDAD	NIVEL DE RIESGO				
5	5	6	7	7	8
4	4	5	6	7	7
3	3	4	5	6	7
2	2	3	4	5	6
1	2	2	3	4	5
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN		2			
PROBABILIDAD	NIVEL DE RIESGO				
5	6	7	7	8	9
4	5	6	7	7	8
3	4	5	6	7	7
2	3	4	5	6	7
1	2	3	4	5	6
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN		3			
PROBABILIDAD	NIVEL DE RIESGO				
5	7	7	8	9	10
4	6	7	7	8	9
3	5	6	7	7	8
2	4	5	6	7	7
1	3	4	5	6	7
IMPACTO	1	2	3	4	5

7. PERFILADO PARA LA APLICABILIDAD DE MEDIDAS

A continuación, se muestran las categorías o agrupación de medidas de seguridad que deberán ser aplicadas a Windows Server 2019, en función de los resultados obtenidos por el análisis de riesgos y la cuantificación de cada uno de éstos.

Para una mejor comprensión, se han agrupado las medidas en tres (3) alcances de implementación, cada uno de ellos asociado a un grupo de niveles de riesgos.

- a) Alcance BÁSICO.
- b) Alcance INTERMEDIO.
- c) Alcance AVANZADO.

Una vez obtenido el nivel de riesgo de cada uno de los riesgos identificados, se aplicará la siguiente tabla para determinar las medidas necesarias en cada nivel.

Esta tabla indica que, si se ha obtenido un valor menor o igual a 3, se deberán aplicar las categorías de perfilado de seguridad de alcance BÁSICO. Si el valor obtenido para un riesgo determinado está entre 4 y 6, se deberán aplicar las categorías de perfilado de seguridad de alcance INTERMEDIO. Por último, si el valor obtenido es 7 o superior, se deberán aplicar las categorías de perfilado de alcance AVANZADO.

NIVEL DE RIESGO	ALCANCE		
	(B)ÁSICO	(I)NTERMEDIO	(A)VANZADO
9	SI	SI	SI
8	SI	SI	SI
7	SI	SI	SI
6	SI	SI	
5	SI	SI	
4	SI	SI	
3	SI		
2	SI		
1	SI		

En la siguiente tabla se muestra la asociación entre los riesgos identificados en el primer paso de esta guía y las categorías de perfilado de seguridad que mitiga, controlan o reducen dicho riesgo.

Como se puede observar, pueden existir categorías de perfilado de seguridad que actúen sobre uno o varios riesgos. Por lo tanto, para una mejor identificación, se han codificado cada una de las categorías, asociándolas al primer riesgo que mitigan, obteniendo la siguiente nomenclatura de categorías.

- a) A.3: corresponde con el código de riesgo que especifica la herramienta PILAR.
- b) SEC1: corresponde con la categoría de seguridad 1 para dicho riesgo. El número se incrementará en uno para cada nueva categoría que se haya identificado.

La siguiente tabla define qué conjunto de medidas de seguridad deben ser aplicadas, en función de los niveles de riesgo obtenidos.

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA WINDOWS SERVER 2019	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log)	[A.3.SEC1] Se auditan los inicios de sesión.			
	[A.3.SEC2] Se controla quien puede acceder a los registros de seguridad y auditoría.			
	[A.3.SEC3] Se controla el cambio de hora del sistema.			
	[A.3.SEC4] Se controla quién puede generar registros de seguridad.			
	[A.3.SEC5] Se ha implementado la auditoría detallada basada en subcategorías.			
	[A.3.SEC6] Se garantiza al menos 90 días de registros de actividad.			
	[A.3.SEC7] Se audita el uso de copias de seguridad y restauración.			
	[A.3.SEC8] El sistema se apaga si no se pueden generar auditorías de seguridad.			
[A.4] Manipulación de los ficheros de configuración	[A.4.SEC1] Los usuarios estándar no disponen de permisos de administrador local.			
	[A.4.SEC2] El sistema tiene un antivirus y éste está actualizado.			
	[A.4.SEC3] Está habilitado el arranque seguro (Secure Boot).			
	[A.4.SEC4] Está habilitada la seguridad basada en virtualización (aislamiento del núcleo).			
[A.5] Suplantación de la identidad	[A.5.SEC1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC2] UAC está habilitado y controla los intentos de elevación.			
	[A.5.SEC3] Se han reforzado las conexiones de canal seguro. ¹			
	[A.5.SEC4] Se controla el acceso a las claves de cifrado.			
	[A.5.SEC5] Se han deshabilitado los algoritmos de cifrado inseguros.			
	[A.5.SEC6] Se cifran los datos de las conexiones de canal seguro.			
	[A.5.SEC7] Se exige el cambio de contraseña de forma recurrente en entornos de dominio.			
	[A.5.SEC8] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.5.SEC9] Se controla la inactividad de la sesión de red.			
	[A.5.SEC10] Se controla el uso de NTLM y se deshabilita si es posible.			
[A.6] Abuso de privilegios de acceso	[A.6.SEC1] Se controla la unión de equipos al dominio.			
	[A.6.SEC2] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC3] Se restringe el acceso en modo depuración.			
	[A.6.SEC4] Se controla quién puede hacer copias de seguridad y tareas de mantenimiento.			

¹ Se entiende como canal seguro aquellas conexiones utilizadas para realizar operaciones como autenticación de paso NTLM, búsqueda SID/nombre de LSA, consultas LDAP y de Catálogo Global, SMB, etc.

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA WINDOWS SERVER 2019	ALCANCE		
		B	I	A
	[A.6.SEC5] Se controla el uso de consolas de administración o recuperación.			
	[A.6.SEC6] Se refuerza la seguridad de los objetos COM.			
	[A.6.SEC7] Se restringe el uso de sesiones NULL.			
	[A.3.SEC4] Se controla quien puede generar registros de seguridad.			
	[A.5.SEC1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC2] UAC está habilitado y controla los intentos de elevación.			
[A.8] Difusión de software dañino	[A8.SEC1] Se controla quién puede instalar software en el sistema.			
	[A.8.SEC2] El sistema operativo está actualizado.			
	[A.8.SEC3] El sistema tiene un firewall local activado.			
	[A.8.SEC4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			
	[A.8.SEC5] Se controla la ejecución de aplicaciones.			
	[A.8.SEC6] Se dispone de medidas anti ransomware habilitadas.			
	[A.4.SEC2] El sistema tiene un antivirus y éste está actualizado.			
	[A.4.SEC3] Está habilitado el arranque seguro (Secure Boot).			
	[A.4.SEC4] Está habilitada la seguridad basada en virtualización (aislamiento del núcleo).			
	[A.5.SEC1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC2] UAC está habilitado y controla los intentos de elevación.			
	[A.6.SEC2] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC5] Se refuerza la seguridad de los objetos COM.			
	[A.11.SEC1] Se controla el inicio de sesión local en el sistema.			
[A.11] Acceso no autorizado	[A.11.SEC2] Se ha reforzado la seguridad del protocolo SMB.			
	[A.11.SEC3] Se dispone de una política de credenciales robusta.			
	[A.11.SEC4] Durante el inicio de sesión, el sistema muestra un texto en cumplimiento con las normas o directivas de la organización.			
	[A.11.SEC5] Se requiere validación de nombres de destino SPN del servidor.			
	[A.11.SEC6] Se controla el acceso al sistema a través de la red.			
	[A.11.SEC7] Sólo se permite TLS 1.2 y superior con algoritmos de cifrado robustos.			
	[A.11.SEC8] Se utiliza autenticación de doble factor.			
	[A.3.SEC4] Se controla quién puede generar registros de seguridad.			
	[A.3.SEC7] Se audita el uso de copias de seguridad y restauración.			
	[A.5.SEC1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC2] UAC está habilitado y controla los intentos de elevación.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA WINDOWS SERVER 2019	ALCANCE		
		B	I	A
	[A.5.SEC3] Se han reforzado las conexiones de canal seguro. ²			
	[A.5.SEC4] Se controla el acceso a las claves de cifrado.			
	[A.5.SEC7] Se exige el cambio de contraseña de forma recurrente en entornos de dominio.			
	[A.5.SEC8] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.5.SEC9] Se controla la inactividad de la sesión de red.			
	[A.5.SEC10] Se controla el uso de NTLM y se deshabilita si es posible.			
	[A.6.SEC2] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC3] Se restringe el acceso en modo depuración.			
	[A.6.SEC4] Se controla quién puede hacer copias de seguridad y tareas de mantenimiento.			
	[A.6.SEC5] Se controla el uso de consolas de administración o recuperación.			
	[A.6.SEC7] Se restringe el uso de sesiones NULL.			
[A.15] Modificación de la información	[A.15.SEC1] Se controla el uso de medios de almacenamiento extraíbles.			
	[A.5.SEC3] Se han reforzado las conexiones de canal seguro.			
	[A.5.SEC8] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.6.SEC2] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC4] Se controla quién puede hacer copias de seguridad y tareas de mantenimiento.			
	[A.11.SEC2] Se ha reforzado el uso del protocolo SMB.			
[A.19] Revelación de información	[A.11.SEC7] Sólo se permite TLS 1.2 y superior con algoritmos de cifrado robustos.			
	[A.19.SEC1] Se controla el acceso al árbol de carpetas y ficheros.			
	[A.19.SEC2] Se controla el derecho de sincronización de datos del directorio.			
	[A.19.SEC3] Se borra el archivo de paginación de la memoria virtual en el apagado.			
	[A.19.SEC4] Se aplican medidas para la protección de las cuentas.			
	[A.19.SEC5] Está habilitada la protección de credenciales (Credential Guard).			
	[A.3.SEC2] Se controla quien puede acceder a los registros de seguridad y auditoría.			
	[A.3.SEC7] Se audita el uso de copias de seguridad y restauración.			
	[A.5.SEC3] Se han reforzado las conexiones de canal seguro.			
	[A.5.SEC4] Se controla el acceso a las claves de cifrado.			
	[A.5.SEC8] Se hace uso de protocolos seguros para los procesos de autenticación de red.			
	[A.6.SEC2] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC3] Se restringe el acceso en modo depuración.			

² Se entiende como canal seguro aquellas conexiones utilizadas para realizar operaciones como autenticación de paso NTLM, búsqueda SID/nombre de LSA, consultas LDAP y de Catálogo Global, SMB, etc.

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA WINDOWS SERVER 2019	ALCANCE		
		B	I	A
	[A.6.SEC4] Se controla quién puede hacer copias de seguridad y tareas de mantenimiento.			
	[A.6.SEC5] Se controla el uso de consolas de administración o recuperación.			
	[A.11.SEC1] Se controla el inicio de sesión local en el sistema.			
	[A.11.SEC2] Se ha reforzado la seguridad del protocolo SMB.			
	[A.11.SEC6] Se controla el acceso al sistema a través de la red.			
	[A.11.SEC7] Sólo se permite TLS 1.2 y superior con algoritmos de cifrado robustos.			
	[A.15.SEC1] Se controla el uso de medios de almacenamiento extraíbles.			
[A.22] Manipulación de programas	[A.4.SEC3] Está habilitado el arranque seguro (Secure Boot).			
	[A.4.SEC4] Está habilitada la seguridad basada en virtualización (aislamiento del núcleo).			
	[A.6.SEC2] Se refuerza la seguridad de los objetos sensibles del sistema.			
	[A.6.SEC3] Se restringe el acceso en modo depuración.			
	[A.6.SEC6] Se refuerza la seguridad de los objetos COM.			
	[A.8.SEC4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			
	[A.8.SEC6] Se controla la ejecución de aplicaciones.			
	[A.11.SEC2] Se ha reforzado el uso del protocolo SMB.			
[A.23] Manipulación del hardware	[A.23.SEC1] Se controla la instalación y uso de cualquier dispositivo conectado al equipo.			
	[A.15.SEC1] Se controla el uso de medios de almacenamiento extraíbles.			
[A.24] Denegación de servicio	[A.24.SEC1] Se controlan los privilegios que afectan al rendimiento del sistema.			
	[A.24.SEC2] Se controla quien puede apagar el sistema.			
	[A.8.SEC6] Se dispone de medidas anti ransomware habilitadas.			
	[A.3.SEC3] Se controla el cambio de hora del sistema.			
	[A.3.SEC4] Se controla quién puede generar registros de seguridad.			
[A.25] Robo de equipos	[A.25.SEC1] El disco del sistema está cifrado.			
	[A.25.SEC2] El disco de datos está cifrado.			
	[A.25.SEC3] Se hace uso de TPM para cifrado de disco.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA WINDOWS SERVER 2019	ALCANCE		
		B	I	A
[A.29] Extorsión	[A.4.SEC2] El sistema tiene un antivirus y éste está actualizado.			
	[A.4.SEC4] Está habilitada la seguridad basada en virtualización (aislamiento del núcleo).			
	[A.8.SEC1] Se controla quién puede instalar software en el sistema.			
	[A.8.SEC2] El sistema operativo está actualizado.			
	[A.8.SEC3] El sistema tiene un firewall local activado.			
	[A.8.SEC4] Se deshabilitan servicios innecesarios, reduciendo la superficie de exposición.			
	[A.8.SEC5] Se controla la ejecución de aplicaciones.			
	[A.8.SEC6] Se dispone de medidas anti ransomware habilitadas.			
	[A.11.SEC8] Se utiliza autenticación de doble factor.			
[A.30] Ingeniería social	[A.30.SEC1] Existe una política de bloqueo de cuentas ante inicios de sesión incorrectos.			
	[A.11.SEC8] Se utiliza autenticación de doble factor.			
[E.25] Pérdida de equipos	[A.25.SEC1] El disco del sistema está cifrado.			
	[A.25.SEC2] El disco de datos está cifrado.			
	[A.25.SEC3] Se hace uso de TPM para cifrado de disco.			

ANEXO A. PASO A PASO CONFIGURACIÓN BASE DE SEGURIDAD SOBRE WINDOWS SERVER 2019

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento de los sistemas Windows Server 2019, según los aspectos definidos en cada uno de los puntos anteriores de este documento. Esta configuración se ofrece a modo de referencia o ejemplo de aplicabilidad de medidas en función de unos resultados concretos del análisis de riesgos. Es posible que en otros escenarios y con otra superficie de exposición, el perfilado de aplicación de medidas sea distinto.

Este anexo, contempla la aplicación de tres directivas en los siguientes niveles.

- Nivel de dominio: Cubre las configuraciones de bloqueo de cuenta y longitud de contraseñas, es decir las directivas de contraseñas que aseguran la correcta configuración y uso de estas.
- Nivel de la unidad organizativa Domain Controllers: Incluye las configuraciones necesarias para el aseguramiento de Controladores de Dominio con sistema operativo Windows Server 2019.
- Nivel de unidad organizativa Servidores Miembro: Contempla las configuraciones base de seguridad para cualquier servicio implementado en el dominio bajo el sistema operativo Windows Server 2019.

Es necesario remarcar que la línea base de seguridad establecida dentro del presente anexo corresponde con un **perfilado intermedio**.

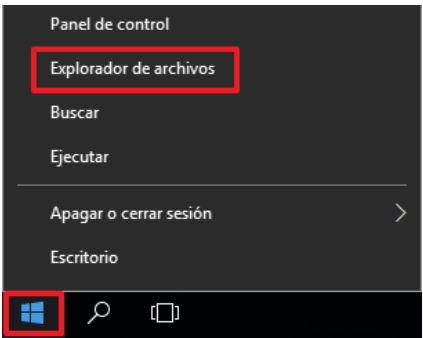
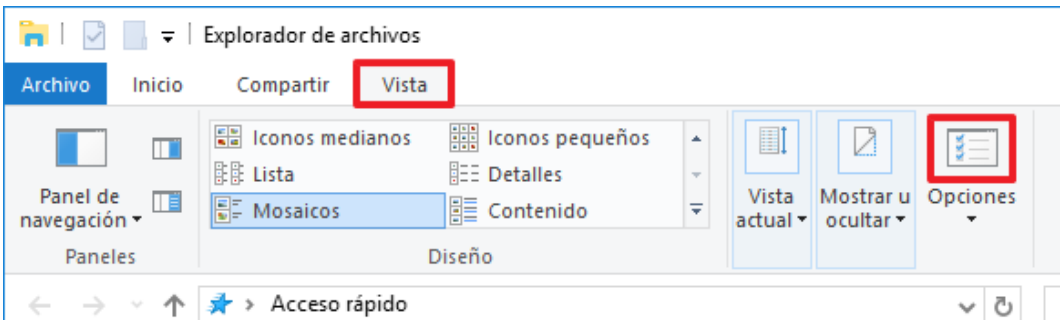
Nota: Debido a lo indicado con anterioridad, en caso de que el perfilado de seguridad obtenido en base al análisis realizado y la superficie de exposición obtenida, requiera de una **configuración de seguridad avanzada, será necesario implementar medidas adicionales de seguridad**. Por el contrario, es posible que el resultado de dicho análisis indique que la necesidad de configuración solo se establezca según el perfilado básico por lo que será posible evitar ciertas medidas de seguridad establecidas por medio del presente anexo.

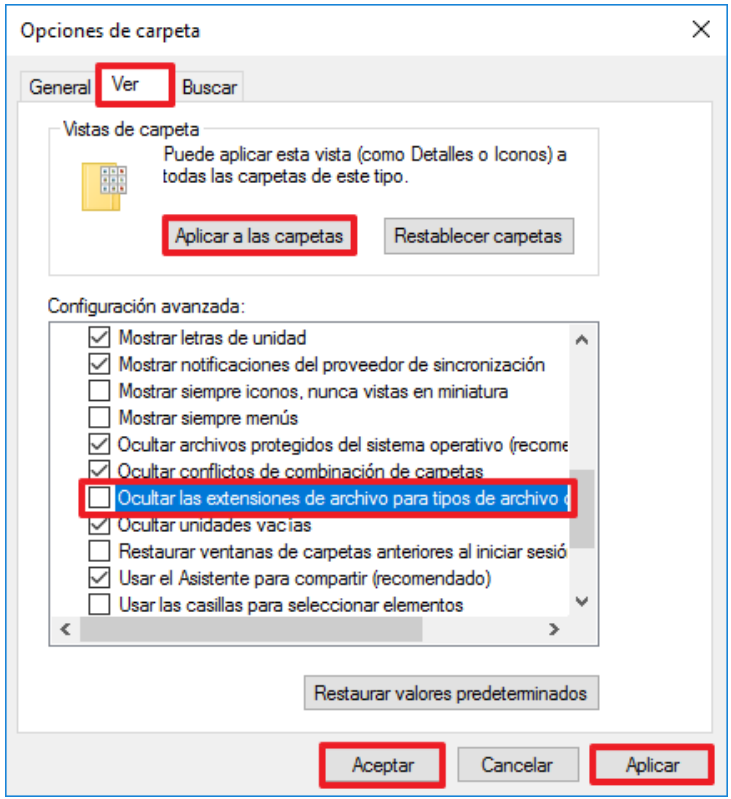
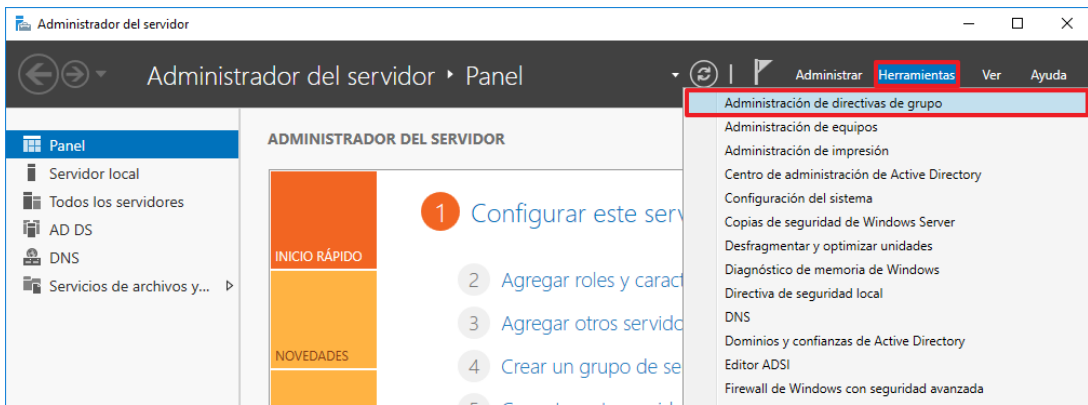
Por otro lado, es necesario indicar que ciertas categorías de seguridad no puedan ser aplicadas por medio de objetos GPO o configuraciones exactas a nivel de Windows. Por ello, se ha dedicado un apartado específico que permita establecer ejemplos de configuración sobre este tipo de categorías las cuales deberán ser adaptadas por cada organización.

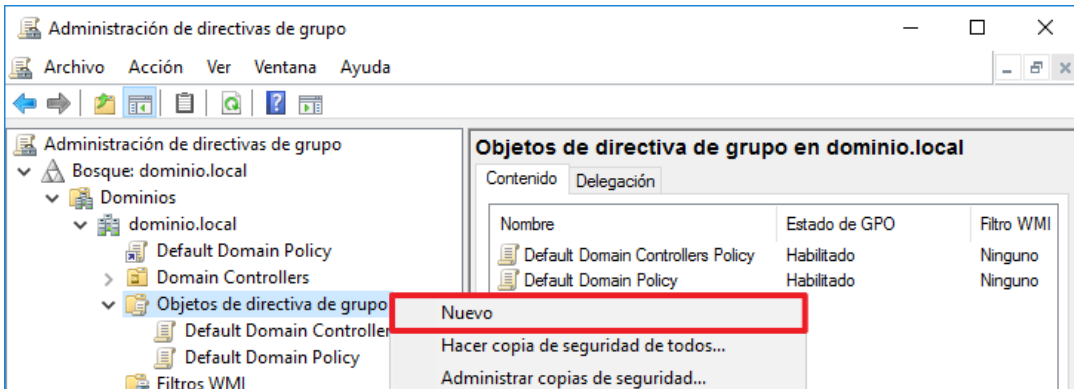
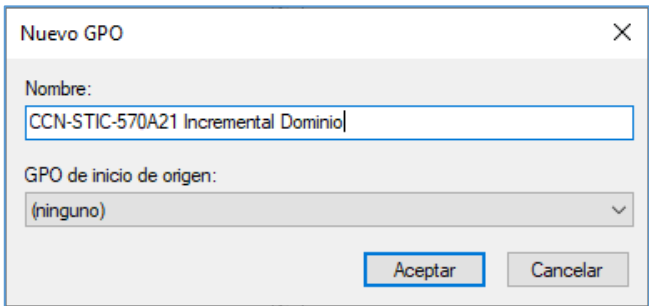
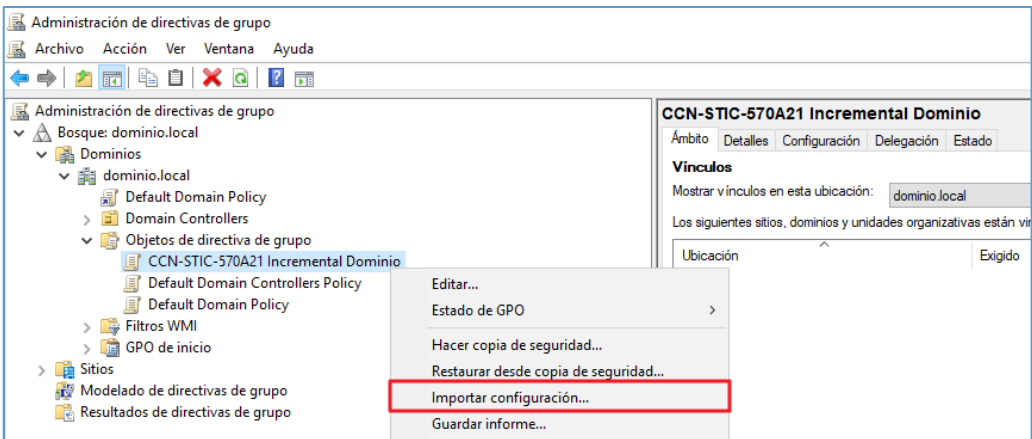
ANEXO A.1. PREPARACIÓN DEL DOMINIO

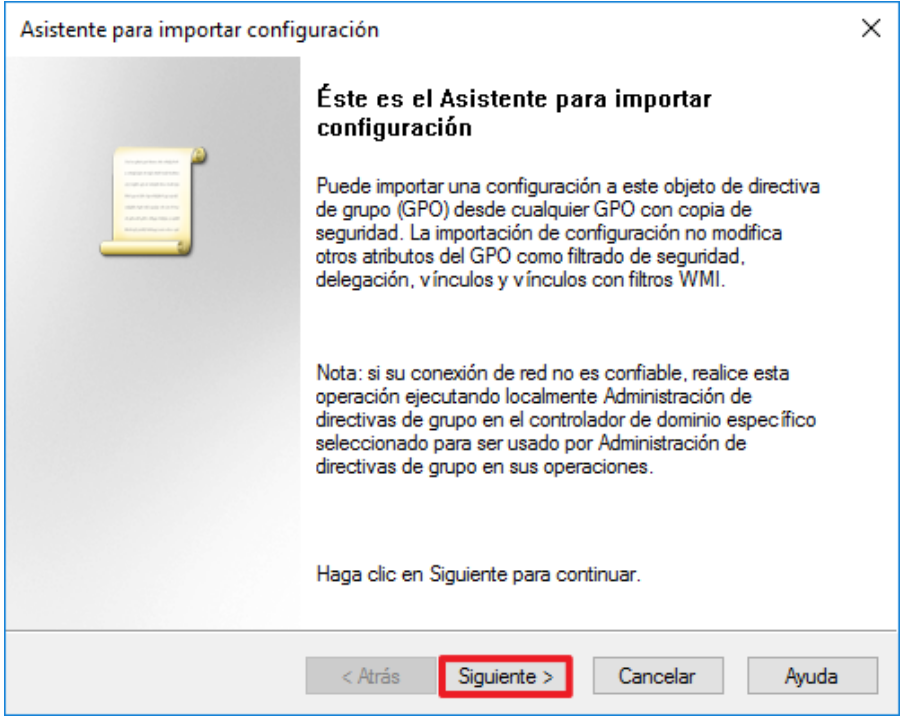
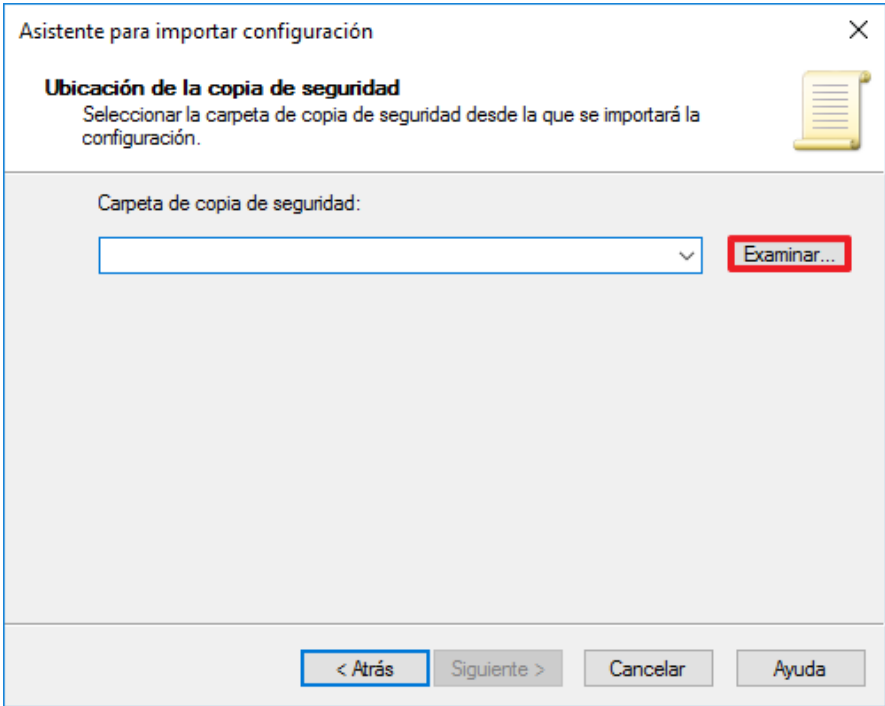
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las plantillas de seguridad. Solo es necesario realizar este procedimiento una vez.

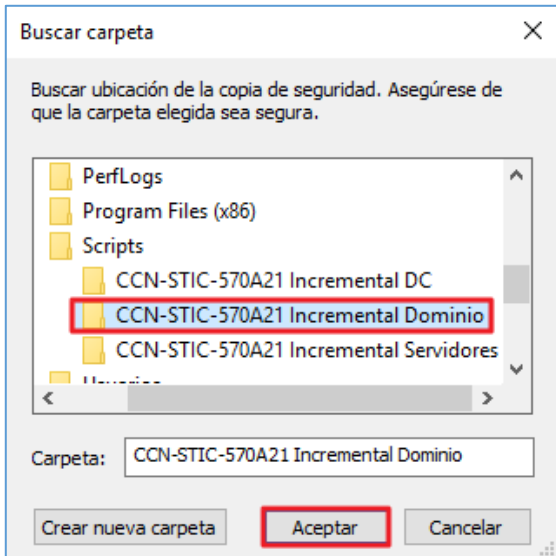
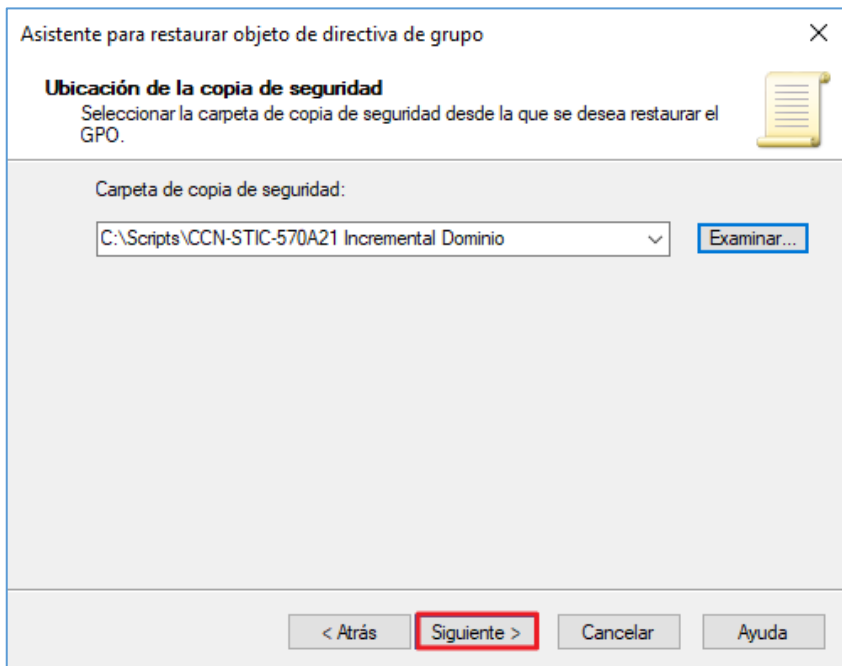
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-570A21.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.

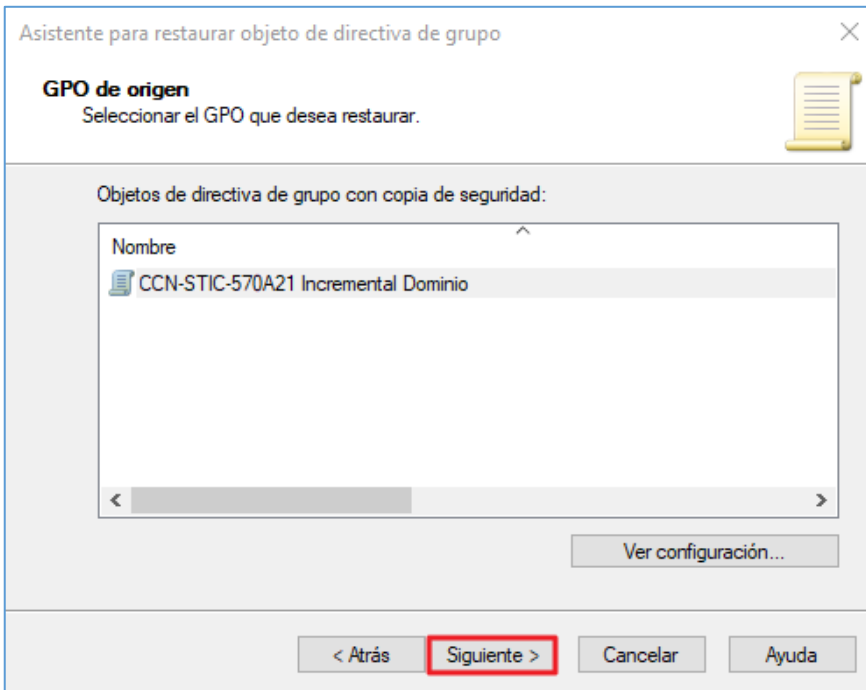
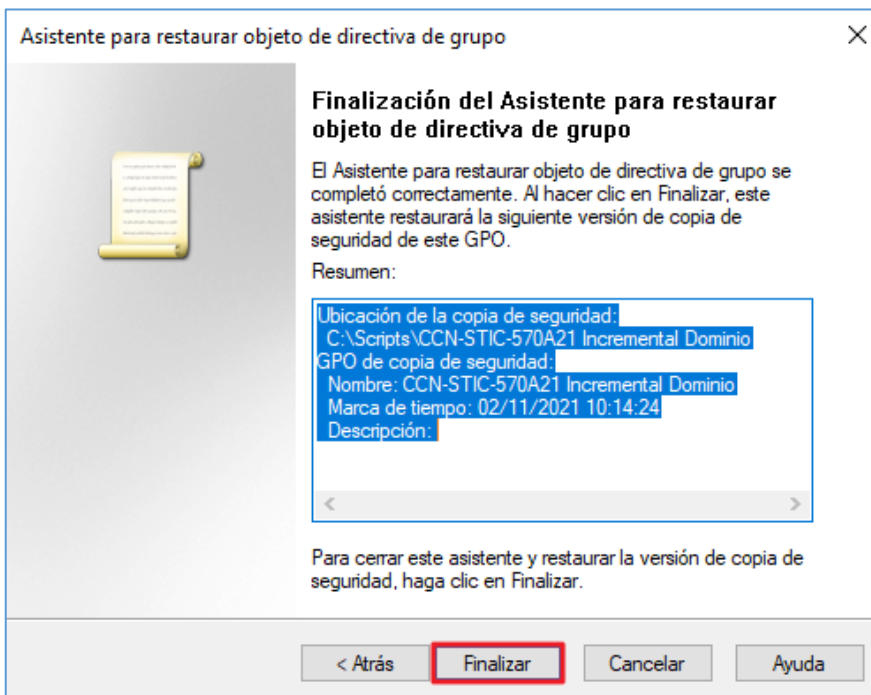
Paso	Descripción
4.	<p>Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts".</p> <p>Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-570A21".</p>
5.	<p>Configure el "Explorador de archivos" para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos" oculta las extensiones conocidas y este hecho dificulta la identificación de estos. Para ello, pulse sobre el botón de "Inicio" con el botón derecho y seleccione "Explorador de archivos".</p> 
6.	<p>En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones".</p> 

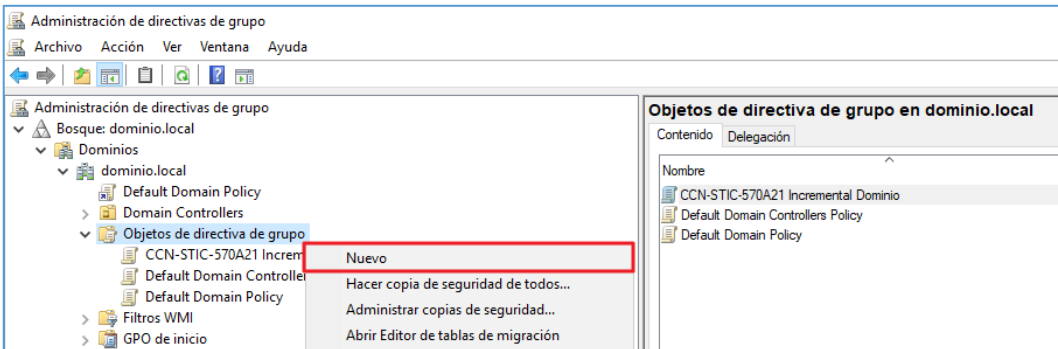
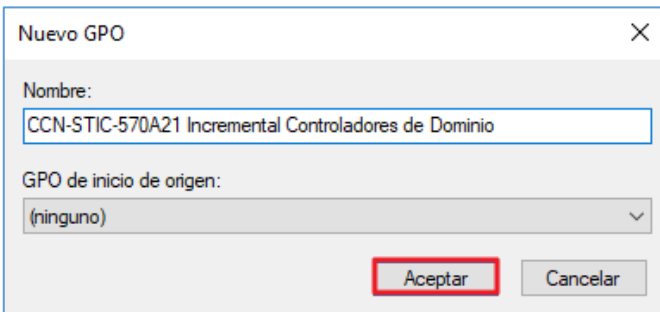
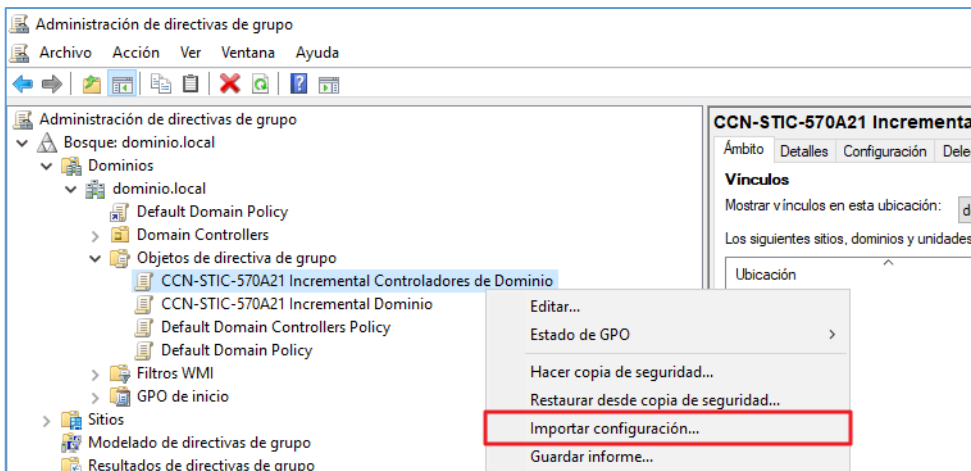
Paso	Descripción
7.	<p>En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”.</p> 
8.	<p>Asegúrese de que al menos los siguientes directorios hayan sido copiados a la ruta “C:\Scripts” del controlador de dominio:</p> <ul style="list-style-type: none"> – CCN-STIC-570A21 Incremental DC (directorio) – CCN-STIC-570A21 Incremental Servidores (directorio) – CCN-STIC-570A21 Incremental Dominio (directorio)
9.	<p>Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: “Herramientas → Administración de directivas de grupo”</p> 

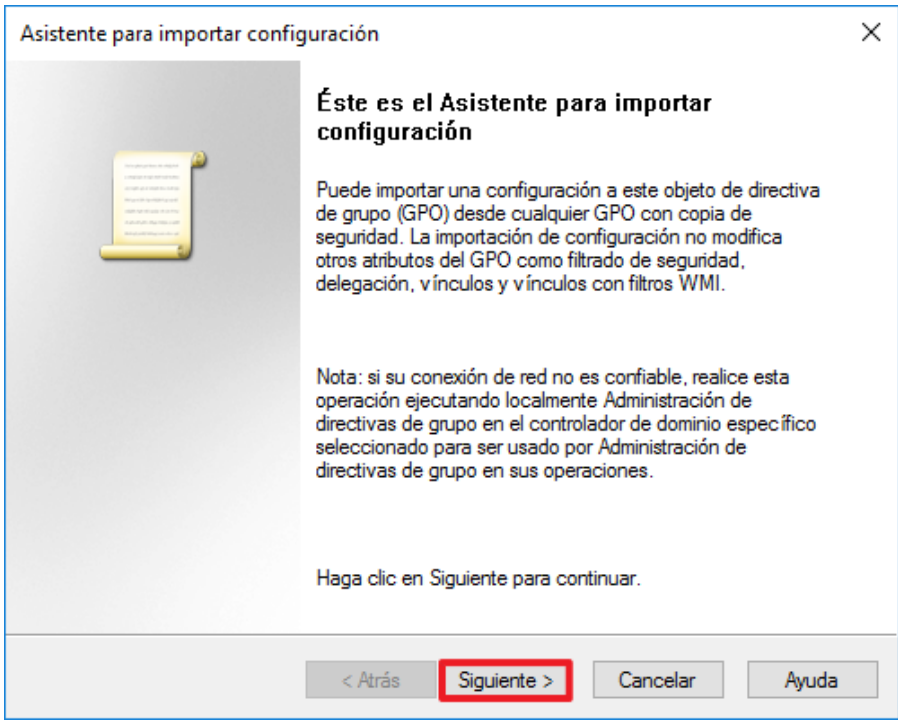
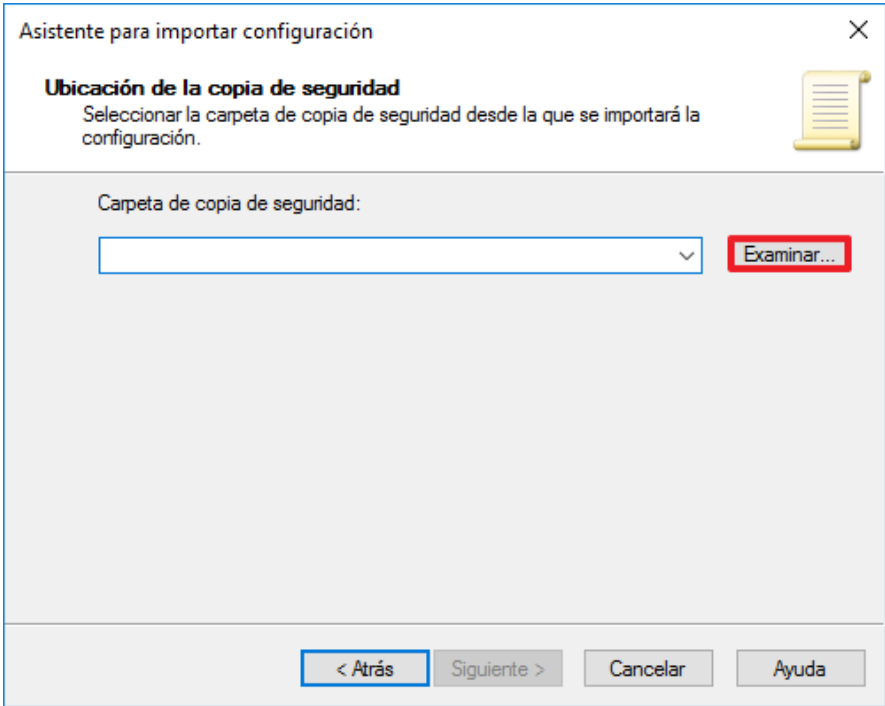
Paso	Descripción
10.	Despliegue los contenedores y sitúese sobre el nodo “Objetos de directiva de grupo”.
11.	<p>Pulse con el botón derecho, sobre dicho nodo y seleccione la opción “Nuevo”.</p> 
12.	<p>Introduzca como nombre “CCN-STIC-570A21 Incremental Dominio” y pulse el botón “Aceptar”.</p> 
13.	<p>Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración...”.</p> 

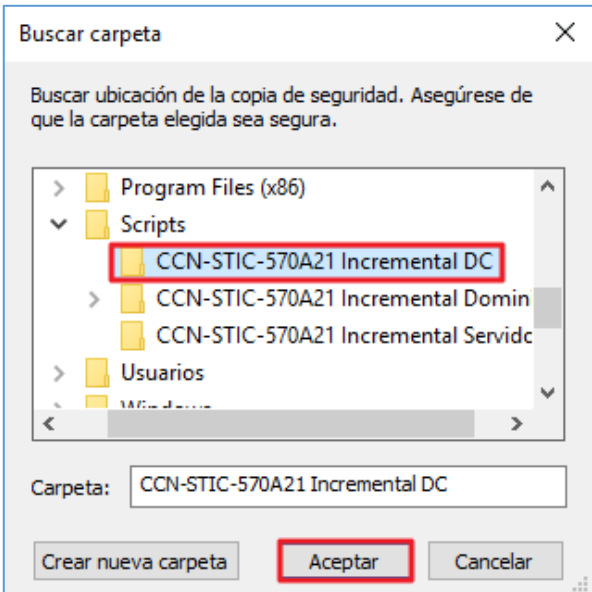
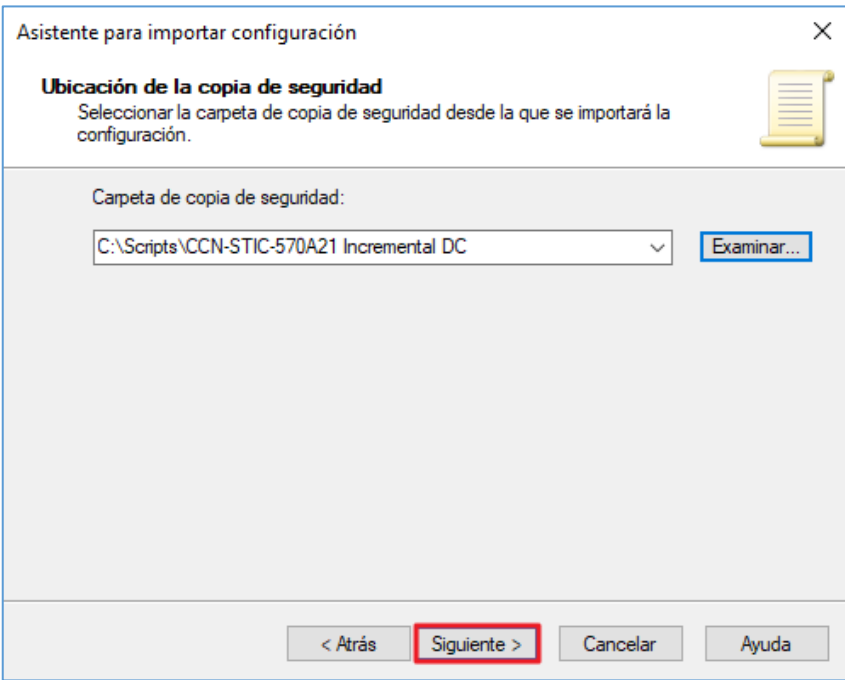
Paso	Descripción
14.	<p>En el asistente de importación de configuración, pulse el botón “Siguiente >”.</p> 
15.	<p>En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.</p>
16.	<p>En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.</p> 

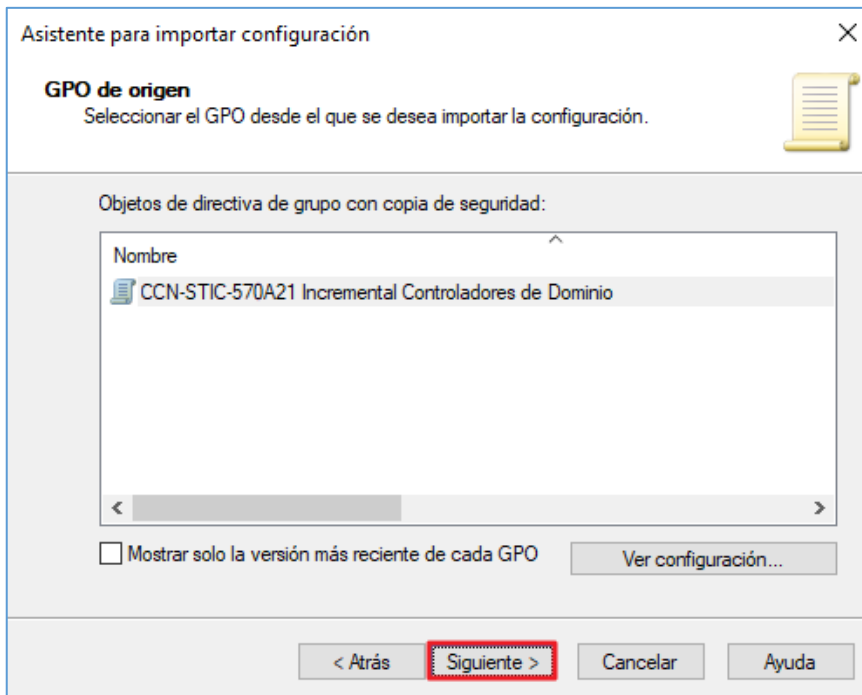
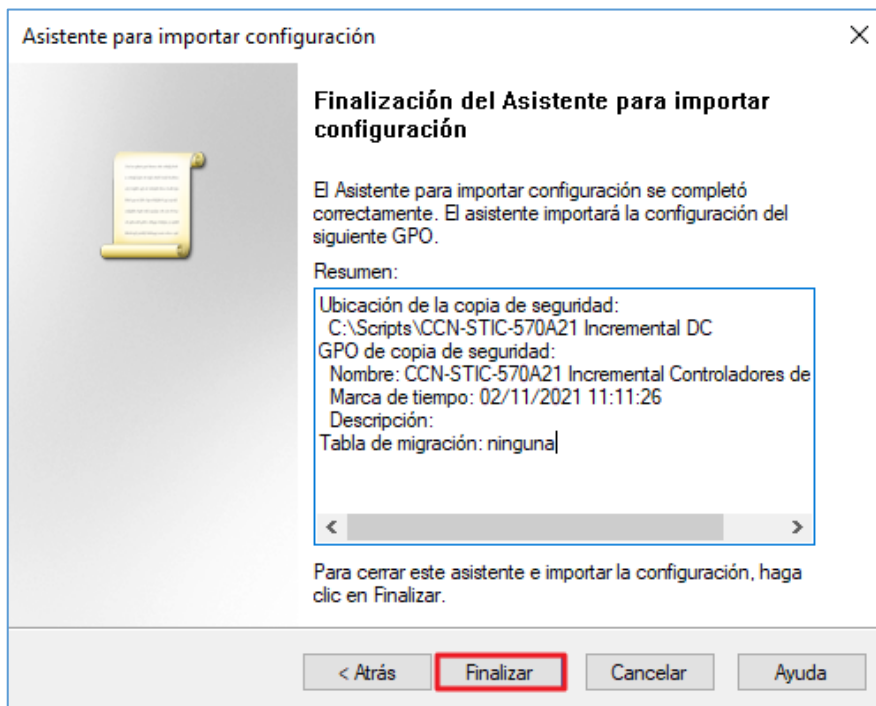
Paso	Descripción
17.	<p>Seleccione la carpeta “CCN-STIC-570A21 Incremental Dominio” que encontrará en el directorio “C:\Scripts” y pulse el botón “Aceptar”.</p> 
18.	<p>Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada.</p> 

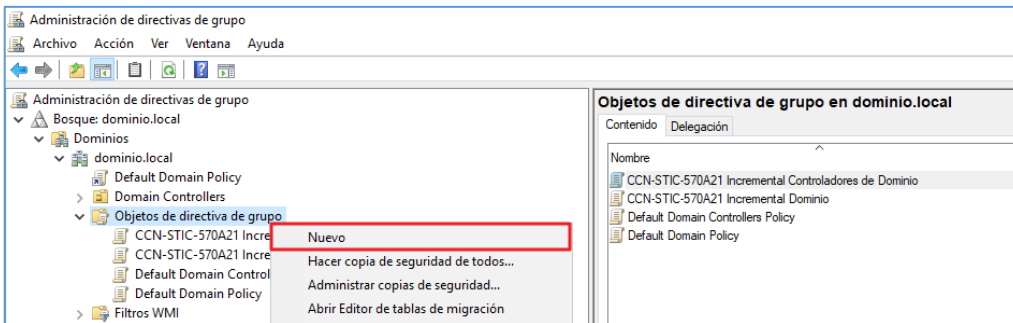
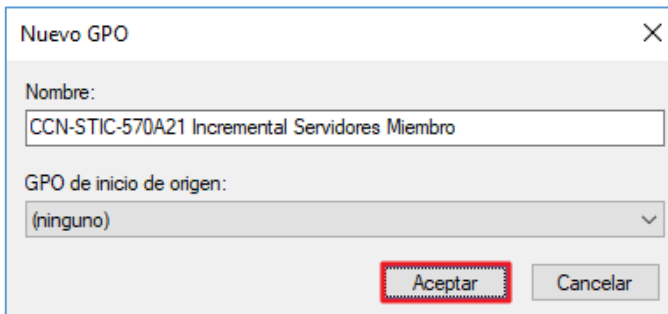
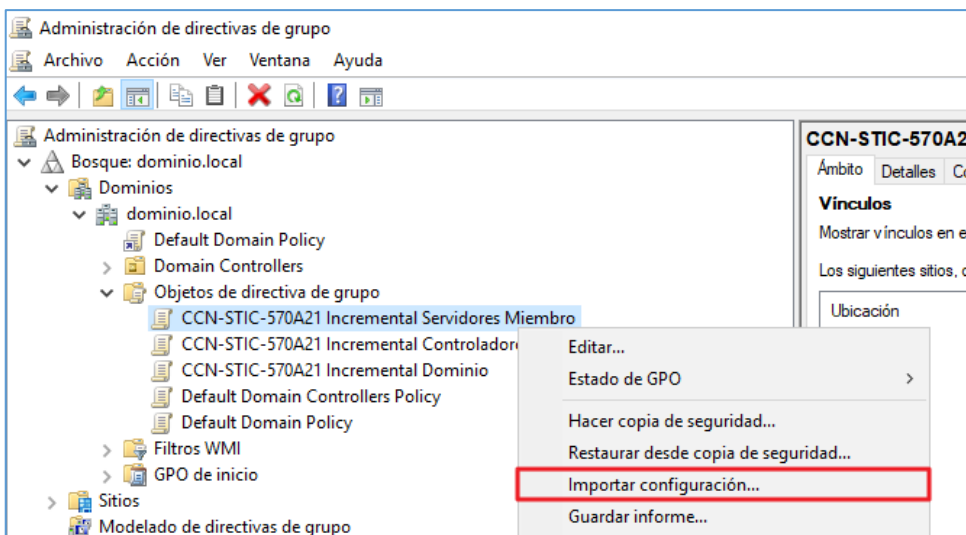
Paso	Descripción
19.	<p>En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A21 Incremental Dominio” y pulse el botón “Siguiente >”.</p> 
20.	<p>Para completar el asistente pulse el botón “Finalizar”.</p> 
21.	<p>Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración y continúe con el siguiente paso.</p>

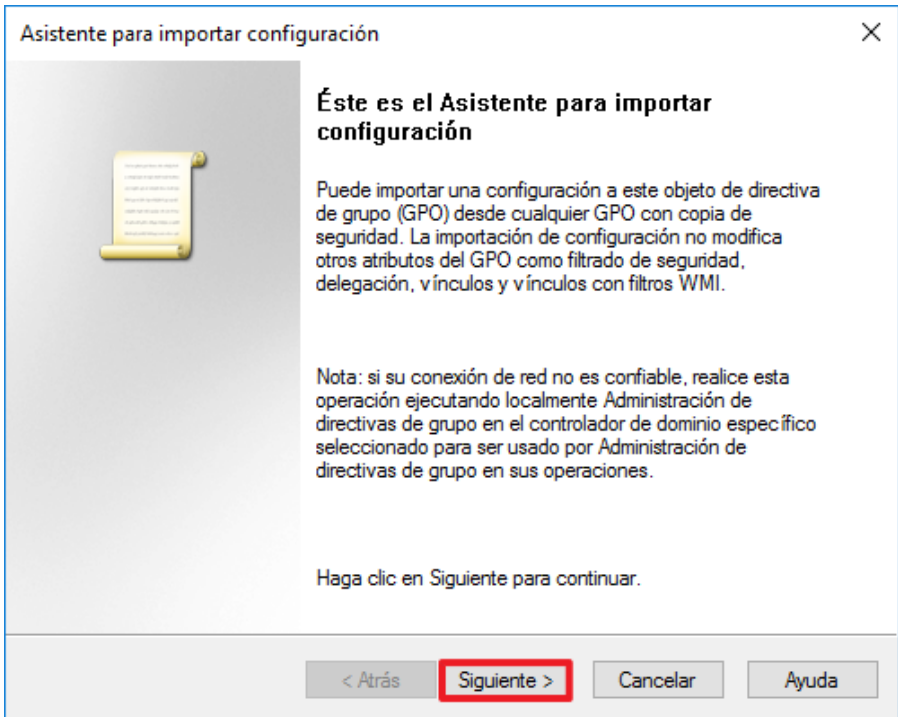
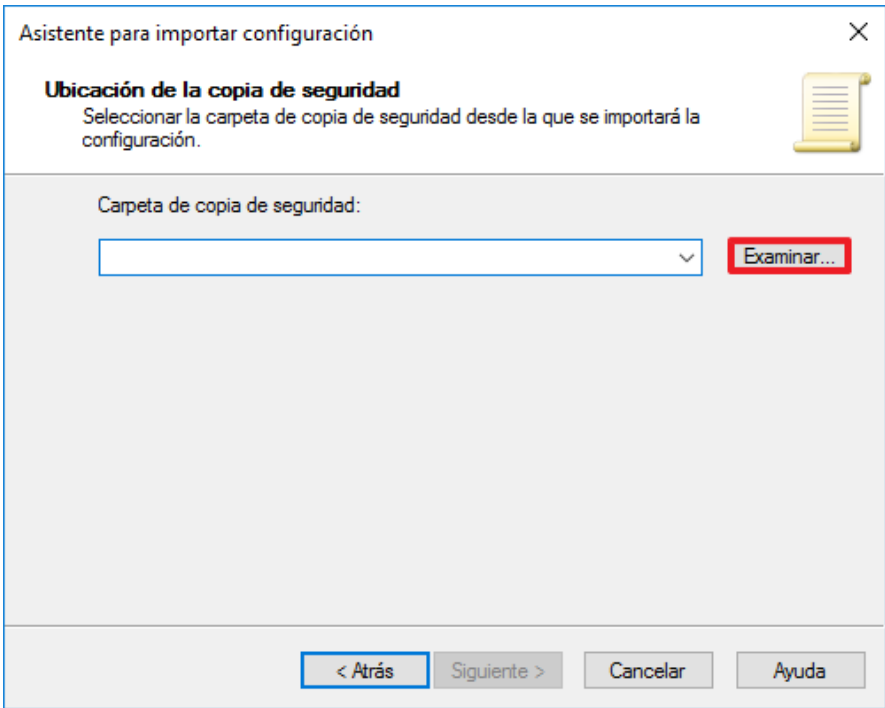
Paso	Descripción
22.	<p>Nuevamente, pulse con el botón derecho, sobre “Objetos de directiva de grupo” y seleccione la opción “Nuevo”.</p> 
23.	<p>Introduzca como nombre “CCN-STIC-570A21 Incremental Controladores de Dominio” y pulse el botón “Aceptar”.</p> 
24.	<p>Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración...”.</p> 

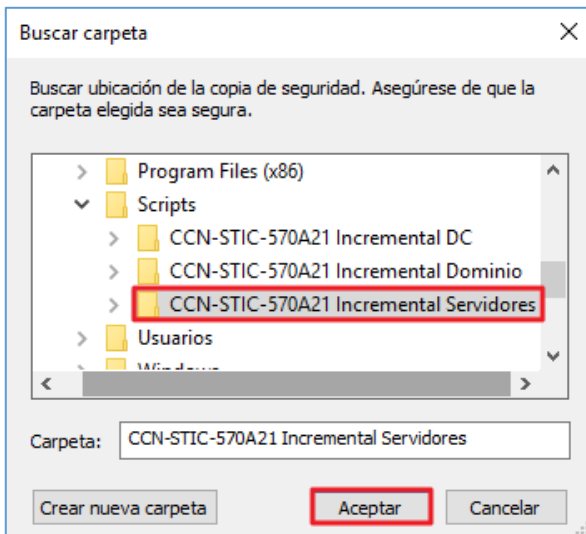
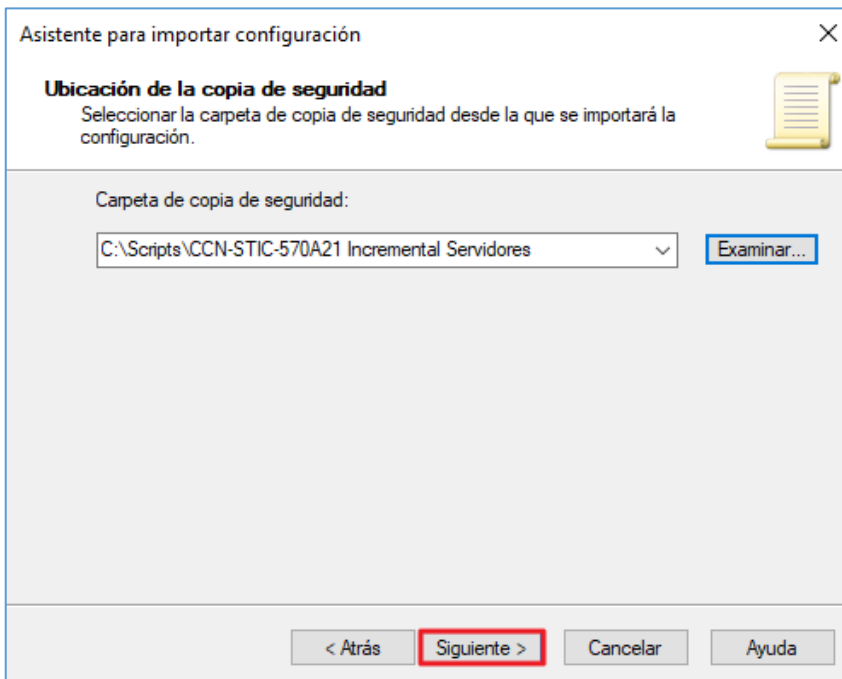
Paso	Descripción
25.	<p>En el asistente de importación de configuración, pulse el botón “Siguiente >”.</p> 
26.	<p>En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.</p>
27.	<p>En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.</p> 

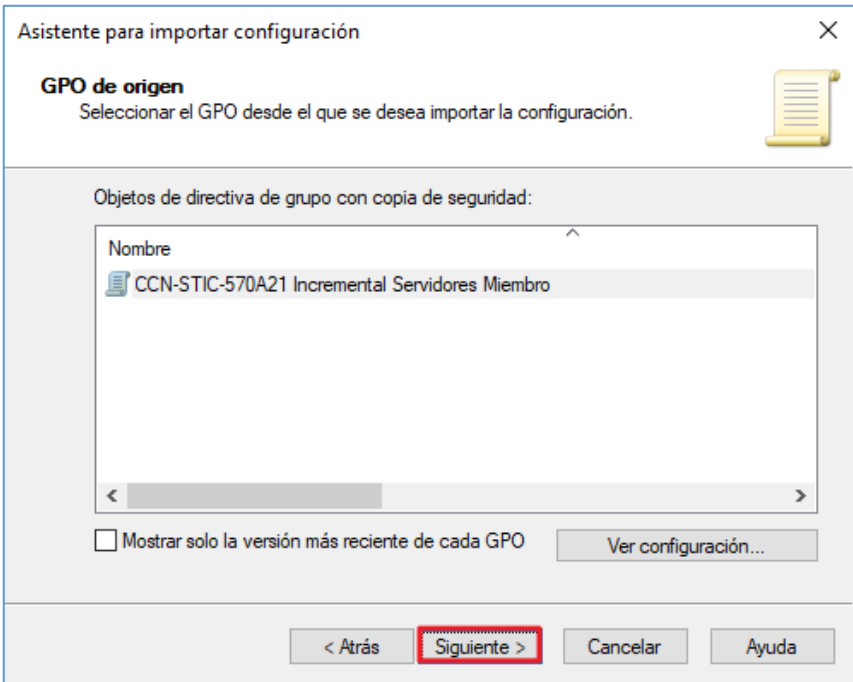
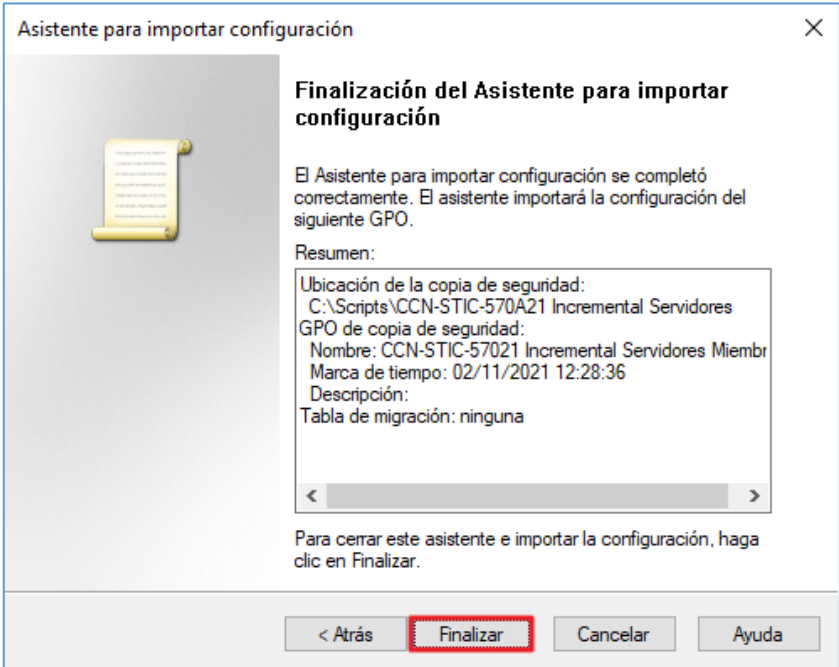
Paso	Descripción
28.	<p>Seleccione la carpeta “CCN-STIC-570A21 Incremental DC” que encontrará en el directorio “C:\Scripts” y pulse el botón “Aceptar”.</p> 
29.	<p>Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada.</p> 

Paso	Descripción
30.	<p>En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A21 Incremental Controladores de Dominio” y pulse el botón “Siguiente >”.</p> 
31.	<p>Para completar el asistente pulse el botón “Finalizar”.</p> 
32.	<p>Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración y continúe con el siguiente paso.</p>

Paso	Descripción
33.	<p>Para finalizar, pulse de nuevo con el botón derecho sobre “Objetos de directiva de grupo” y seleccione la opción “Nuevo”. En este punto se realiza la creación de la directiva de grupo para los Servidores Miembro con Windows Server 2019.</p> 
34.	<p>Introduzca como nombre “CCN-STIC-570A21 Incremental Servidores Miembro” y pulse el botón “Aceptar”.</p> 
35.	<p>Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración...”.</p> 

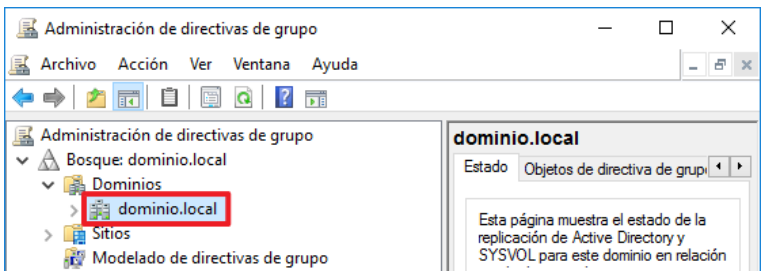
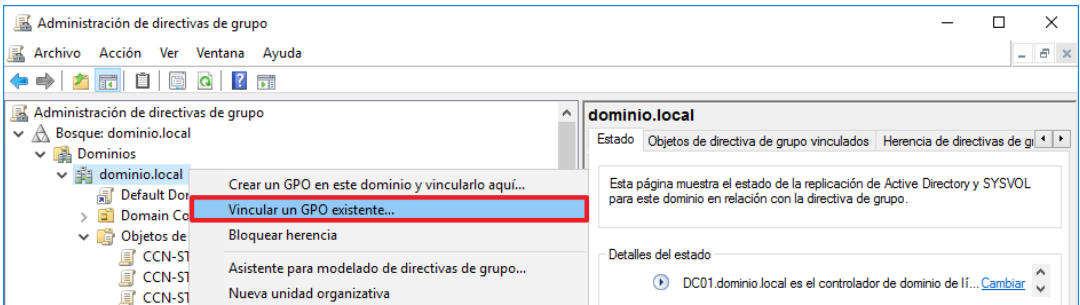
Paso	Descripción
36.	<p>En el asistente de importación de configuración, pulse el botón “Siguiente >”.</p> 
37.	<p>En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.</p>
38.	<p>En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.</p> 

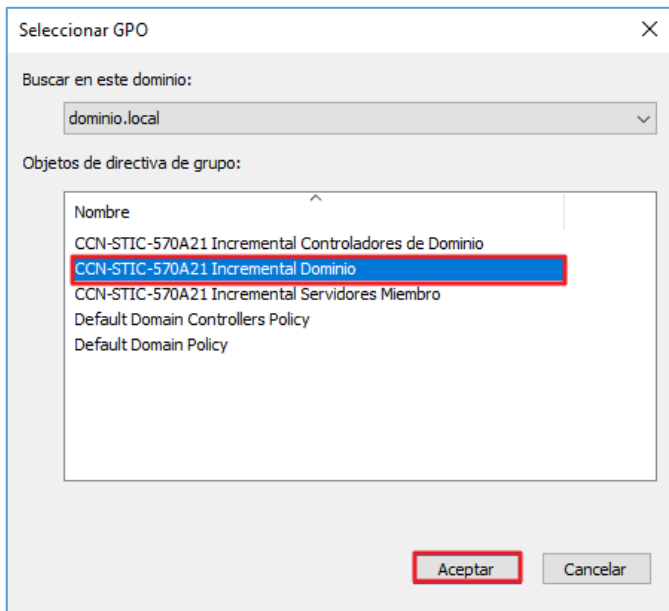
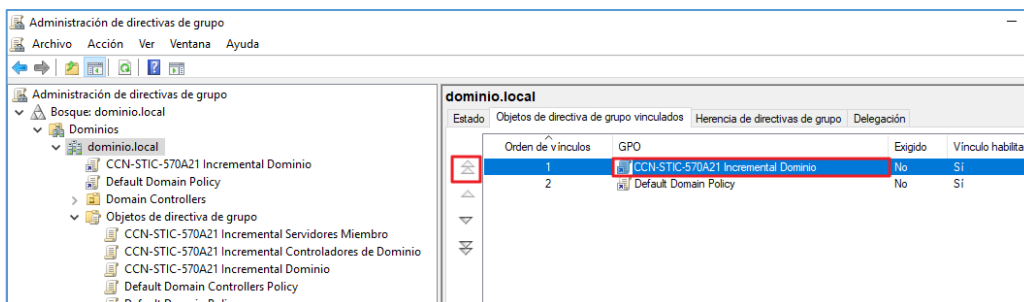
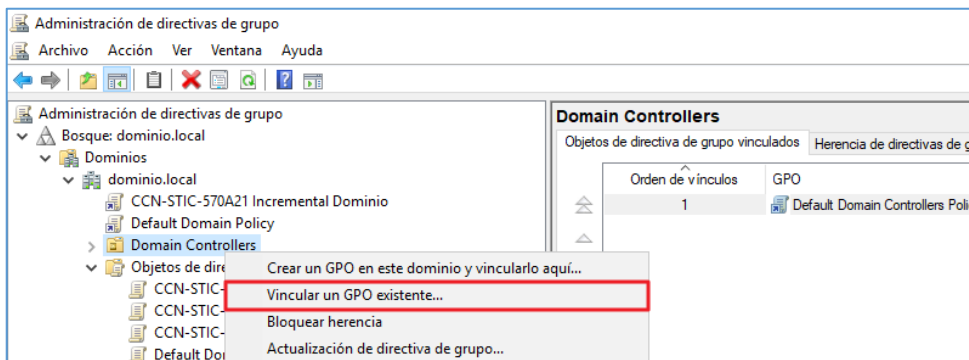
Paso	Descripción
39.	<p>Seleccione la carpeta “CCN-STIC-570A21 Incremental Servidores” que encontrará en el directorio “C:\Scripts” y pulse el botón “Aceptar”.</p> 
40.	<p>Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada.</p> 

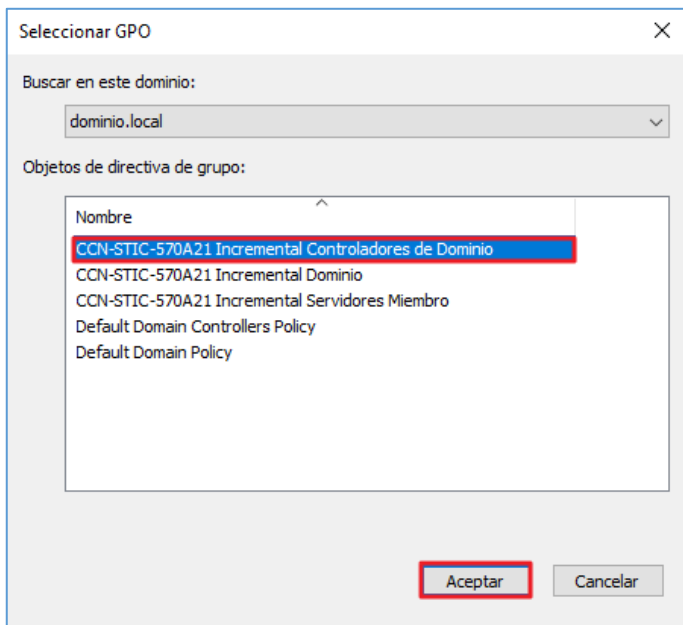
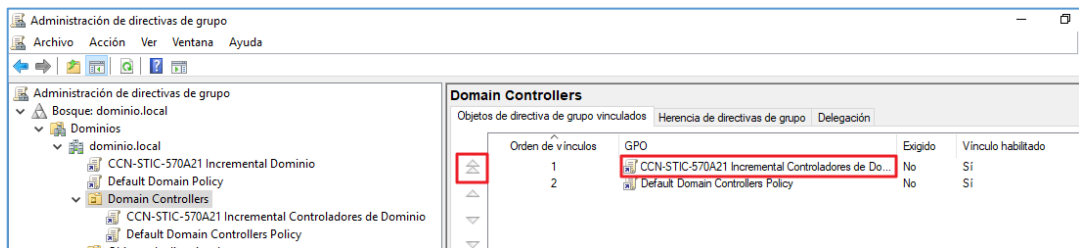
Paso	Descripción
41.	<p>En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A21 Incremental Servidores Miembro” y pulse el botón “Siguiente >”.</p> 
42.	<p>Para completar el asistente pulse el botón “Finalizar”.</p> 
43.	<p>Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración y continúe con el siguiente paso.</p>
44.	<p>Las políticas se encuentran ya creadas correctamente. No obstante, no se aplicarán hasta más adelante.</p>

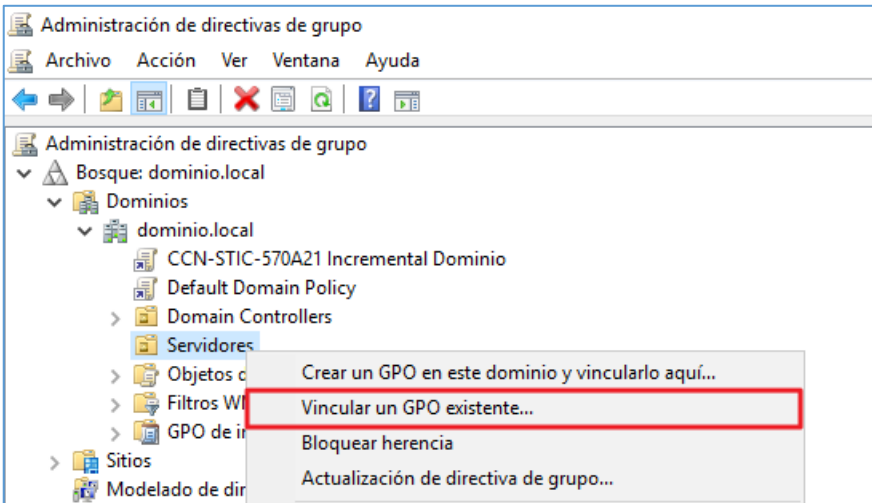
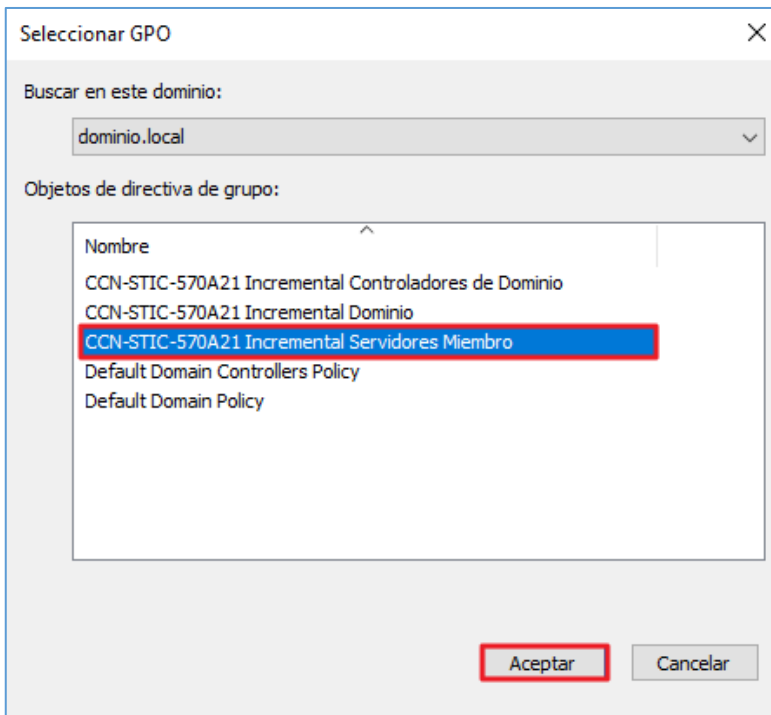
ANEXO A.2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

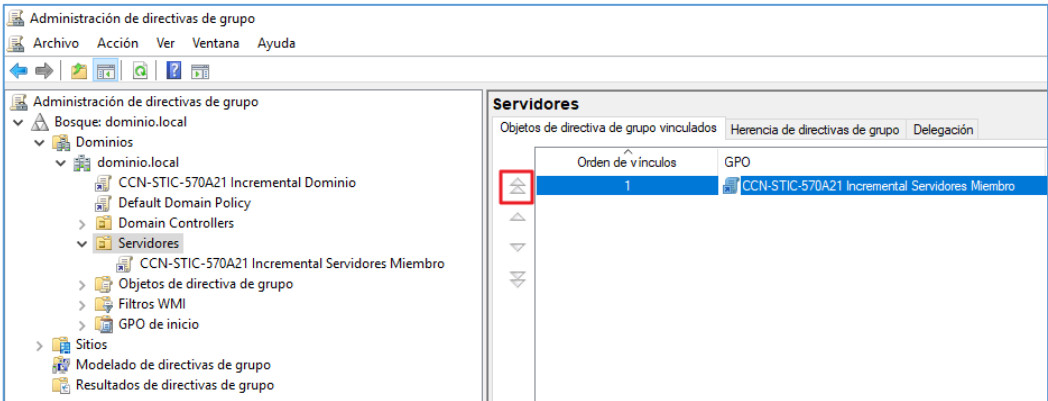
El presente punto establece la aplicación de las políticas de seguridad una vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
45.	Si previamente ha cerrado la consola, inicie la herramienta de administración de directivas de grupo de nuevo siguiendo para ello lo indicado en el paso “9”.
46.	<p>Despliegue el nodo y posicione sobre su dominio.</p>  <p>Nota: En el ejemplo el dominio utilizado se denomina “dominio.local”.</p>
47.	<p>Pulse con el botón derecho sobre el mismo y seleccione la opción “Vincular un GPO existente...”.</p> 

Paso	Descripción												
48.	<p>Seleccione la política “CCN-STIC-570A21 Incremental Dominio” y pulse el botón “Aceptar”.</p> <div></div>												
49.	<p>Una vez agregado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 570A21 Incremental Dominio”</p>												
50.	<p>Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC-570A21 Incremental Dominio” en primer lugar dentro del orden de vínculo.</p> <div></div> <table><thead><tr><th>Orden de vínculos</th><th>GPO</th><th>Exigido</th><th>Vínculo habilitado</th></tr></thead><tbody><tr><td>1</td><td>CCN-STIC-570A21 Incremental Dominio</td><td>No</td><td>Si</td></tr><tr><td>2</td><td>Default Domain Policy</td><td>No</td><td>Si</td></tr></tbody></table>	Orden de vínculos	GPO	Exigido	Vínculo habilitado	1	CCN-STIC-570A21 Incremental Dominio	No	Si	2	Default Domain Policy	No	Si
Orden de vínculos	GPO	Exigido	Vínculo habilitado										
1	CCN-STIC-570A21 Incremental Dominio	No	Si										
2	Default Domain Policy	No	Si										
51.	<p>Para continuar con la aplicación de las directivas anteriormente creadas, seleccione la Unidad Organizativa “Domain Controllers” y seleccione la opción “Vincular un GPO existente...”.</p> <div></div>												

Paso	Descripción												
52.	<p>Seleccione la política “CCN-STIC-570A21 Incremental Controladores de Dominio” y pulse el botón “Aceptar”.</p> <div></div>												
53.	<p>Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A21 Incremental Controladores de Dominio” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo.</p> <div><table><tr><th>Orden de vínculos</th><th>GPO</th><th>Exigido</th><th>Vínculo habilitado</th></tr><tr><td>1</td><td>CCN-STIC-570A21 Incremental Controladores de Do...</td><td>No</td><td>SI</td></tr><tr><td>2</td><td>Default Domain Controllers Policy</td><td>No</td><td>SI</td></tr></table></div>	Orden de vínculos	GPO	Exigido	Vínculo habilitado	1	CCN-STIC-570A21 Incremental Controladores de Do...	No	SI	2	Default Domain Controllers Policy	No	SI
Orden de vínculos	GPO	Exigido	Vínculo habilitado										
1	CCN-STIC-570A21 Incremental Controladores de Do...	No	SI										
2	Default Domain Controllers Policy	No	SI										

Paso	Descripción
54.	<p>Para finalizar con la aplicación de las directivas anteriormente creadas, seleccione la Unidad Organizativa “Servidores” y seleccione la opción “Vincular un GPO existente...”.</p>  <p>Nota: En este ejemplo se hace uso de la Unidad Organizativa (OU) “Servidores”. Si sus servidores con sistema operativo Windows Server 2019 se encontraran en otra ubicación vincule la siguiente GPO en dicha OU.</p>
55.	<p>Seleccione la política “CCN-STIC-570A21 Incremental Servidores Miembro” y pulse el botón “Aceptar”.</p> 

Paso	Descripción
56.	<p>Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A21 Incremental Servidores Miembro” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo.</p>  <p>Nota: Si la anterior directiva es la única vinculada a la unidad organizativa Servidores, no es necesario que realice este paso.</p>
57.	Cierre la herramienta de administración de directivas de grupo.
58.	Elimine la carpeta “C:\Scripts” de su servidor.

En este punto se encuentran configuradas y aplicadas las directivas sobre cada uno de los niveles descritos en la presente guía, no obstante, puede realizar la ejecución del comando “gpupdate /force” sobre los distintos servidores y controladores de dominio de su organización.

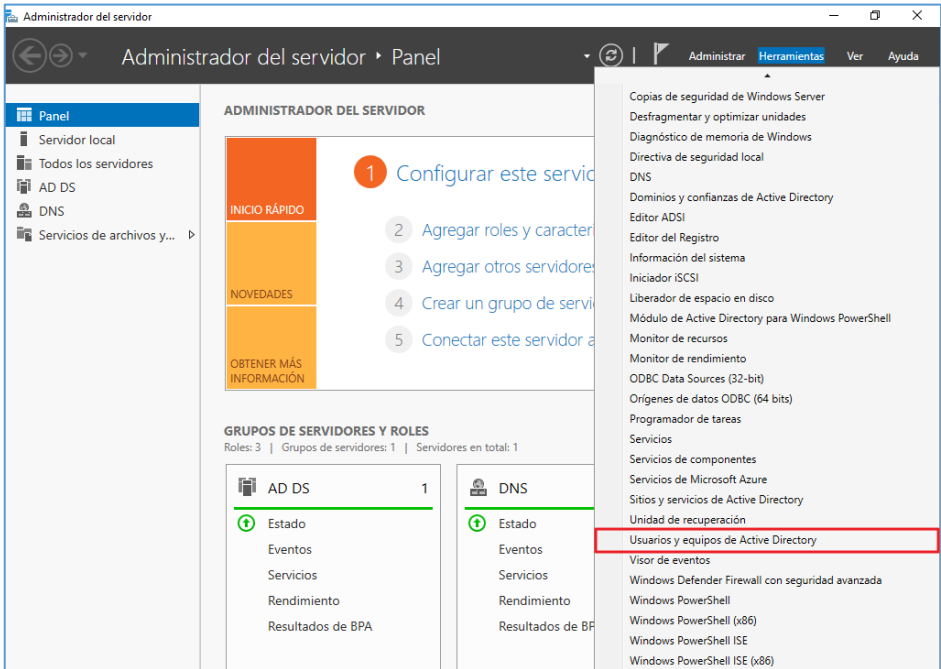
ANEXO A.3. CONFIGURACIONES ADICIONALES

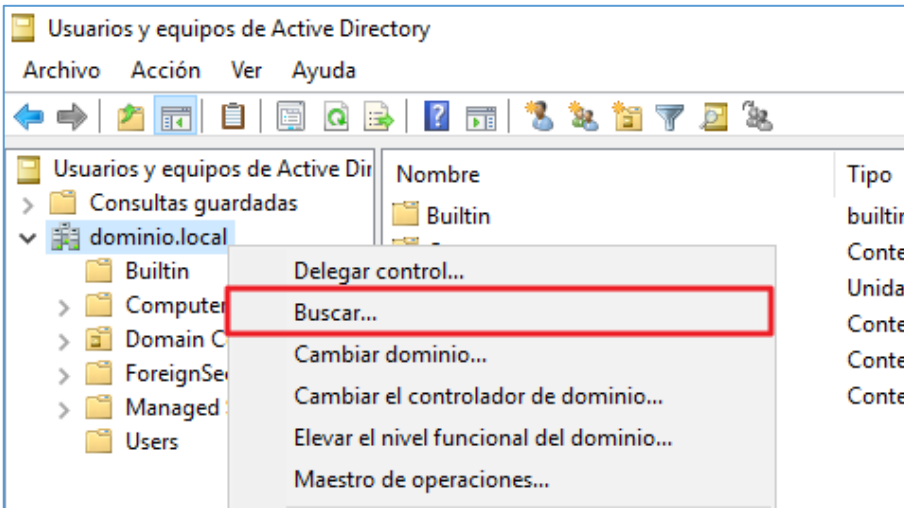
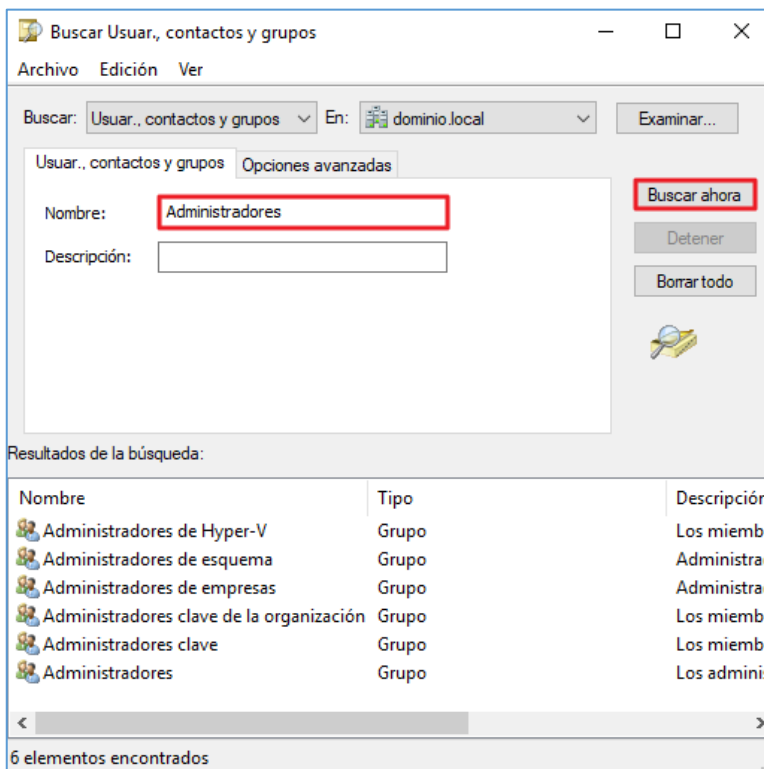
El presente apartado recoge aquellas categorías de perfilado de seguridad asociadas a un riesgo concreto las cuales no pueden ser aplicadas por medio de configuraciones a nivel de Windows al depender del entorno en el que vaya a realizarse la aplicación del bastionado. Esto puede deberse a muchos factores, entre ellos el uso de otro software que realiza la misma función o bien debido a que se establecen las medidas que evitan el riesgo por medio otros parámetros y/o configuraciones.




















Para estos casos, se desarrolla el presente anexo, en el cual se establecen comentarios sobre las categorías de perfilado de seguridad afectadas y se determina un ejemplo de configuración o validación que permita garantizar el aseguramiento de los sistemas operativos Windows Server 2019 con la premisa de apoyar a los operadores a realizar un correcto aseguramiento de los sistemas operativos.

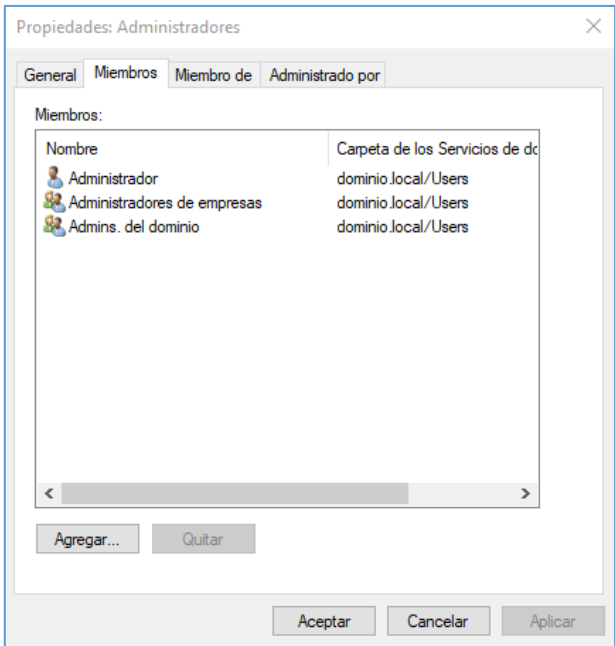
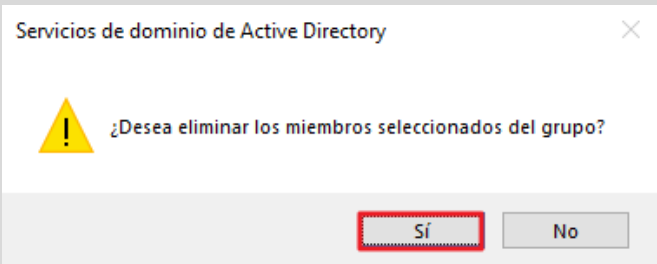
Categorías de perfilado de seguridad:

- a) [A.4.SEC1] Los usuarios estándar no disponen de permisos de administrador local. Para cumplir con esta premisa se debe revisar por cada servidor y/o equipo que cuente con el sistema operativo Windows Server 2019, que los grupos Administradores y Administradores del dominio (Admins. del Dominio) no contienen usuarios no necesarios.

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-570A21.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Ejecute el “Administrador del Servidor” por medio del botón “Inicio → Administrador del Servidor”.
4.	<p>Pulse sobre el apartado “Herramientas” y abra la consola “Usuarios y equipos de Active Directory”.</p>  <p>Nota: Al abrir la aplicación, puede que el control de cuentas de usuario le solicite las credenciales de un administrador.</p>

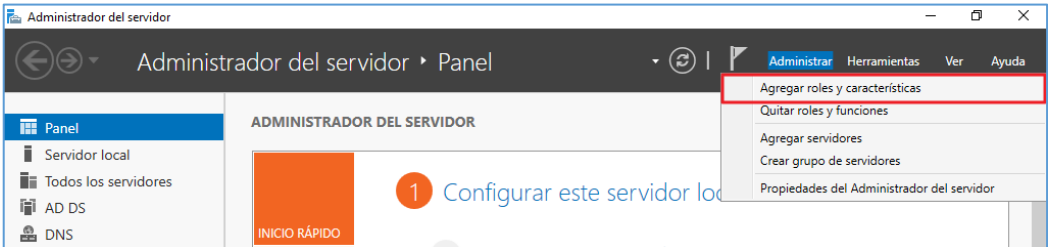
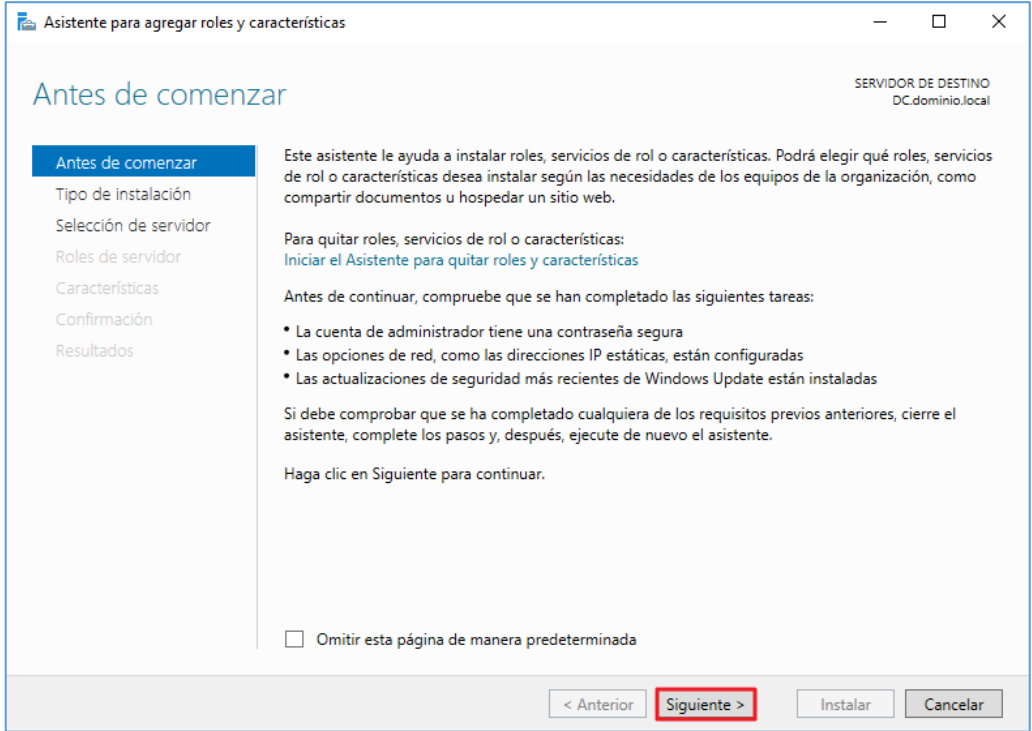
Paso	Descripción
5.	<p>Despliegue el árbol de su dominio y pulse con el botón derecho sobre el mismo, sobre el menú desplegable, pulse sobre “Buscar”.</p> 
6.	<p>Sobre la consola emergente, introduzca el nombre del grupo a verificar y pulse sobre “Buscar ahora”, esta acción mostrará todos los resultados que coincidan con los parámetros introducidos. En este caso, a modo de ejemplo, se introduce el grupo Administradores.</p>  <p>Nota: Los resultados de la búsqueda pueden variar en función de su organización.</p>

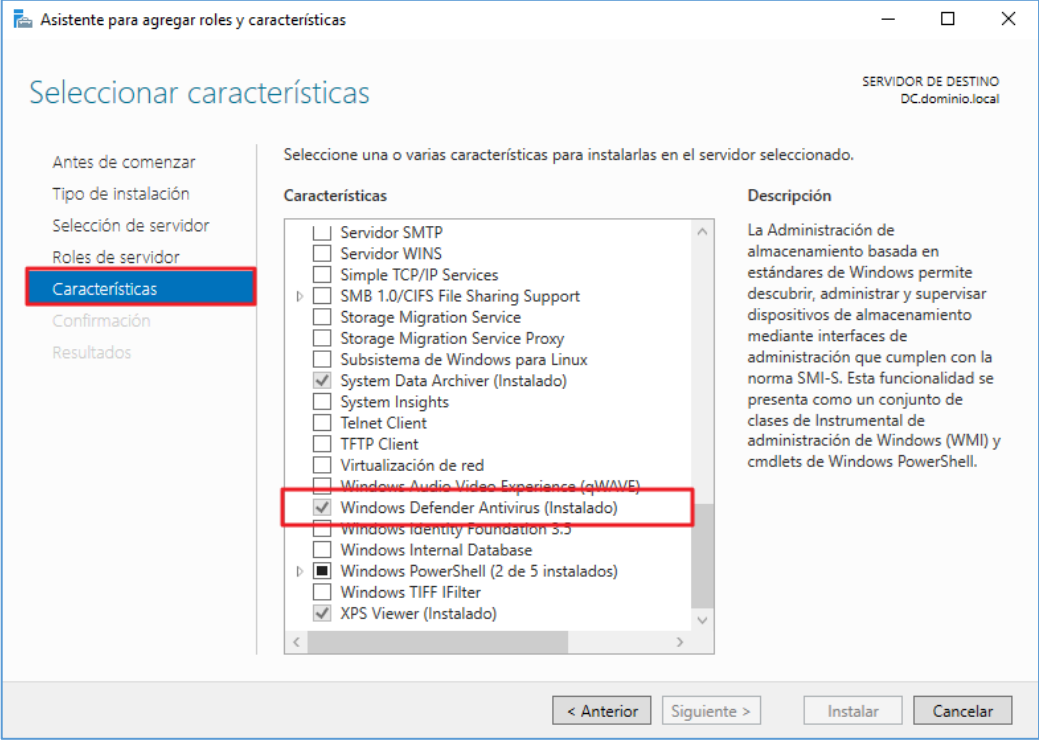
Paso	Descripción																					
7.	<p>Sobre los resultados anteriores, haga doble click sobre el grupo “Administradores”.</p> <div><p>Resultados de la búsqueda:</p><table><thead><tr><th>Nombre</th><th>Tipo</th><th>Descripción</th></tr></thead><tbody><tr><td> Administradores de Hyper-V</td><td>Grupo</td><td>Los miemb</td></tr><tr><td> Administradores de esquema</td><td>Grupo</td><td>Administrad</td></tr><tr><td> Administradores de empresas</td><td>Grupo</td><td>Administrad</td></tr><tr><td> Administradores clave de la organización</td><td>Grupo</td><td>Los miemb</td></tr><tr><td> Administradores clave</td><td>Grupo</td><td>Los miemb</td></tr><tr><td> Administradores</td><td>Grupo</td><td>Los administ</td></tr></tbody></table><p>< ></p><p>6 elementos encontrados</p></div>	Nombre	Tipo	Descripción	 Administradores de Hyper-V	Grupo	Los miemb	 Administradores de esquema	Grupo	Administrad	 Administradores de empresas	Grupo	Administrad	 Administradores clave de la organización	Grupo	Los miemb	 Administradores clave	Grupo	Los miemb	 Administradores	Grupo	Los administ
Nombre	Tipo	Descripción																				
 Administradores de Hyper-V	Grupo	Los miemb																				
 Administradores de esquema	Grupo	Administrad																				
 Administradores de empresas	Grupo	Administrad																				
 Administradores clave de la organización	Grupo	Los miemb																				
 Administradores clave	Grupo	Los miemb																				
 Administradores	Grupo	Los administ																				
8.	<p>Se abrirán las propiedades del grupo seleccionado. Pulse sobre el apartado “Miembros”.</p> <div><p>Propiedades: Administradores</p><p>General Miembros Miembro de Administrado por</p><div> Administradores</div><p>Nombre de grupo (anterior a Windows 2000): Administradores</p><p>Descripción: Los administradores tienen acceso completo y sin res</p><p>Correo electrónico:</p><div><p>Ámbito de grupo</p><p><input checked="" type="radio"/> Integrado local <input type="radio"/> Global <input type="radio"/> Universal</p><p>Tipo de grupo</p><p><input checked="" type="radio"/> Seguridad <input type="radio"/> Distribución</p></div><p>Notas:</p><div></div><p>Aceptar Cancelar Aplicar</p></div>																					

Paso	Descripción
9.	<p>En este punto, deberá asegurarse de que este grupo contiene los usuarios que necesitan los privilegios administrativos sobre su organización, elimine cualquier usuario innecesario del grupo de seguridad. Para ello, seleccione el usuario y pulse sobre “Quitar”.</p>  <p>Nota: Al quitar un usuario o grupo desde la ventana anterior, le aparecerá una advertencia de confirmación, pulse sobre “Sí” únicamente si está completamente seguro.</p> 
10.	<p>Repita los pasos anteriores para cada uno de los grupos administrativos de su organización, como mínimo, revise que los grupos “Administradores” y “Admins. Del dominio” contienen los usuarios imprescindibles para su entorno.</p>

- b) [A.4.SEC2] El sistema tiene un antivirus y éste está actualizado. Todos los sistemas operativos Windows Server 2019 deben contar con un Antivirus instalado, activo y totalmente actualizado con las definiciones de virus al día. En el caso de no contar con otro antivirus, Windows Defender estará habilitado como antivirus por defecto en el equipo.

Para evaluar la activación y estado de dicho elemento deberá realizar los siguientes pasos.

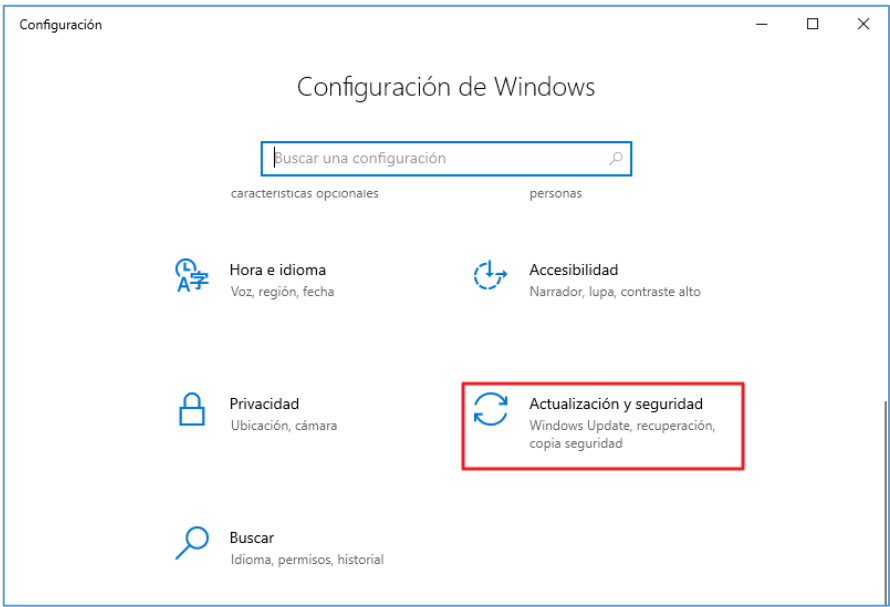
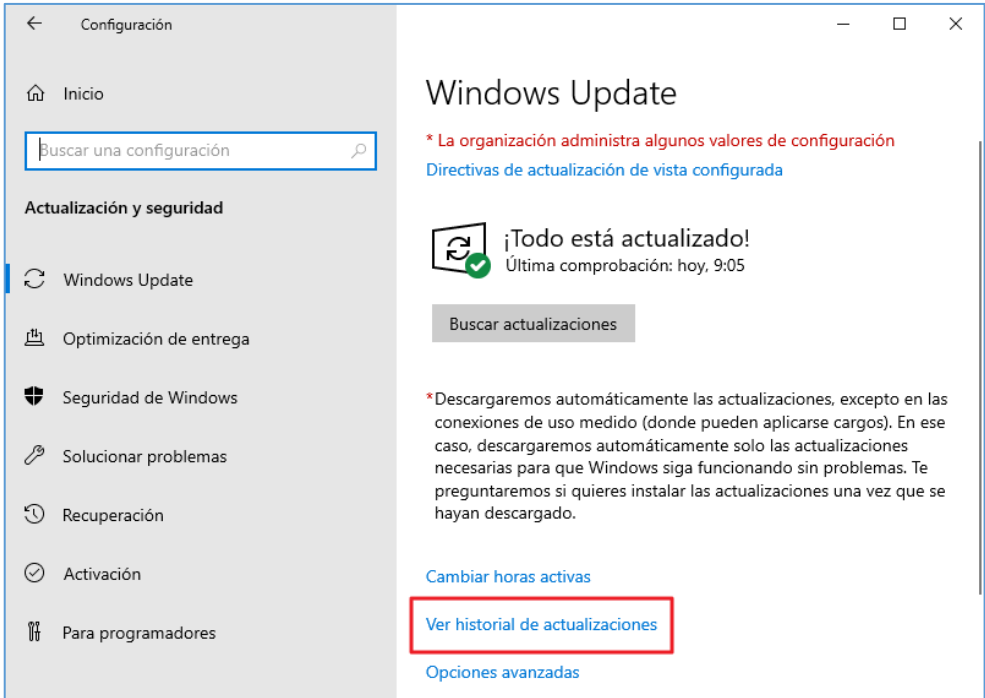
Paso	Descripción
1.	Inicie sesión en un servidor del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-570A21.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Ejecute el “Administrador del Servidor” por medio del botón “Inicio → Administrador del Servidor”.
4.	Pulse sobre el botón “Administrar” en la esquina superior derecha y sobre el menú desplegable pulse sobre “Agregar roles y características”.
	
5.	Se iniciará el asistente para agregar roles y características. Pulse sobre “Siguiente” hasta llegar al apartado “Características”.
	

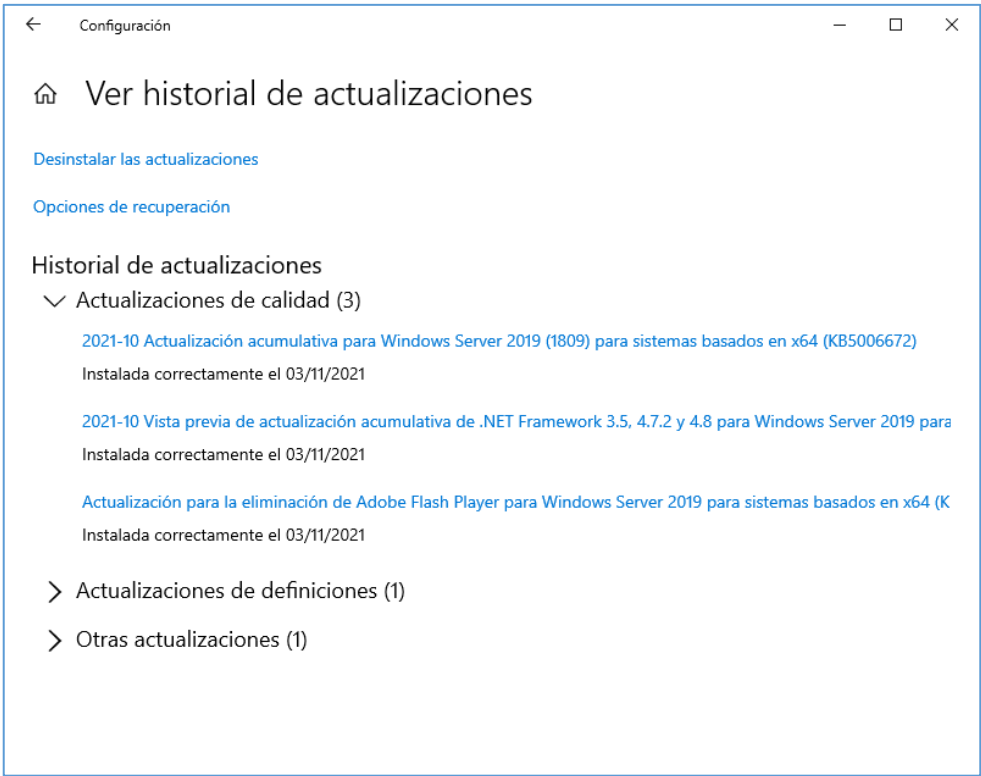
Paso	Descripción
6.	<p>Sobre el apartado “Características” utilizando la barra de desplazamiento, localice la característica “Windows Defender Antivirus”. Si en su sistema se encuentra ya instalada dicha característica, aparecerá marcada y no podrá seleccionarla.</p> 
7.	<p>En el caso de haber desinstalado Windows Defender de su sistema, marque la opción anterior y continúe con el asistente para realizar la instalación de Windows Defender sobre Windows Server 2019.</p> <p>Nota: Por defecto, esta característica se encuentra instalada en los servidores con el sistema operativo Windows Server 2019.</p>

- a) [A.8.SEC2] El sistema operativo está actualizado. Se debe asegurar que los equipos cuentan con las actualizaciones mensuales que proporciona el fabricante. Puede realizar esta actualización de forma manual o apoyarse en algún sistema de control de actualizaciones.

Paso	Descripción
1.	Inicie sesión en un servidor del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-570A21.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio o con un usuario con privilegios de administración sobre el servidor.
3.	Ejecute el aplicativo “Configuración” por medio del botón “Inicio → Configuración”.

Nota: La imagen ilustra dos formas de acceder al mismo panel de configuración. Únicamente deberá pulsar sobre una de las dos opciones.

Paso	Descripción
4.	<p>En el menú de Configuración de Windows localice el apartado “Actualización y seguridad” y acceda al mismo.</p> 
5.	<p>En la vista general se puede apreciar el estado de actualizaciones de su equipo, si no existen actualizaciones disponibles se indicará mediante un mensaje. Este mensaje puede indicar que no hay actualizaciones disponibles para descargar desde su punto de actualización lo que puede llevarle a pensar que su sistema está completamente actualizado.</p> <p>Para confirmar que el sistema operativo tiene instaladas las actualizaciones del mes vigente deberá acceder al apartado “Ver historial de actualizaciones”.</p> 

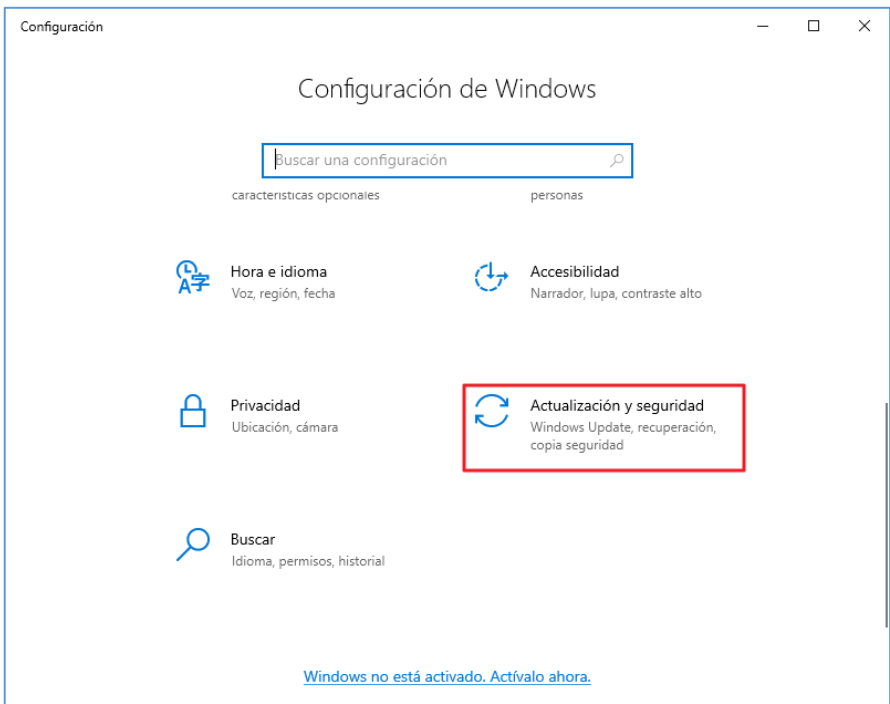
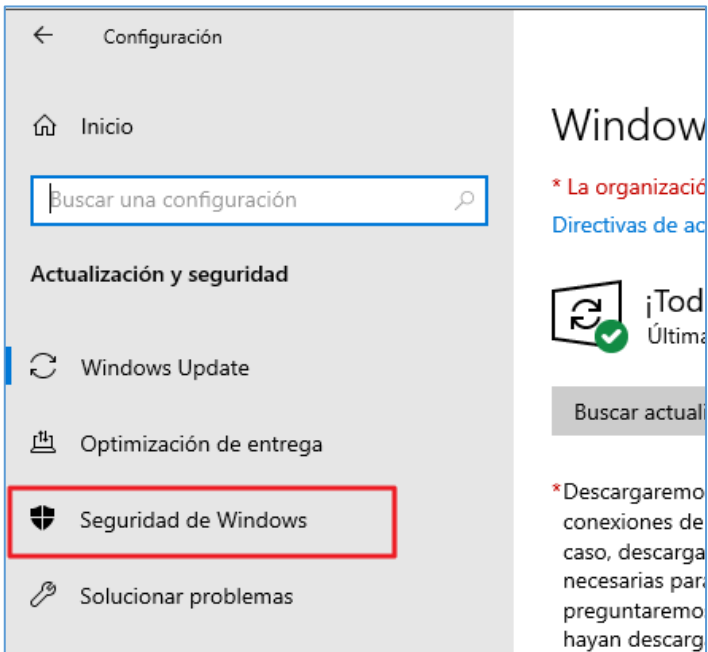
Paso	Descripción
6.	<p>En el historial de actualizaciones encontrará las actualizaciones del mes vigente, en caso de no ser así, contacte con su equipo de actualización para que le proporcione las últimas actualizaciones de Windows Server 2019.</p> 

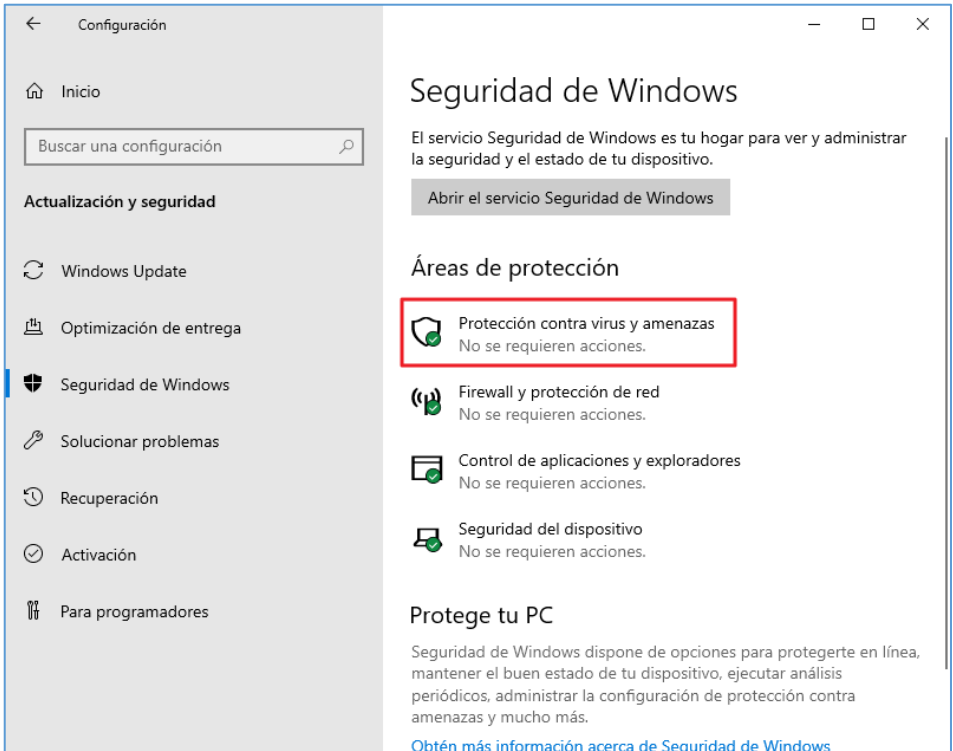
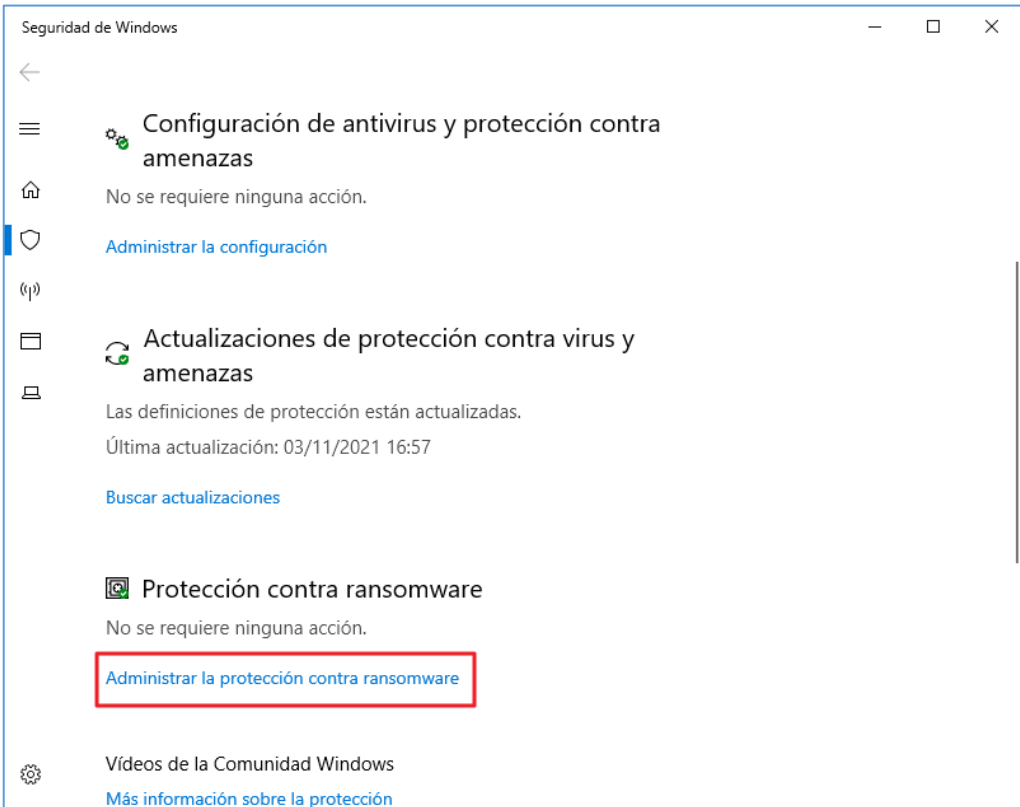
- b) [A.8.SEC6] Se dispone de medidas anti ransomware habilitadas. Si su infraestructura cuenta con un sistema antivirus con dichas funcionalidades, estas, deberán ser habilitadas por los administradores para garantizar la seguridad ante el riesgo de ransomware.

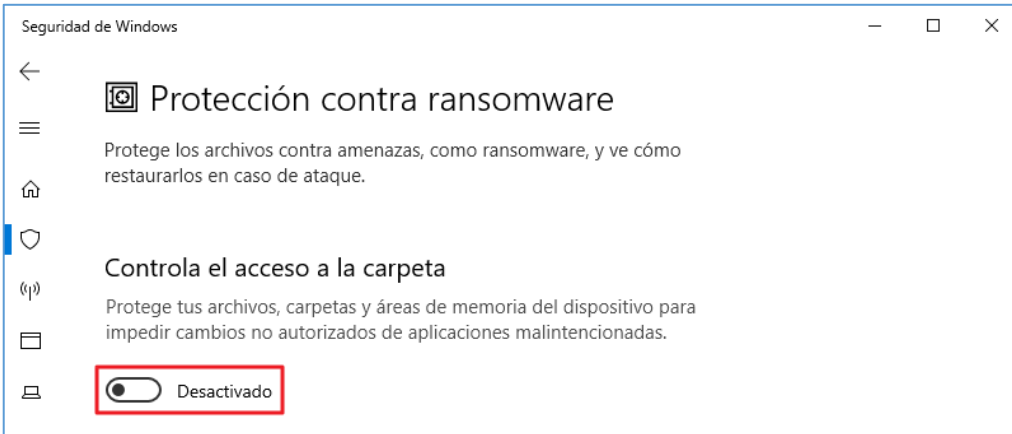
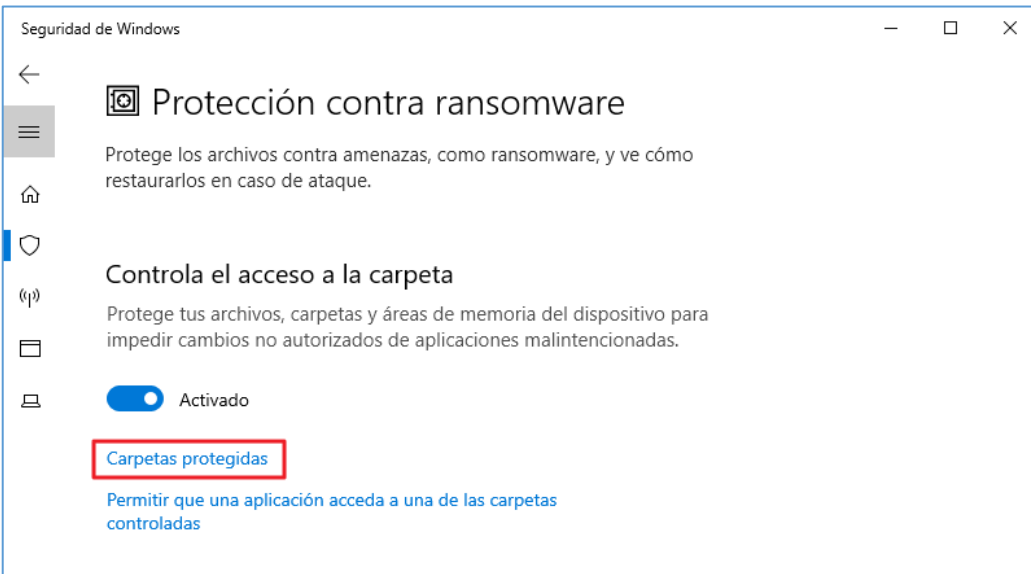
En el caso de no contar con ninguna medida anti ransomware, y si está haciendo uso del antivirus Windows Defender podrá hacer uso de los siguientes pasos para habilitar esta funcionalidad.

Paso	Descripción
1.	Inicie sesión en un servidor del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-570A21.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio o con un usuario con privilegios de administración sobre el servidor.
3.	Ejecute el aplicativo “Configuración” por medio del botón “Inicio → Configuración”.

Nota: La imagen ilustra dos formas de acceder al mismo panel de configuración. Únicamente deberá pulsar sobre una de las dos opciones.

Paso	Descripción
4.	<p>En el menú de Configuración de Windows localice el apartado “Actualización y seguridad” y acceda al mismo.</p> 
5.	<p>A continuación, pulse sobre “Seguridad de Windows”.</p> 

Paso	Descripción
6.	<p>En el nodo de configuración, pulse sobre “Protección contra virus y amenazas”</p> 
7.	<p>Se abrirá el panel de seguridad de Windows con las distintas funciones de Windows Defender. Localice la funcionalidad “Protección contra ransomware” y haga click sobre “Administrar la protección contra ransomware”.</p> 

Paso	Descripción
8.	<p>Por defecto, la mayoría de los sistemas mantienen dicha protección desactivada, en este caso deberá habilitar la funcionalidad pulsando sobre la barra de activación.</p> 
9.	<p>Al habilitar la funcionalidad, se protegen automáticamente ciertas rutas del sistema. Puede gestionar las rutas, añadiendo o quitando carpetas desde el apartado "Carpetas protegidas".</p> 

- c) [A.23.SEC1] Se controla la instalación y uso de cualquier dispositivo conectado al equipo. Se deberán establecer directivas o un software que permitan bloquear el uso y/o instalación de drivers no permitidos, impidiendo así el uso de dispositivos de almacenamiento externos.

Puede realizar esta acción mediante directivas de Windows o utilizando medidas de seguridad que proporcione otro fabricante, siempre garantizando que únicamente los dispositivos permitidos están disponibles para su instalación en los sistemas.

En la siguiente tabla, se describen las directivas a implementar sobre un objeto GPO del dominio para restringir y proteger la instalación de dispositivos en los sistemas que cuenten con sistema operativo Windows Server 2019. Todas las directivas se encuentran bajo el siguiente árbol de configuración.

- i. Configuración de equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos

Categoría	Directiva	Configuración
[A.23.SEC1] Se controla la instalación y uso de cualquier dispositivo conectado al equipo.	Impedir la instalación de dispositivos no descritos por otras configuraciones de directiva	Habilitado
	Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos	Deshabilitada
	Permitir la instalación de dispositivos con controladores que coincidan con estas clases de instalación de dispositivos	Habilitado (Incluir los GUID de sus dispositivos)
	Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. De dispositivo	Habilitado (Incluir los identificadores hardware de sus dispositivos)

- d) [A.25.SEC1] El disco del sistema está cifrado. Para cumplir con las configuraciones descritas en el riesgo A.25.SEC1 el sistema operativo deberá contar con una característica o software que permita el cifrado de los discos.

En este ejemplo se hace uso de la característica nativa de Windows BitLocker. Para habilitar y configurar este software puede guiarse de la siguiente tabla, la cual incluye las directivas a aplicar para una primera configuración de la funcionalidad.

Todas las directivas se encuentran bajo el siguiente nodo de configuración:

- i. Configuración de equipo → Plantillas administrativas → Componentes de Windows → Cifrado de la unidad BitLocker → Unidades de sistema operativo

Categoría	Directiva	Configuración
[A.25.SEC1] El disco del sistema está cifrado.	Configurar longitud mínima de PIN para el inicio	5
	Elegir cómo se pueden recuperar unidades fijas protegidas por BitLocker	Habilitado
	Permitir agente de recuperación de datos.	Habilitado
	Guardar información de recuperación de BitLocker en AD DS para unidades del sistema operativo.	Habilitado
	Configurar almacenamiento de la información de recuperación de BitLocker en AD DS:	Realizar copia de seguridad de contraseñas de recuperación y paquetes de claves.
	No habilitar BitLocker hasta que la información de recuperación se almacene en AD DS para unidades del sistema operativo.	Habilitado
	No permitir que usuarios estándar cambien el PIN o la contraseña	Habilitado
	Requerir autenticación adicional al iniciar.	Habilitado
	Permitir agente de recuperación de datos.	Habilitado

Categoría	Directiva	Configuración
	Configurar almacenamiento de usuario de la información de recuperación de BitLocker	Permitir contraseña de recuperación de 48 dígitos. Permitir clave de recuperación de 256 bits
	Guardar información de recuperación de BitLocker en AD DS para unidades de datos fijas.	Habilitado
	Configurar almacenamiento de la información de recuperación de BitLocker en AD DS:	Realizar copia de seguridad de contraseñas de recuperación y paquetes de claves.
	No habilitar BitLocker hasta que la información de recuperación se almacene en AD DS para unidades de datos fijas.	Deshabilitado

- a) [A.25.SEC2] El disco de datos está cifrado. Al igual que en el apartado anterior, para cumplir con las configuraciones descritas en el riesgo A.25.SEC2 el sistema operativo deberá contar con una característica o software que permita el cifrado de los discos que contienen los datos.

En este ejemplo se hace uso de la característica nativa de Windows BitLocker. Para habilitar y configurar este software puede guiarse de la siguiente tabla, la cual incluye las directivas a aplicar para una primera configuración de la funcionalidad.

Todas las directivas se encuentran bajo los siguientes nodos de configuración:

- Configuración de equipo → Plantillas administrativas → Componentes de Windows → Cifrado de la unidad BitLocker → Unidades de datos extraíbles
- Configuración de equipo → Plantillas administrativas → Componentes de Windows → Cifrado de la unidad BitLocker → Unidades de datos fijas

Categoría	Directiva	Configuración
[A.25.SEC2] El disco de datos está cifrado.	Elegir cómo se pueden recuperar unidades extraíbles protegidas por BitLocker	Habilitado
	Permitir agente de recuperación de datos.	Habilitado
	Configurar almacenamiento de usuario de la información de recuperación de BitLocker	Permitir contraseña de recuperación de 48 dígitos. Permitir clave de recuperación de 256 bits

Categoría	Directiva	Configuración
	Guardar información de recuperación de BitLocker en AD DS para unidades de datos extraíbles.	Habilitado
	Configurar almacenamiento de la información de recuperación de BitLocker en AD DS:	Realizar copia de seguridad de contraseñas de recuperación y paquetes de claves.
	No habilitar BitLocker hasta que la información de recuperación se almacene en AD DS para unidades de datos extraíbles.	Deshabilitado
	Elegir cómo se pueden recuperar unidades fijas protegidas por BitLocker	Habilitado
	Permitir agente de recuperación de datos.	Habilitado
	Configurar almacenamiento de usuario de la información de recuperación de BitLocker	Permitir contraseña de recuperación de 48 dígitos. Permitir clave de recuperación de 256 bits
	Guardar información de recuperación de BitLocker en AD DS para unidades de datos fijas.	Habilitado
	Configurar almacenamiento de la información de recuperación de BitLocker en AD DS:	Realizar copia de seguridad de contraseñas de recuperación y paquetes de claves.
	No habilitar BitLocker hasta que la información de recuperación se almacene en AD DS para unidades de datos fijas.	Deshabilitado

