centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-577A21

GUÍA DE APLICACIÓN DE PERFILADO DE SEGURIDAD PARA MICROSOFT SHAREPOINT SERVER 2019 EN MICROSOFT WINDOWS SERVER 2019

SEPTIEMBRE 2022

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.22 12:51:37 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-241-1

Fecha de Edición: septiembre 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

ÍNDICE

1. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos Microsoft (CCN STIC 500), siendo de aplicación para la Administración pública 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 consecutivamente varias de estas guías. En este sentido, se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

2. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para aplicar un perfilado de seguridad basado en la realización de un análisis de riesgos en servidores que tengan instalado Microsoft SharePoint Server 2019, en sistemas con servidores Microsoft Windows Server 2019 y que actúen bien como controlador de dominio o como servidor miembro de un dominio.

Las configuraciones que se aplican a través de la presente guía se han 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 del 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) utilizará de base los niveles del Esquema Nacional de Seguridad validados por el análisis de riesgos preceptivo utilizado en base a una categorización ENS MEDIO.

e) Las medidas de seguridad se podrán aplicar a sistemas ya implementados o nuevos sistemas, minimizando el impacto en la producción.

f) Las guías se revisarán y se actualizarán según las nuevas amenazas y estado del 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 quien implemente las medidas que 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 SharePoint 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 al 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, 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 del 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 el escenario planteado. En particular, se incluirá la configuración para aplicar un perfilado de seguridad de alcance intermedio de un servidor con Microsoft SharePoint Server 2019, instalado en español, con la versión completa del producto, bajo el sistema operativo Microsoft Windows Server 2019, que actúe bien como servidor controlador de dominio, o bien como servidor miembro de un dominio.

Por otro lado, hay que señalar que los equipos que formen el sistema deberán tener aplicadas las medidas de seguridad propias del sistema operativo subyacente, al margen de las medidas propias del servicio de SharePoint Server 2019. Así pues, deberá aplicarse la guía “CCN-STIC 570A21 Guía de aplicación de perfilado de seguridad para Windows Server 2019”.

Para garantizar la seguridad de los equipos cliente 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 el segundo 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 esta guía 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.

Este documento 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 de la 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 del 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 de la que trata la 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**: 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 dónde 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 mitigadora correspondiente a 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.

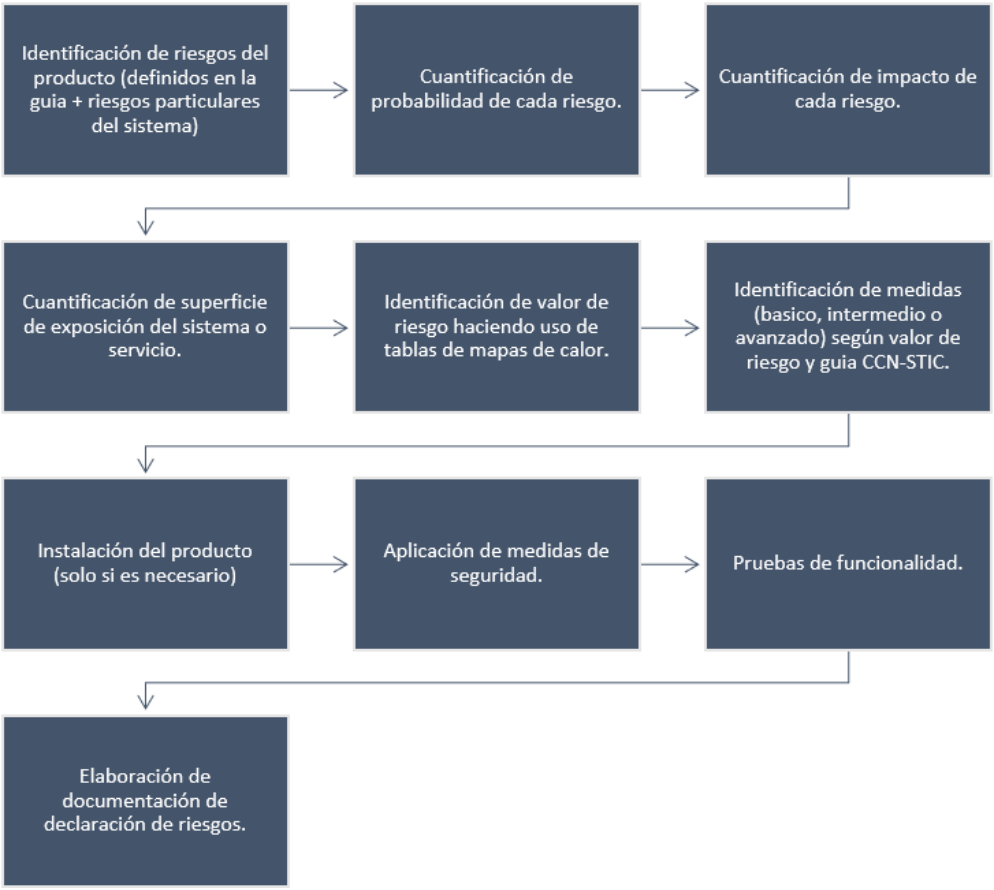
   Cada organización deberá determinar cómo configurar el sistema para el cumplimiento de la medida correspondiente. De esta forma, se ofrece un mayor grado de flexibilidad a la hora de proteger el sistema, necesario sobre todo en sistemas que ya están en funcionamiento o en producción. Es decir, en esta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

g) **Instalación del producto (en nuevas instalaciones)**: Una vez conocidos los riesgos y las medidas de mitigación de estos, se procederá con la instalación del sistema operativo en el caso de nuevas implementaciones. En caso de que el sistema ya se encuentre instalado, se procederá a instalar el producto objeto de la guía.

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 establezcan 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 aplicación, 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 que hace uso de Microsoft SharePoint 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.

a) El primer escenario será un sistema aislado en red, es decir, que estará conectado 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, es decir, que tendría la capacidad de establecer conexiones con elementos de red externos de una organización o entidad.

5.1 RIESGOS ASOCIADOS A MICROSOFT SHAREPOINT 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 podrán 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 (log)			
2.	[A.4] Manipulación de los ficheros de configuración			
3.	[A.5] Suplantación de la identidad			
4.	[A.24] Denegación de servicio			
5.	[A.30] Ingeniería social			

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 existan 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 de que el riesgo se materialice. Los valores de impacto podrán ir desde el valor uno (1) hasta el valor cinco (5), siendo uno (1) cuando no tiene un impacto conocido o es muy pequeño y cinco (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 comprometido 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. 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 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 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 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 MICROSOFT SHAREPOINT 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 Microsoft SharePoint Server 2019, en función de los resultados obtenidos por el análisis de riesgos y la cuantificación de cada uno de estos.

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 tres (3), se deberán aplicar las categorías de perfilado de seguridad de alcance básico. Si el valor obtenido para un riesgo determinado está entre cuatro (4) y seis (6), se deberán aplicar las categorías de perfilado de seguridad de alcance intermedio. Por último, si el valor obtenido es siete (7) o superior, se deberán aplicar las categorías de perfilado de alcance avanzado.

	ALCANCE		
NIVEL DE RIESGO	(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) SEC-SP1: 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 SHAREPOINT SERVER 2019	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log)	[A.3.SEC-SP1] Se garantiza al menos 90 días de registros de actividad.			
[A.4] Manipulación de los ficheros de configuración	[A.4.SEC-SP1] Los usuarios estándar no disponen de permisos de administrador local u otros que no sean necesarios para el desempeño de sus tareas.			
	[A.4.SEC-SP2] Se establece un filtrado de archivos.			
[A.5] suplantación de la identidad	[A.5.SEC-SP1] Se deniega el inicio de sesión anónimo.			
	[A.5.SEC-SP2] Se utilizan protocolos seguros de autenticación.			
[A.24] denegación de servicio	[A.24.SEC-SP1]Los servicios de SharePoint deben encontrarse levantados y corriendo.			
	[A.24.SEC-SP2] Se realizan conexiones a través de protocolos seguros.			
[A.30] Ingeniería social	[A.30.SEC-SP2] Se dispone de medidas anti ransomware habilitadas.			

ANEXO A. PASO A PASO CONFIGURACIÓN BASE DE SEGURIDAD SOBRE SHAREPOINT 2019

En el presente anexo, se detalla un conjunto de medidas encaminadas a reforzar la seguridad dentro de Microsoft SharePoint 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 ejecutado. Es posible que en otros escenarios y con otra superficie de exposición, el perfilado de aplicación de medidas sea diferente.

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

Nota: En caso de que el perfilado de seguridad y superficie de exposición obtenidos, en base al análisis realizado, requieran de una **configuración de seguridad avanzada, será necesario implementar medidas adicionales de seguridad**. Por el contrario, en caso de que el resultado de dicho análisis indique que la necesidad de configuración solo deba establecerse según el perfilado básico, será posible evitar ciertas medidas de seguridad de las establecidas en el 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.

Debe tenerse en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

A modo de ejemplo, se procede a realizar un perfilado intermedio de seguridad, aplicado a un servicio Microsoft SharePoint Server 2019. Antes de aplicar esta guía, se deben haber aplicado las configuraciones de seguridad necesarias sobre el servidor miembro Microsoft Windows Server 2019, para la correcta aplicación de medidas de seguridad del servicio Microsoft SharePoint Server 2019.

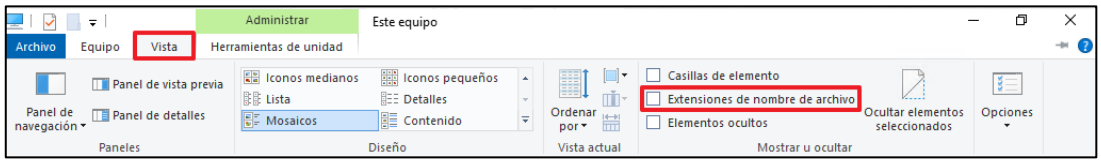
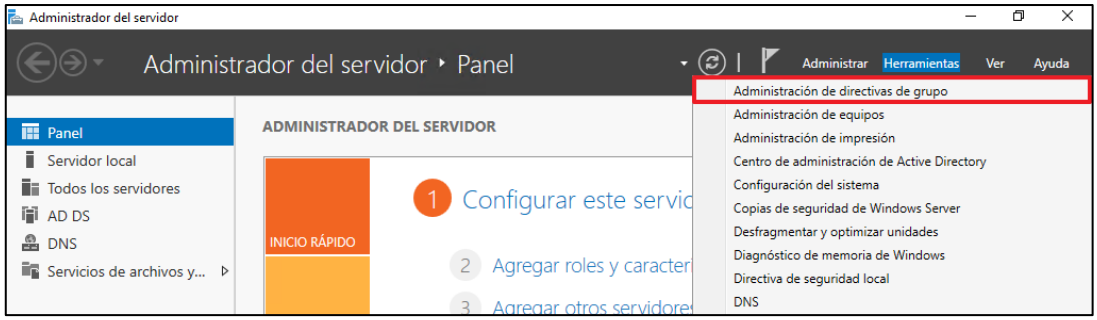
ANEXO A.1. IMPLEMENTACION DE POLITICAS DE SEGURIDAD

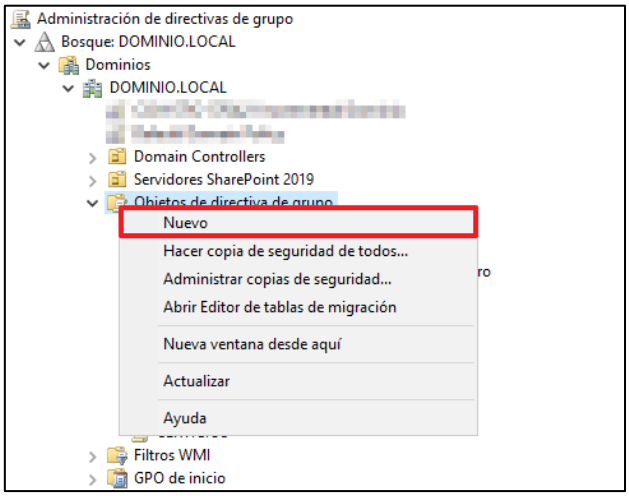
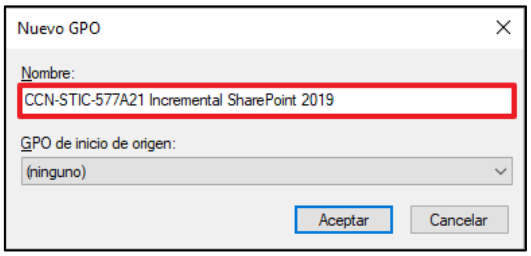
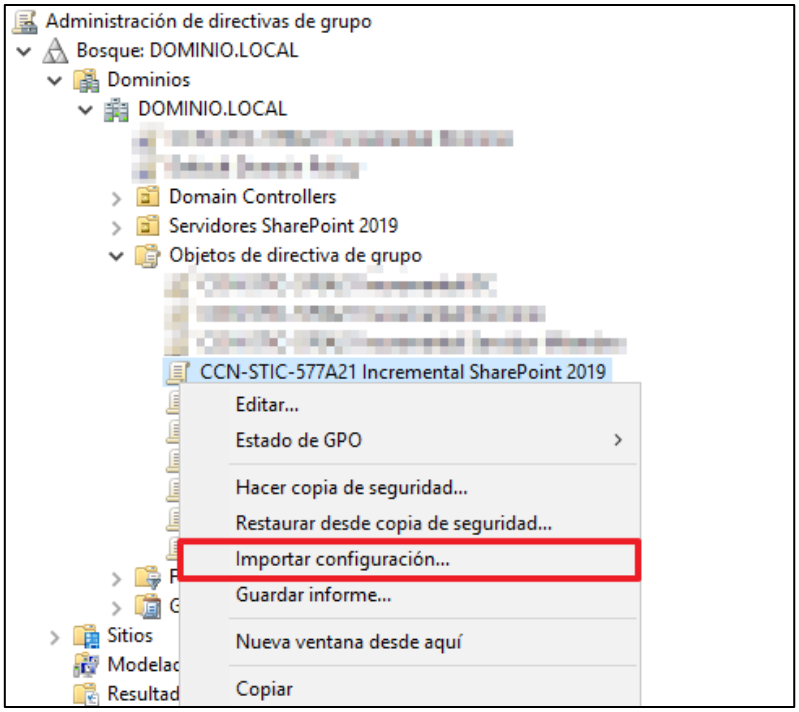
El presente punto establece la aplicación de las políticas de seguridad una vez que se han tenido en consideración las condiciones previas definidas al inicio de este anexo.

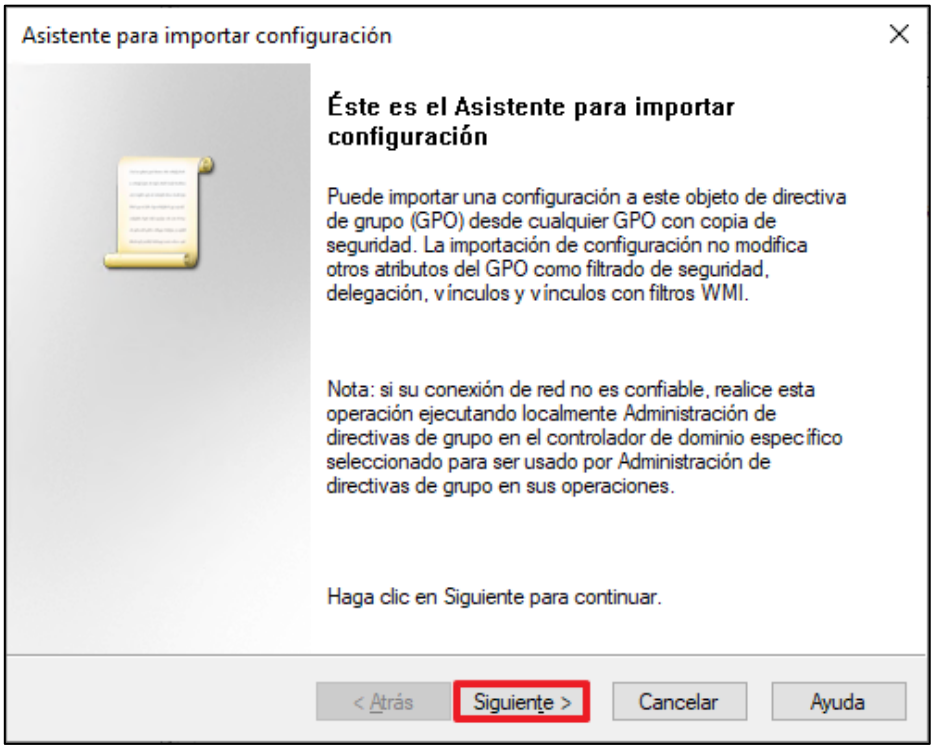
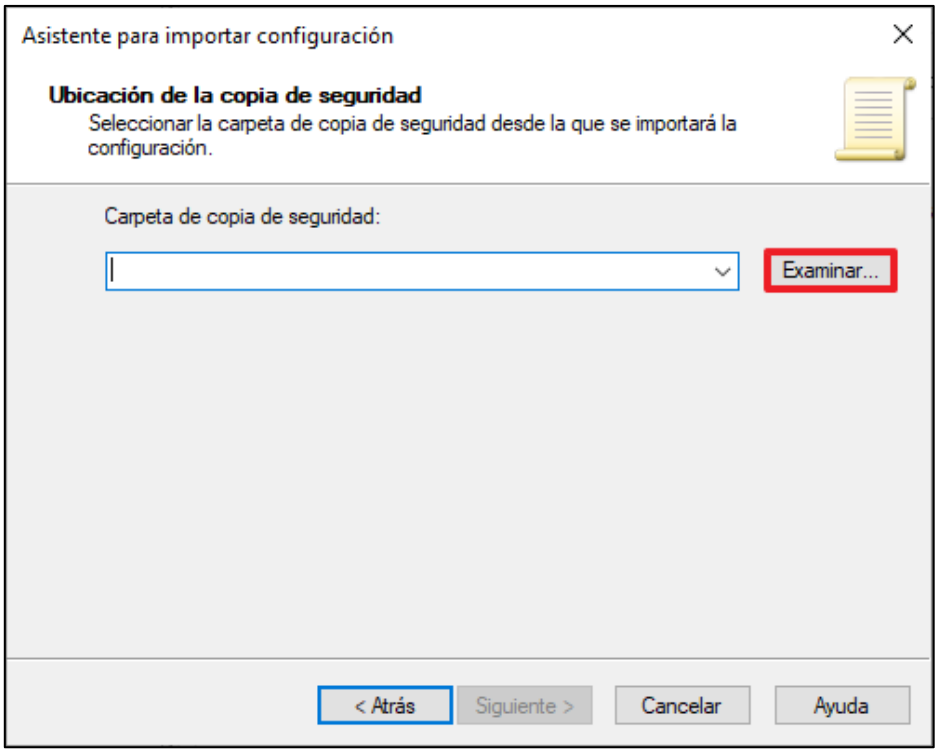
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

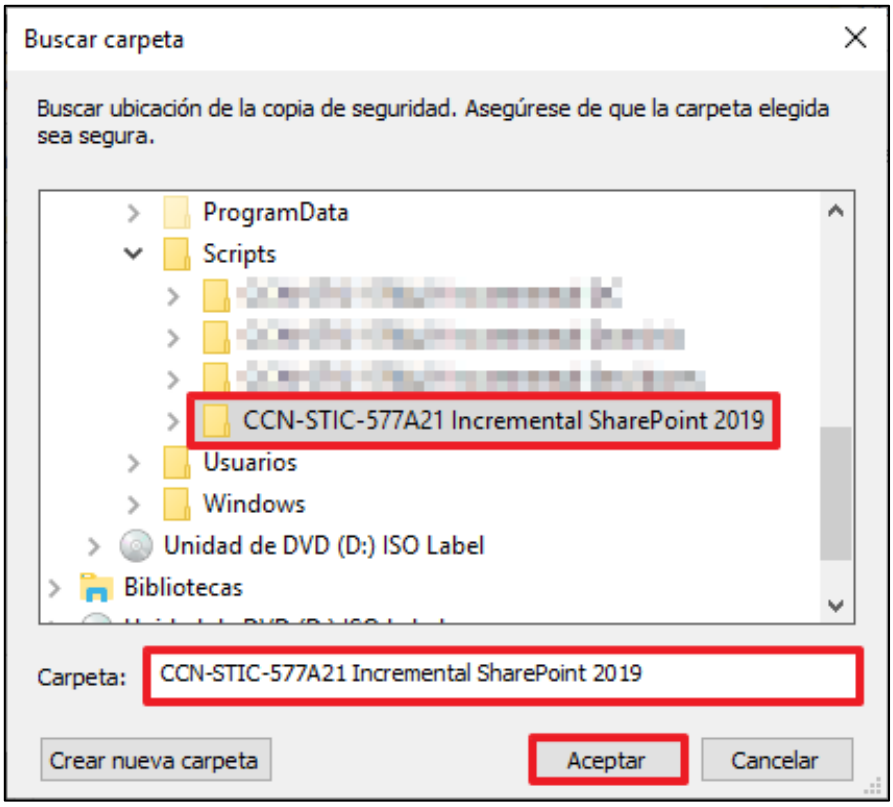
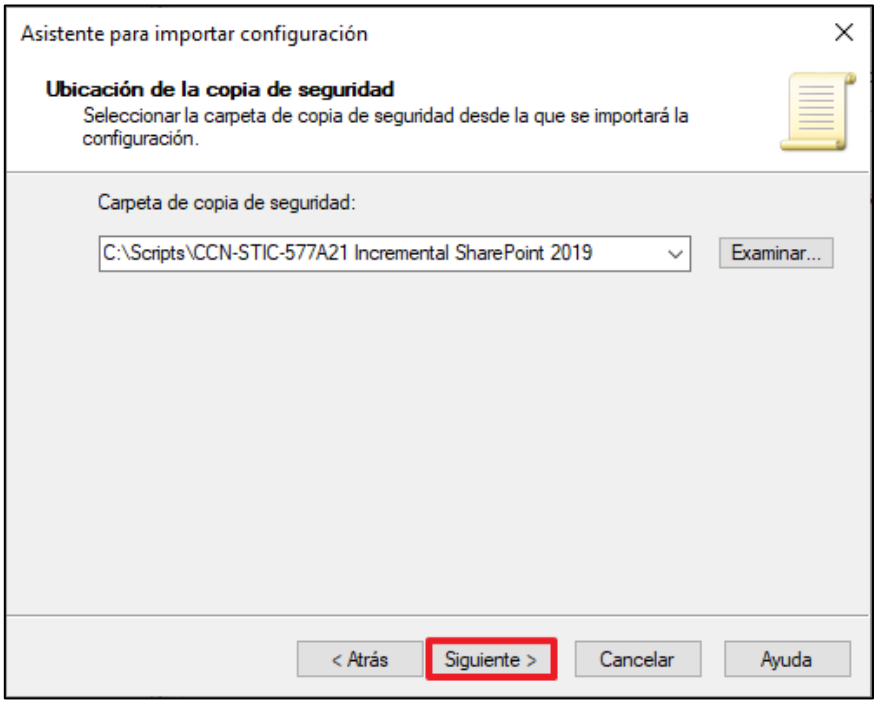
a)**[A.24.SEC-SP1]** Los servicios de SharePoint Server 2019 deben encontrarse en un modo de inicio adecuado y tener establecidos los permisos mínimos requeridos.

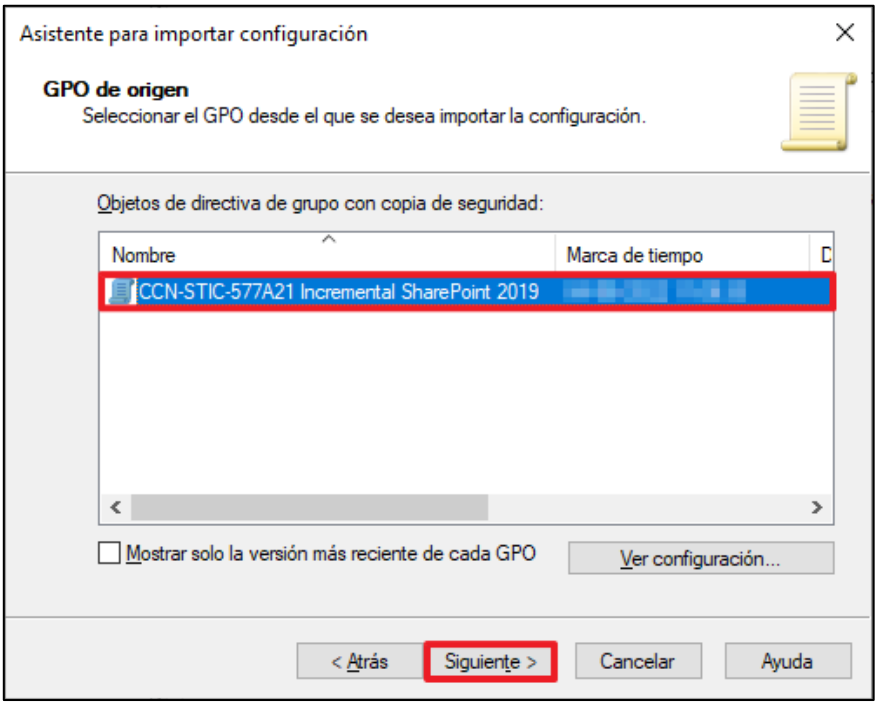
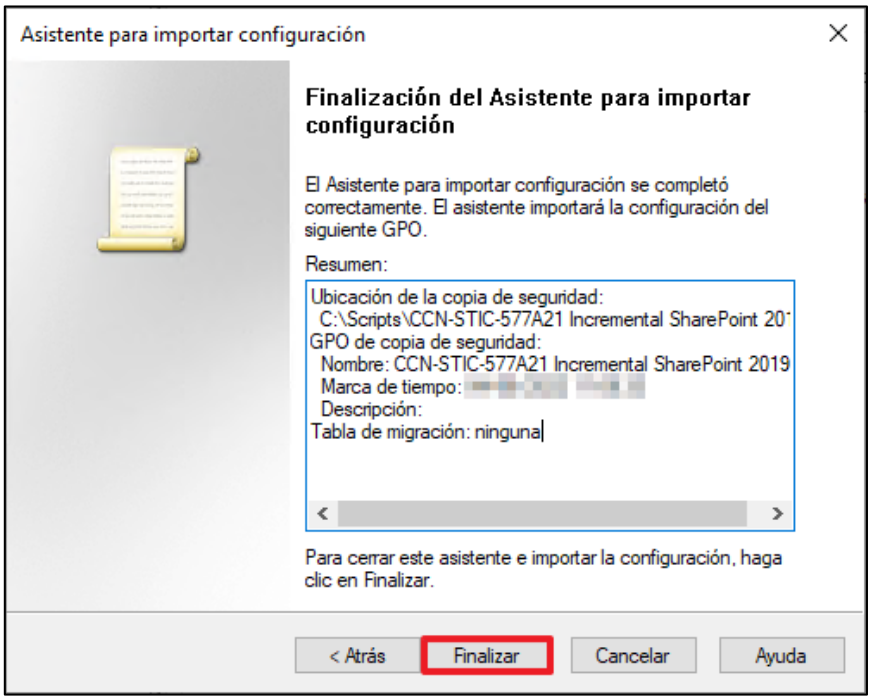
Paso	Descripción
1.	Se ha de Iniciar sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-577A21.
2.	Iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
3.	Se Crea el directorio "**Scripts**" en la unidad C:\.
4.	Ha de copiar los ficheros y directorios que acompañan a esta guía al directorio "**C:\Scripts**".
5.	Se configurará 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 su identificación, para ello se debe pulsar sobre el icono del explorador de archivos desde la barra de tareas. 
6.	En el "**Explorador de archivos**" se hace clic sobre la pestaña "**Vista**" del menú superior y se marca la casilla "**Extensiones de nombre de archivos**". 
7.	Se inicia la herramienta "**Administración de Directivas de Grupo**". Sobre el menú superior de la derecha de la herramienta "**Administrador del servidor**" se selecciona "**Herramientas → Administración de directivas de grupo**". 
8.	Se despliegan los contenedores y se sitúa sobre el nodo "**Objetos de directiva de grupo**".

Paso	Descripción
9.	Se pulsa con el botón derecho, sobre dicho nodo y selecciona la opción "**Nuevo**". 
10.	Se introduce como nombre "CCN-STIC-577A21 Incremental SharePoint 2019" y se pulsa el botón "**Aceptar**". 
11.	Se selecciona la política recién creada, se pulsa con el botón derecho sobre la misma seleccionando la opción "**Importar configuración...**". 

Paso	Descripción
12.	En el asistente de importación de configuración, se pulsa el botón "**Siguiente >**". 
13.	En la selección de copia de seguridad se pulsa el botón "**Siguiente >**". No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
14.	En "**Carpeta de copia de seguridad**", se pulsa el botón "**Examinar...**". 

Paso	Descripción
15.	Se selecciona la carpeta "**CCN-STIC-577A21 Incremental SharePoint 2019**" que se halla en el directorio "**C:\Scripts**" y se selecciona el botón "**Aceptar**". 
16.	Se selecciona el botón "**Siguiente >**" una vez escogida la carpeta adecuada. 

Paso	Descripción
17.	En la pantalla siguiente se comprueba que aparece la política de seguridad "**CCN - STIC - 577A21 Incremental SharePoint 2019**" y se pulsa el botón "**Siguiente >**". 
18.	Para completar el asistente se pulsa el botón "**Finalizar**". 
19.	Se selecciona el botón "**Aceptar**" para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no se tiene en consideración y se continúa con el siguiente paso.

ANEXO A.2. 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 perfilado de seguridad. 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.

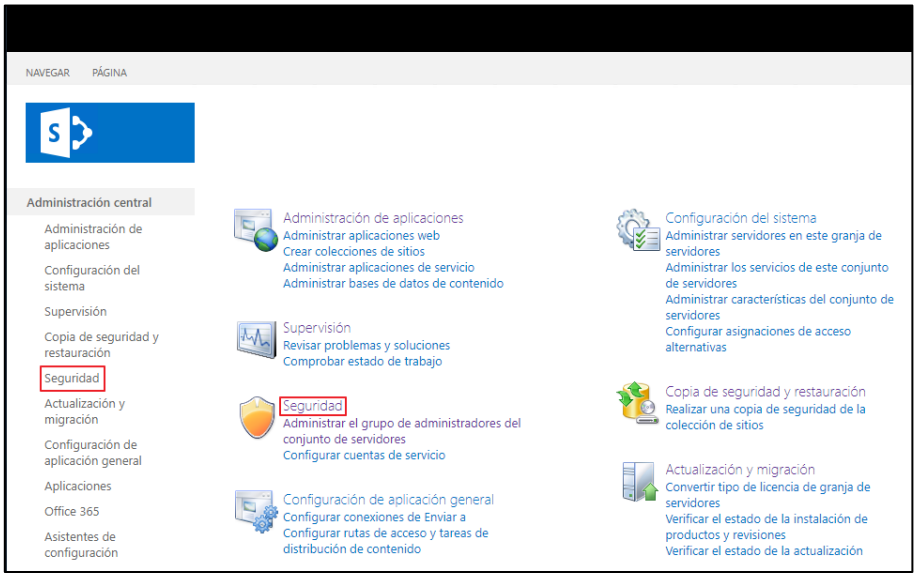
Para estos casos, se desarrolla el presente anexo, en el cual se establecen comentarios sobre las categorías de perfilado de seguridad de nivel intermedio afectadas y se determina un ejemplo de configuración o validación que permita garantizar el aseguramiento de Microsoft SharePoint Server 2019 con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

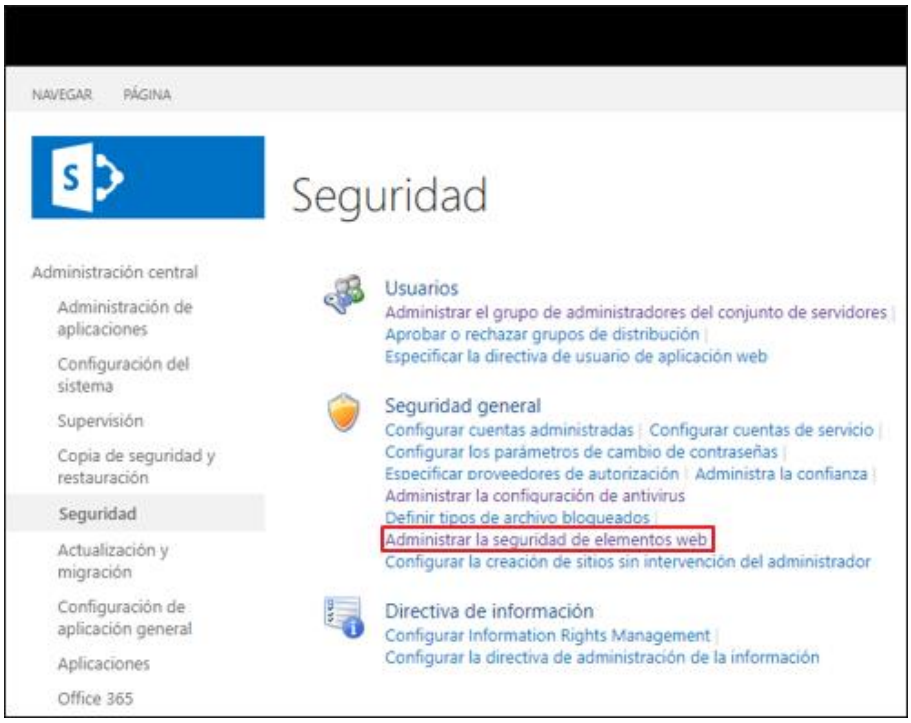
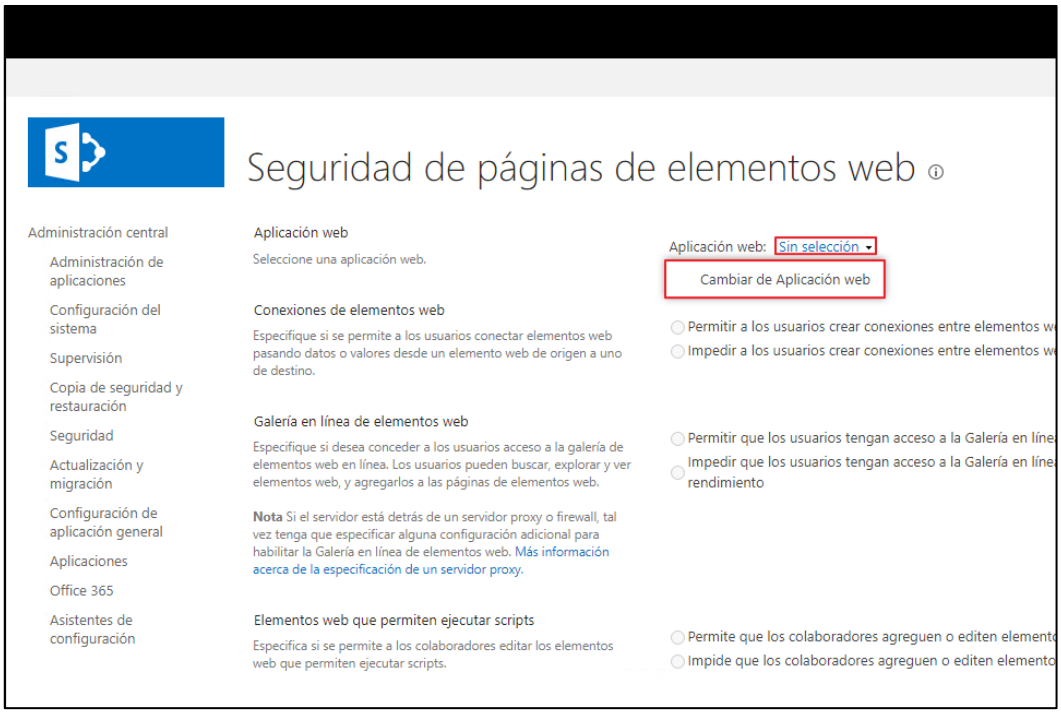
Nota: Las diferentes configuraciones ofrecidas en este anexo son una referencia de las múltiples soluciones que se pueden encontrar para cada uno de los riesgos identificados, es decir, la misma funcionalidad aquí presentada para la mitigación del riesgo puede ser aplicada mediante otros procedimientos, software, o configuraciones. No deben tomarse estas configuraciones como métodos únicos de mitigación.

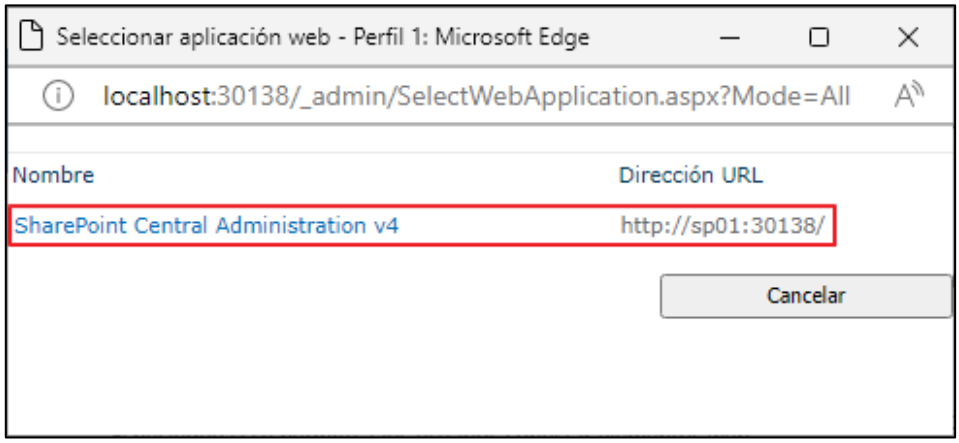
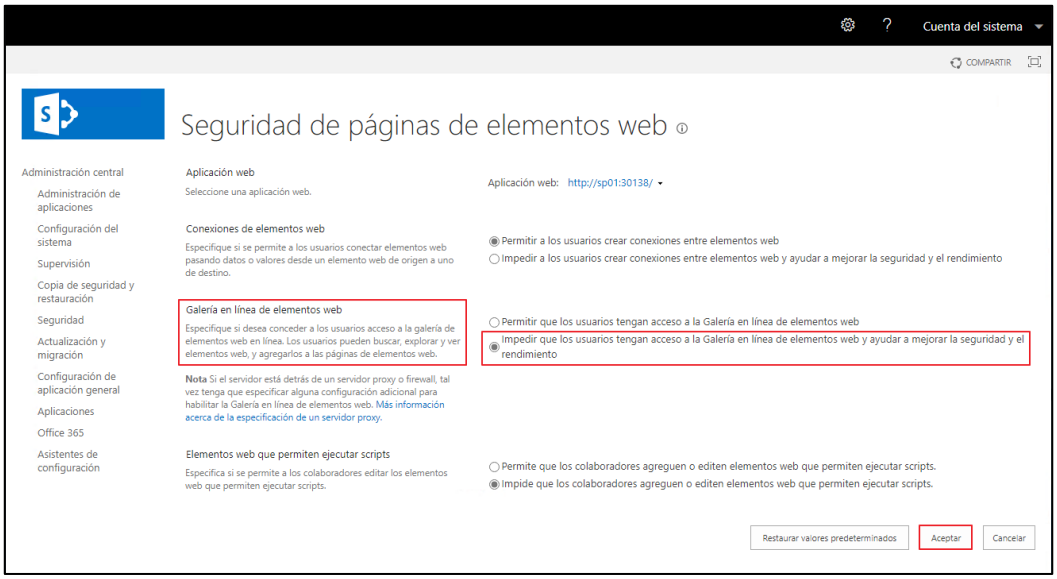
ANEXO A.2.1. SEGURIDAD DE SHAREPOINT

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.4.SEC-SP1]** Los usuarios estándar no disponen de permisos de administrador local u otros que no sean necesarios para el desempeño de sus tareas, gracias a esta medida se consigue reducir la superficie de exposición sobre el servicio.

Paso	Descripción
20.	En el servidor que disponga del servicio de Microsoft SharePoint Server 2019, se accede a la web de "**Administración central de SharePoint**" y se pulsa en "**Seguridad**". 

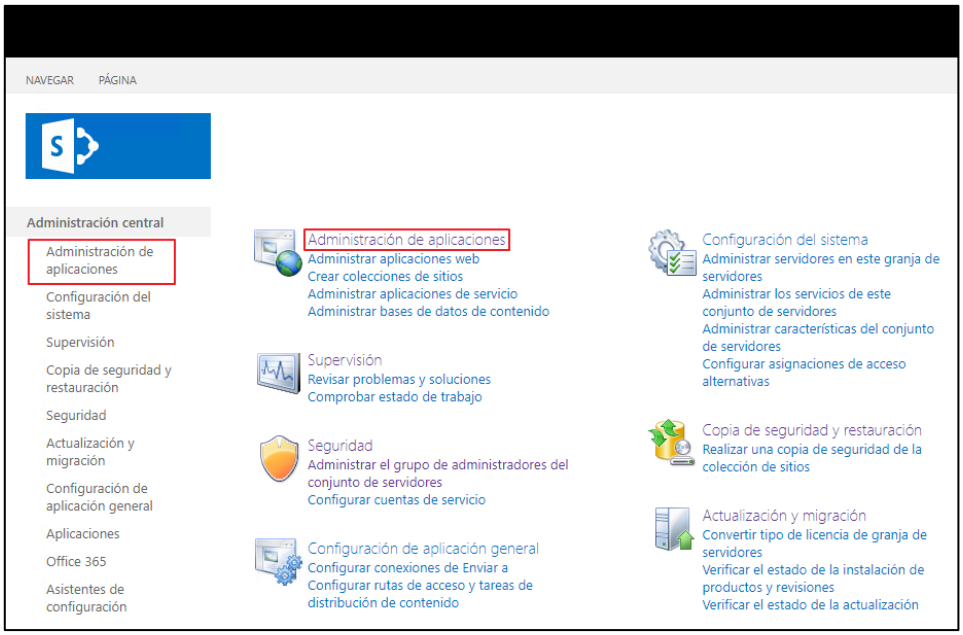
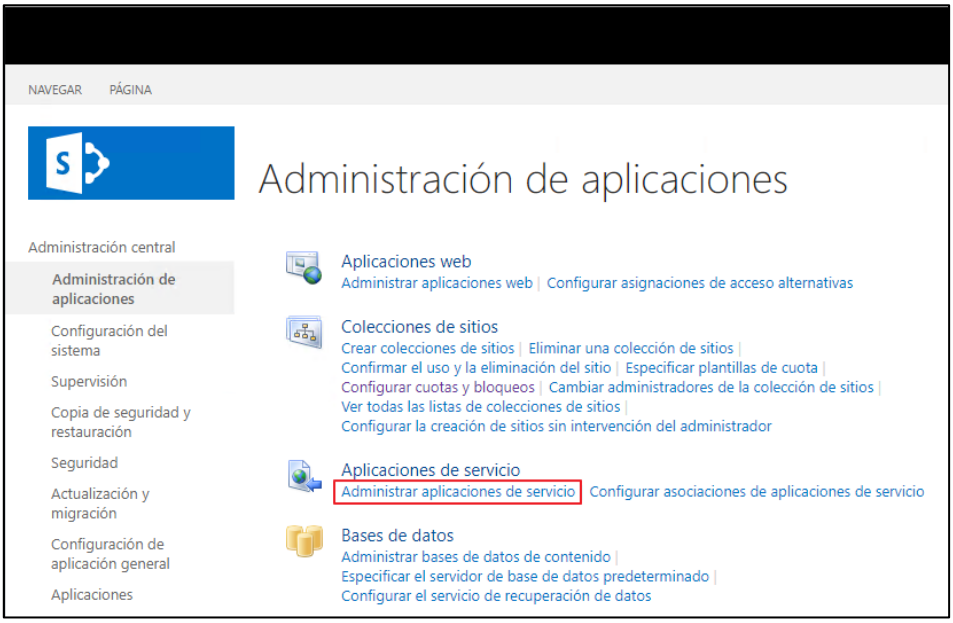
Paso	Descripción
21.	Una vez se ha accedido a la parte de seguridad, se hace clic en el apartado "**Administrar la seguridad de elementos web**". 
22.	Se debe seleccionar la aplicación web para la cual se quiera configurar la seguridad pulsando en "**Aplicación web**" y a continuación, haciendo clic en "**Cambiar de Aplicación web**. 

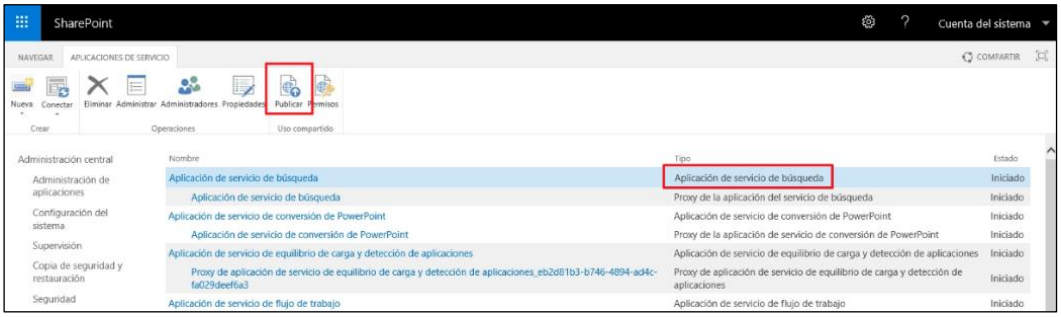
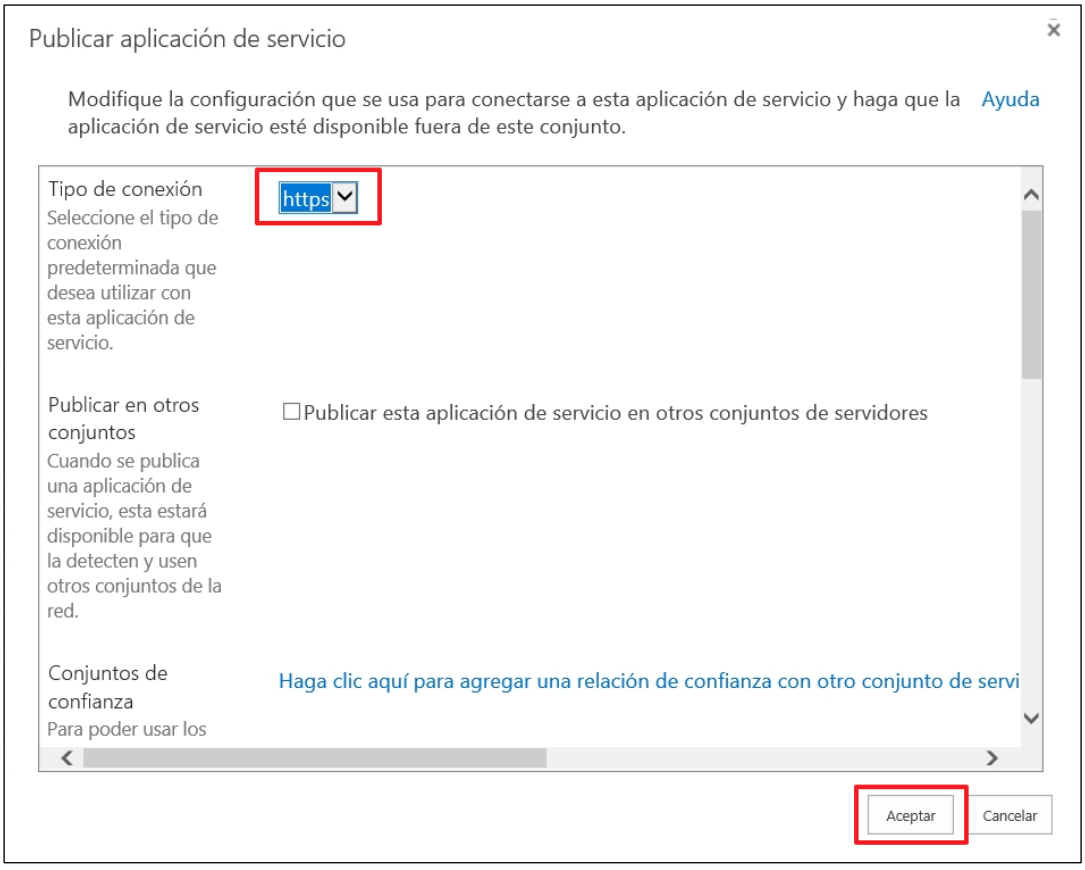
Paso	Descripción
23.	Se desplegará una ventana flotante donde se selecciona la opción correspondiente 
24.	En la sección "**Galería en línea de elementos web**", se selecciona "**Impedir que los usuarios tengan acceso a la Galería en línea de elementos web y ayudar a mejorar la seguridad y el rendimiento**" y por último se pulsa en "**Aceptar**". 

ANEXO A.2.2. CONEXIONES HTTPS SEGURAS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.24.SEC- SP2]** Se realizan conexiones a través de protocolos seguros. La acción que se describe permite la mitigación de ataques de denegación de servicio como el DDoS.

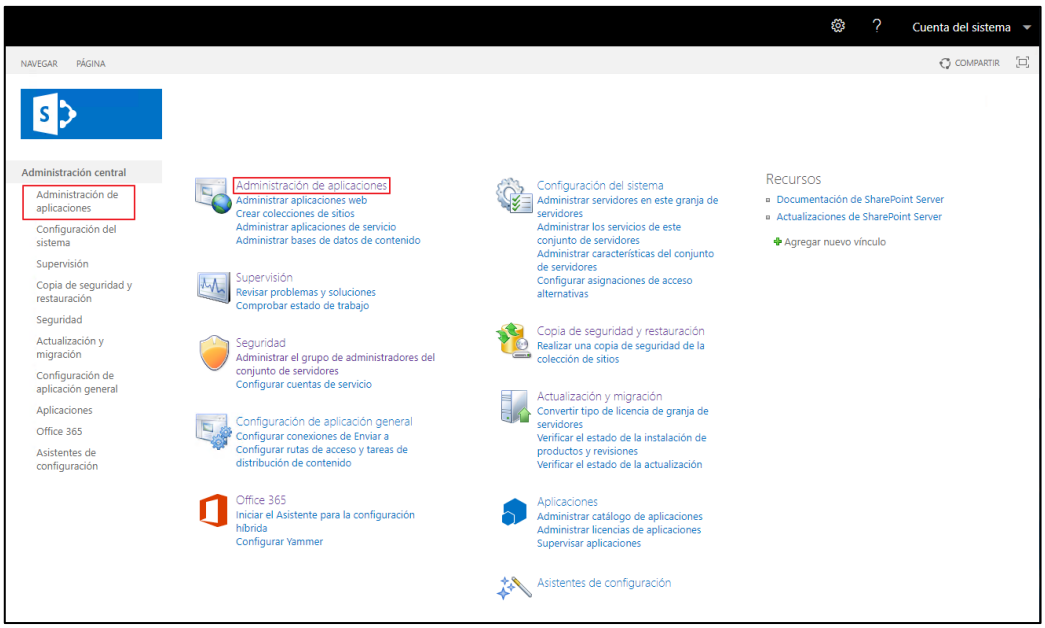
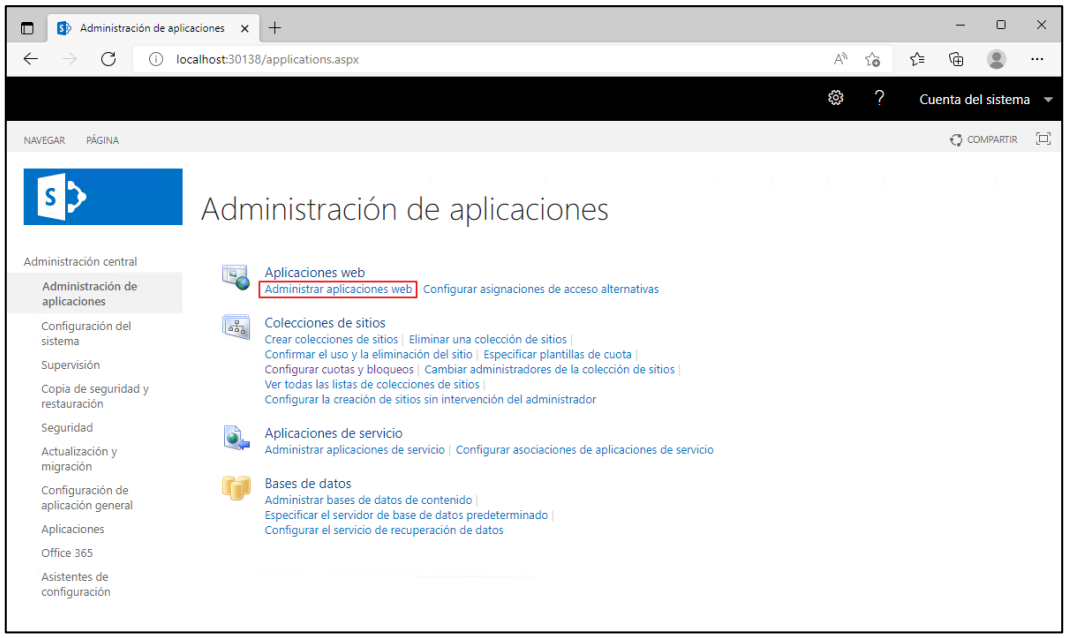
Paso	Descripción
25.	En el servidor con SharePoint Server 2019 instalado, se accede a la "**Administración central de SharePoint**" y se pulsa en "**Administración de aplicaciones**". 
26.	En la sección "**Aplicaciones de servicio**", se pulsa en "**Administrar aplicaciones de servicio**". 

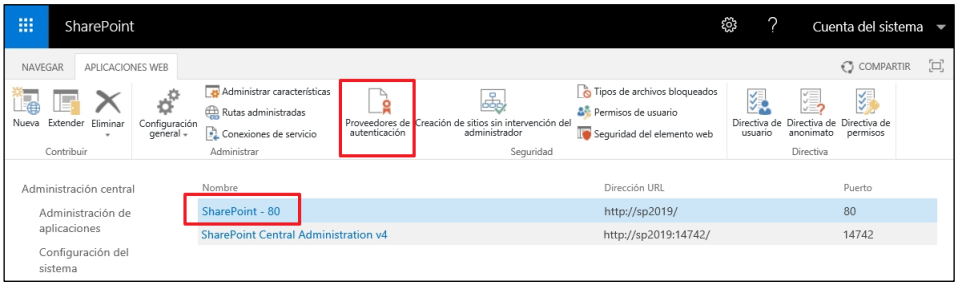
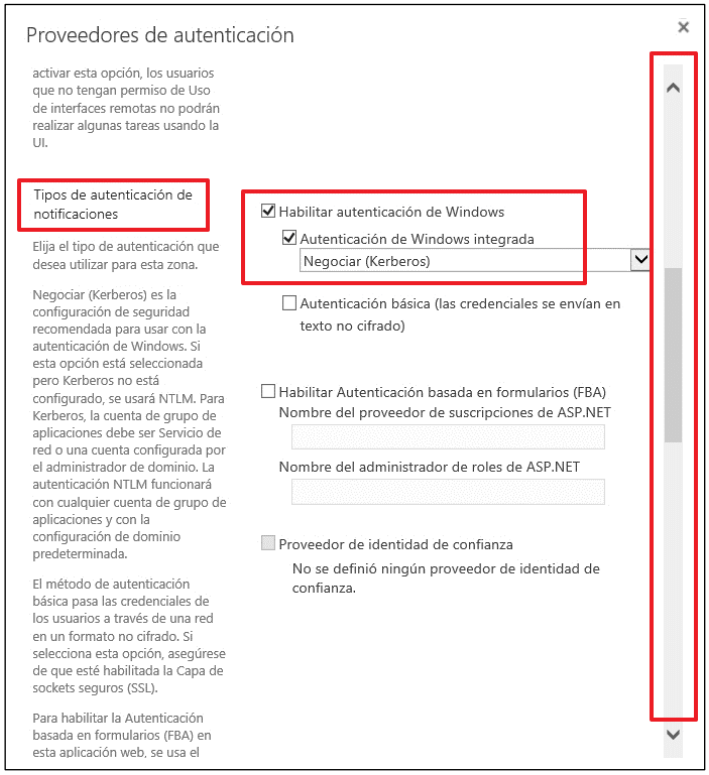
Paso	Descripción
27.	Se selecciona la aplicación de servicio pulsando sobre el campo "**Tipo**" y se hace clic en "**Publicar**". 
28.	Se ha de seleccionar el tipo de conexión como "**https**". Se finaliza, pulsando en "**Aceptar**". 

ANEXO A.2.3. DESHABILITAR PROTOCOLOS INSEGUROS DE AUTENTICACION

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.5.SEC- SP2]** Se utilizan protocolos seguros de autenticación evitando el robo de credenciales mediante ataques del tipo MitM (Man in the Middle) entre otros.

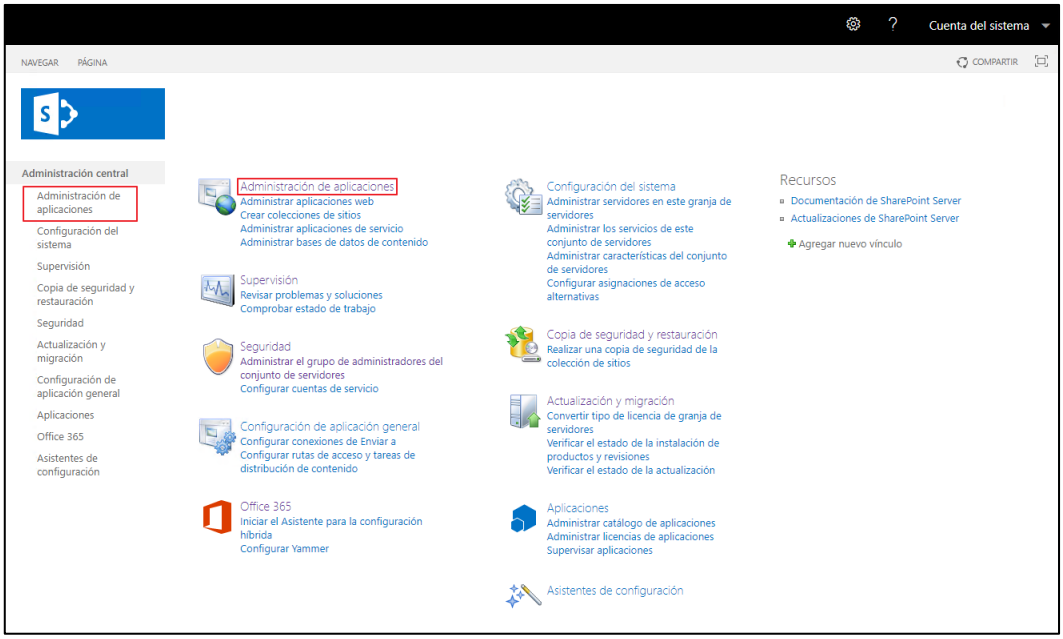
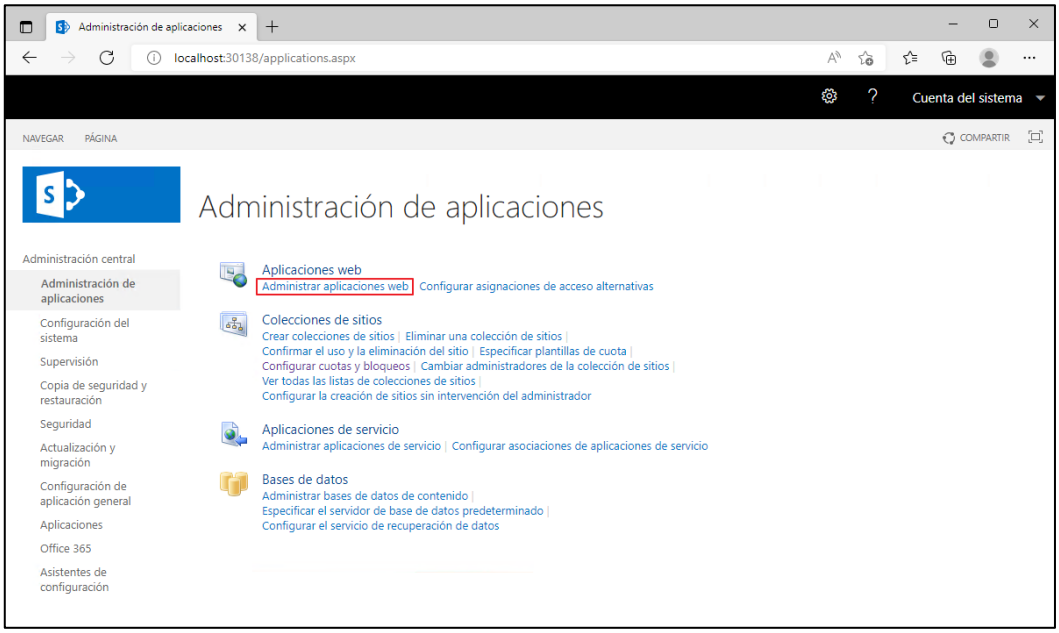
Paso	Descripción
29.	En el servidor con SharePoint Server 2019 instalado, se accede a la "**Administración central de SharePoint**" y pulsa en "**Administración de aplicaciones**". 
30.	En la sección "**Aplicaciones web**", se pulsa en "**Administrar aplicaciones web**". 

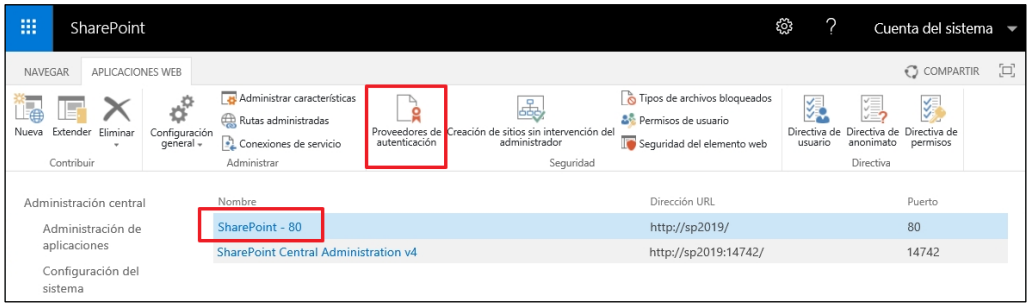
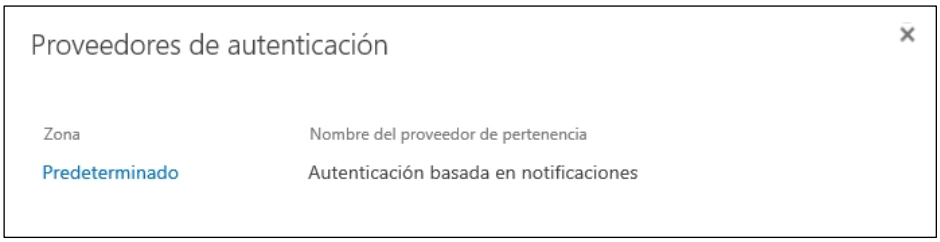
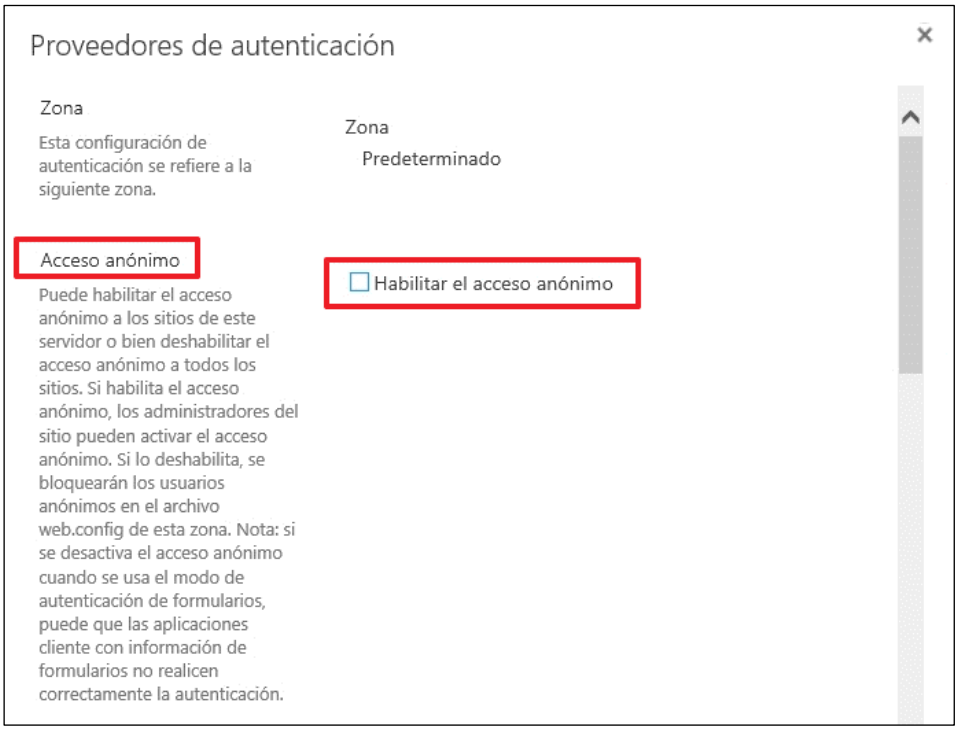
Paso	Descripción
31.	Se selecciona el sitio web para el que se tiene previsto verificar los tipos de autenticación y se pulsa en "**Proveedores de autenticación**". 
32.	En la ventana emergente se selecciona "**Predeterminado**". 
33.	En la ventana "**Proveedores de autenticación**", se desplaza hasta encontrar "**Tipos de autenticación de notificaciones**". Se selecciona "**Habilitar autenticación de Windows**", marcando "**Autenticación de Windows integrada**", y se elige "**Negociar (Kerberos)**". Se finaliza desplazándose hasta la parte inferior de la ventana y pulsando en "**Guardar**". 

ANEXO A.2.4. SE DENIEGA LA AUTENTICACIÓN ANÓNIMA

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.5.SEC-SP1]** Se deniega el inicio de sesión anónimo. Se aplican medidas que impiden el acceso a cuentas de usuario anónimas, así como la posibilidad de activación de dicho acceso anónimo por parte de los administradores.

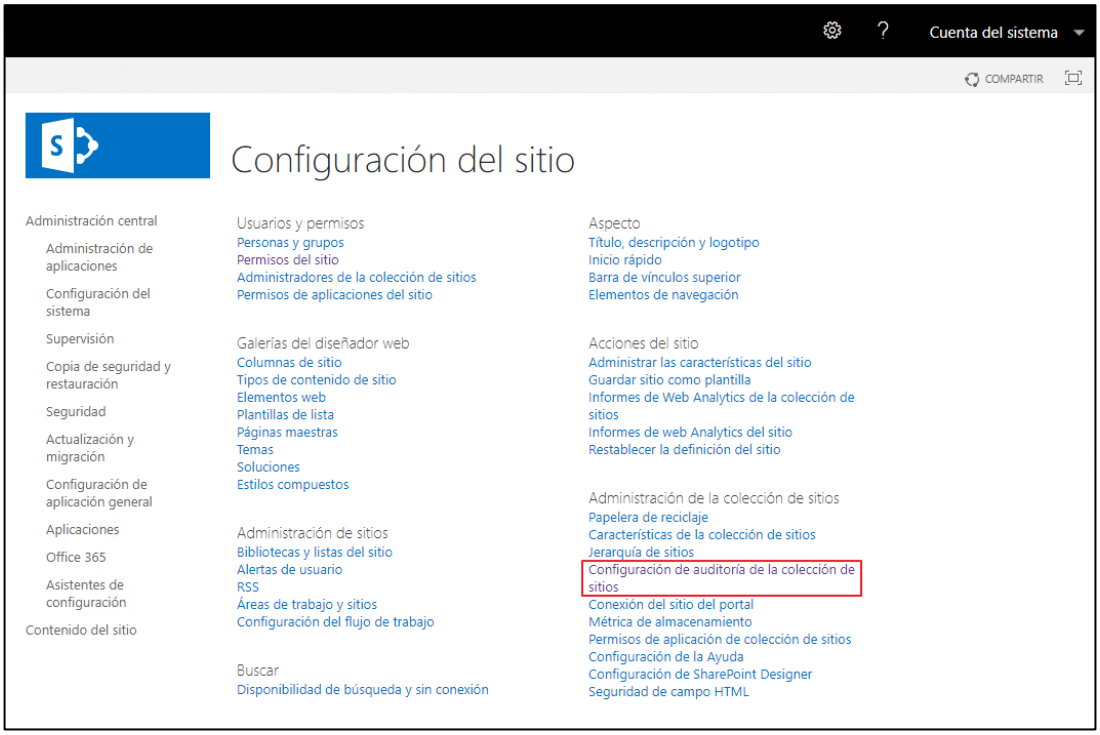
Paso	Descripción
34.	En el servidor con SharePoint Server 2019 instalado, se accede a la "**Administración central de SharePoint**" y se pulsa en "**Administración de aplicaciones**". 
35.	En la sección "**Aplicaciones web**", se elige "**Administrar aplicaciones web**". 

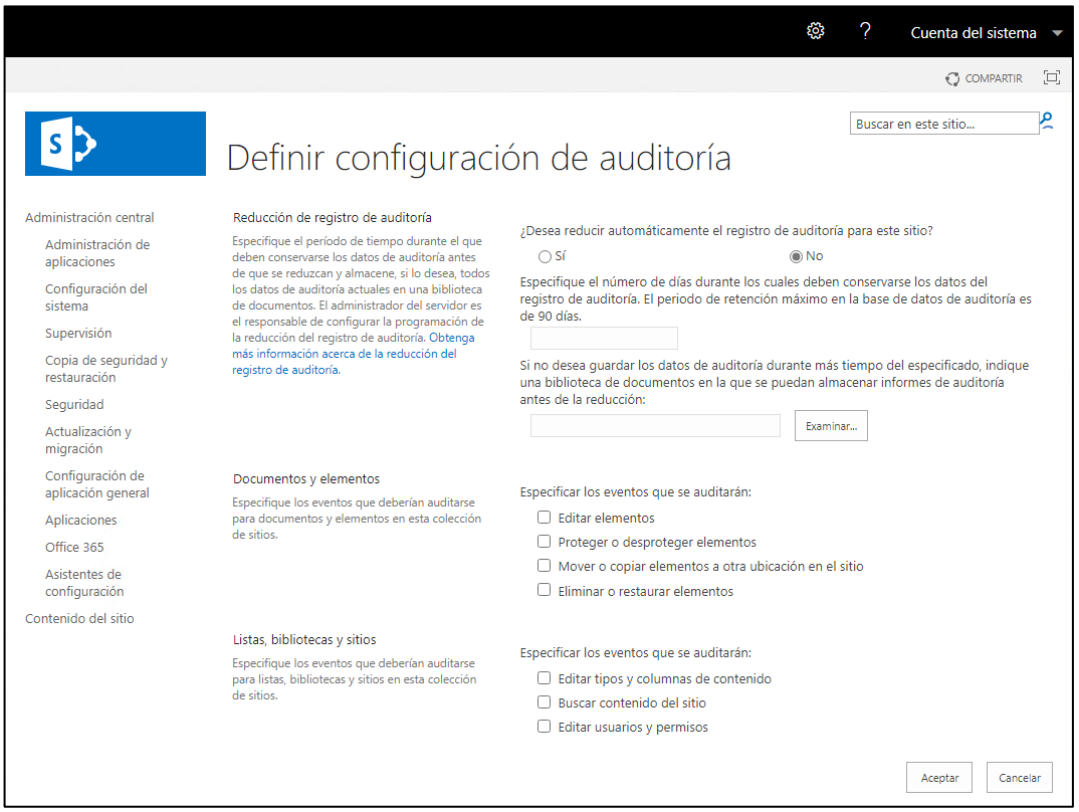
Paso	Descripción
36.	Se selecciona el sitio web para el que tiene previsto denegar la autenticación anónima y se selecciona en "**Proveedores de autenticación**". 
37.	En la pequeña ventana emergente se pulsa en "**Predeterminado**" o, en caso de aparecer otro distinto, se pulsará sobre él. 
38.	En la ventana "**Proveedores de autenticación**", se desplaza hasta encontrar "**Acceso anónimo**". Se desmarca la casilla "**Habilitar el acceso anónimo**". Se finaliza desplazándose hasta la parte inferior de la ventana y pulsando en "**Guardar**". La operación se repite para cada aplicación web. 

ANEXO A.2.5. REGISTROS DE ACTIVIDAD

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.3.SEC-SP1]** Se garantiza al menos 90 días de registros de actividad. La existencia de un historial de logs permite la identificación e investigación de posibles incidentes.

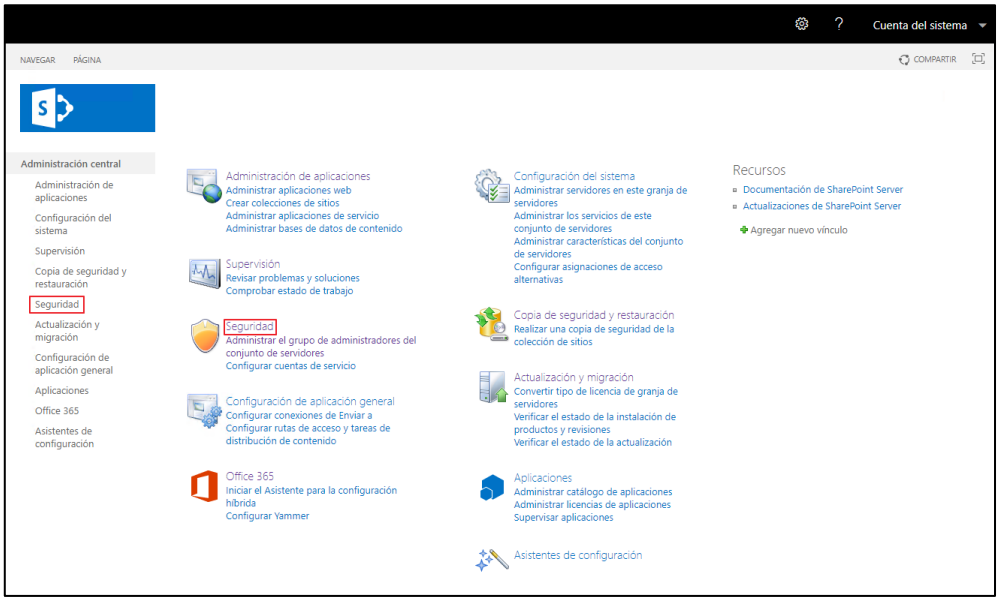
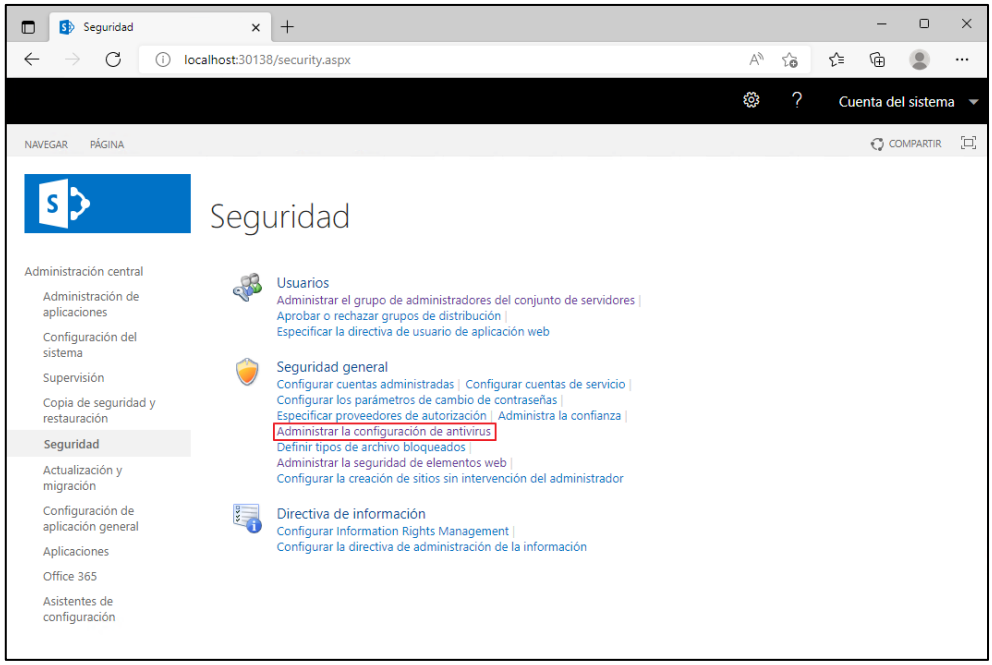
Paso	Descripción
39.	En el servidor con SharePoint Server 2019 instalado, se accede a la "**Administración central de SharePoint**" y pulsa en el icono de engranaje en la parte superior de la ventana. Se accede a "**Configuración del sitio**". 
40.	En la sección "**Administración de la colección de sitios**", se pulsa en "**Configuración de auditoría de la colección de sitios**". 

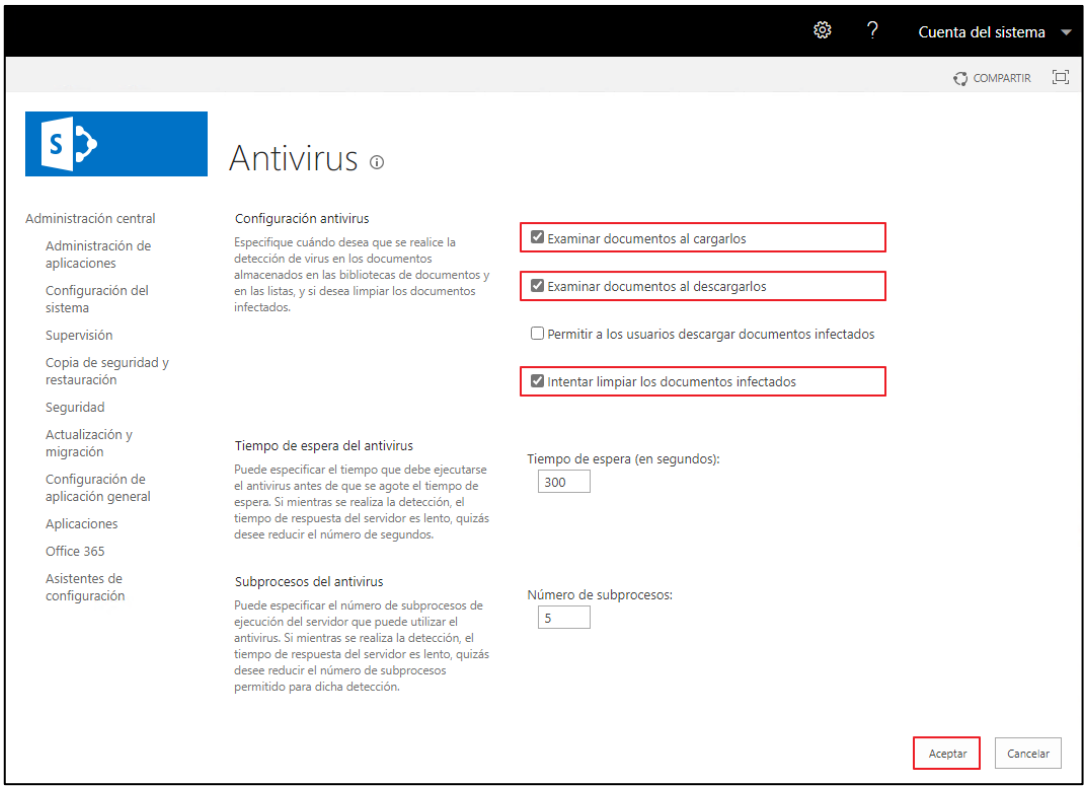
Paso	Descripción
41.	Se seleccionan los eventos que deben ser auditados, según los requisitos de su organización. Para finalizar, se pulsa en "**Aceptar**". 

ANEXO A.2.6. ANTIVIRUS DE SHAREPOINT

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.30.SEC-SP2]** Se dispone de medidas anti ransomware habilitadas. En este caso a través de la configuración del antivirus del SharePoint que permite mitigar la difusión de software malintencionado.

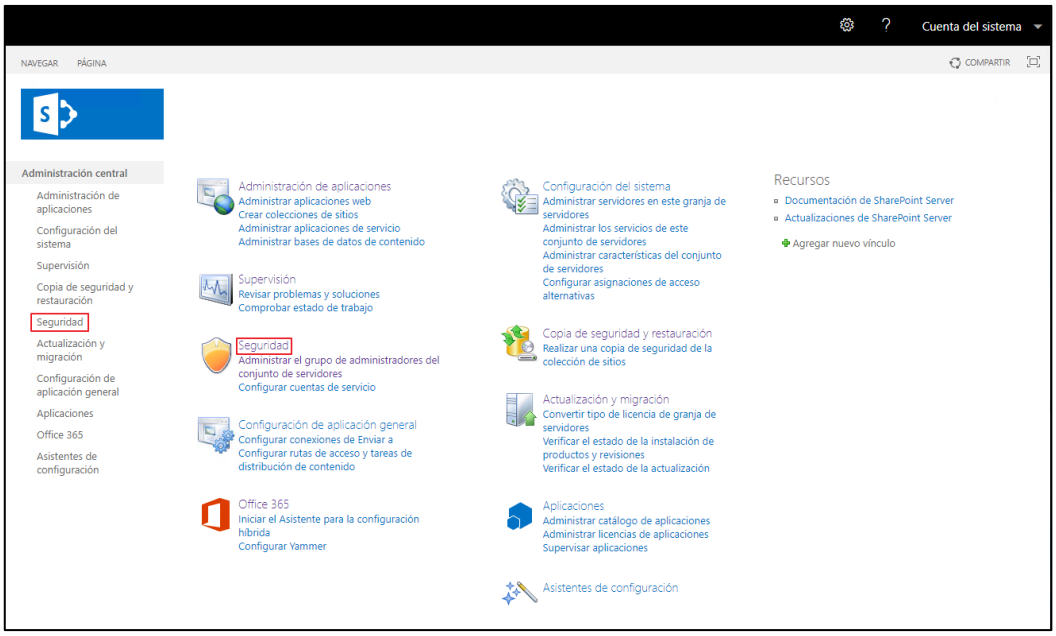
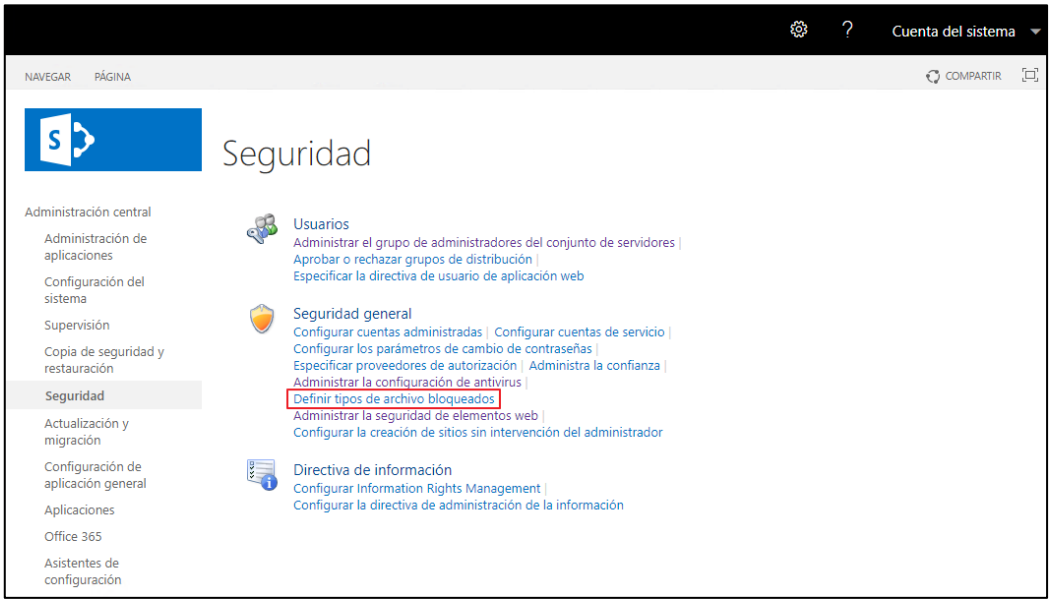
Paso	Descripción
42.	En el servidor que tenga instalado SharePoint Server 2019, se accede vía web a la "**Administración central de SharePoint**" y se pulsa en "**Seguridad**". 
43.	En "**Seguridad general**", se pulsa en "**Administrar la configuración del antivirus**". 

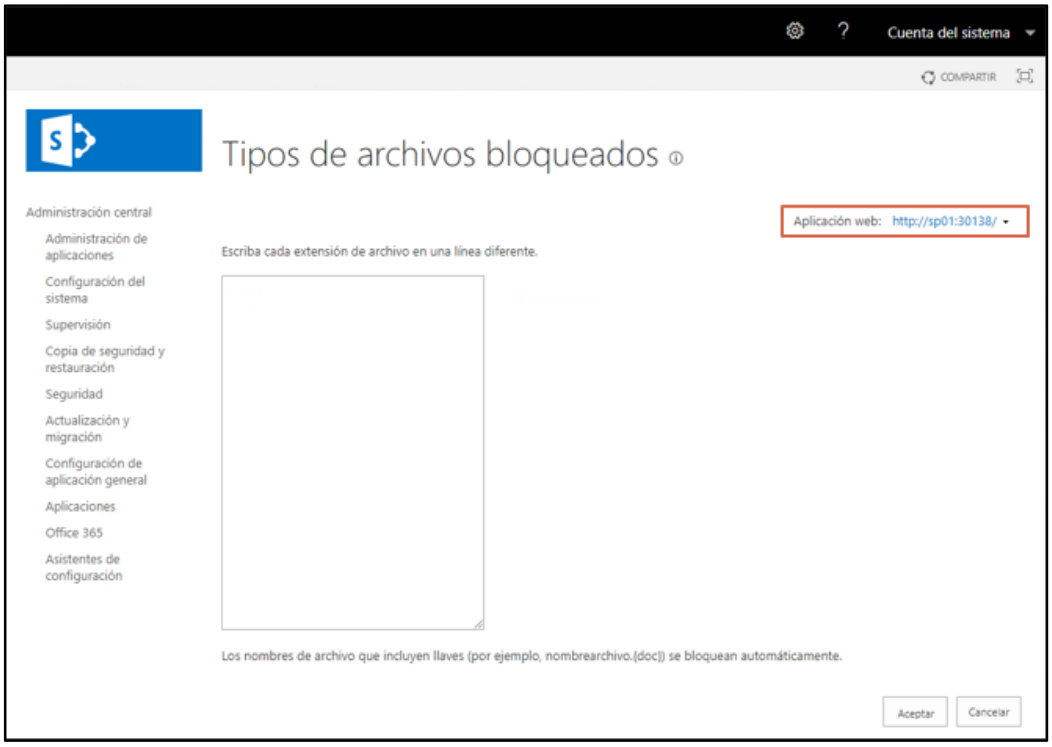
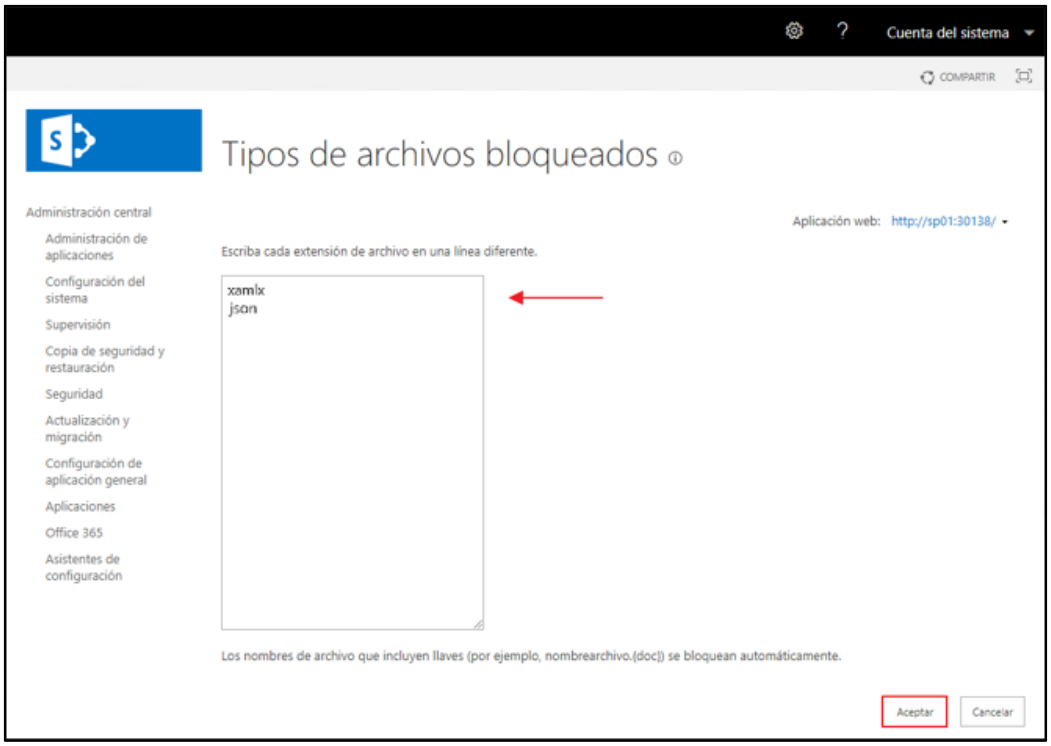
Paso	Descripción
44.	Se ha de asegurar de marcar las opciones “**Examinar documentos al cargarlos**”, “**Examinar documentos al descargarlos**” e “**Intentar limpiar los documentos infectados**”. Dejando desactivado el campo “**Permitir a los usuarios descargar documentos infectados**”. Para finalizar, se pulsa “**Aceptar**”. 

ANEXO A.2.7. FILTRADO DE ARCHIVOS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.4.SEC-SP2]** Se establece un filtrado de archivos evitando la descarga de archivos con extensiones no conocidas o que puedan ser fuente de infecciones mediante software o código malicioso.

Paso	Descripción
45.	En cada servidor donde se tenga instalado SharePoint Server 2019, se accede a la "**Administración central de SharePoint**" haciendo clic en "**Seguridad**". 
46.	En el apartado de "**Seguridad general**", se selecciona "**Definir tipos de archivo bloqueados**". 

Paso	Descripción
47.	Se selecciona la aplicación web para la que se quieran configurar los tipos de archivos bloqueados pulsando en "**Aplicación web**", escogiendo la aplicación correspondiente. 
48.	Para añadir un tipo de archivo a bloquear, se deberá escribir la extensión del archivo, una por línea. Para aplicar los cambios, se selecciona "**Aceptar**". 

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL