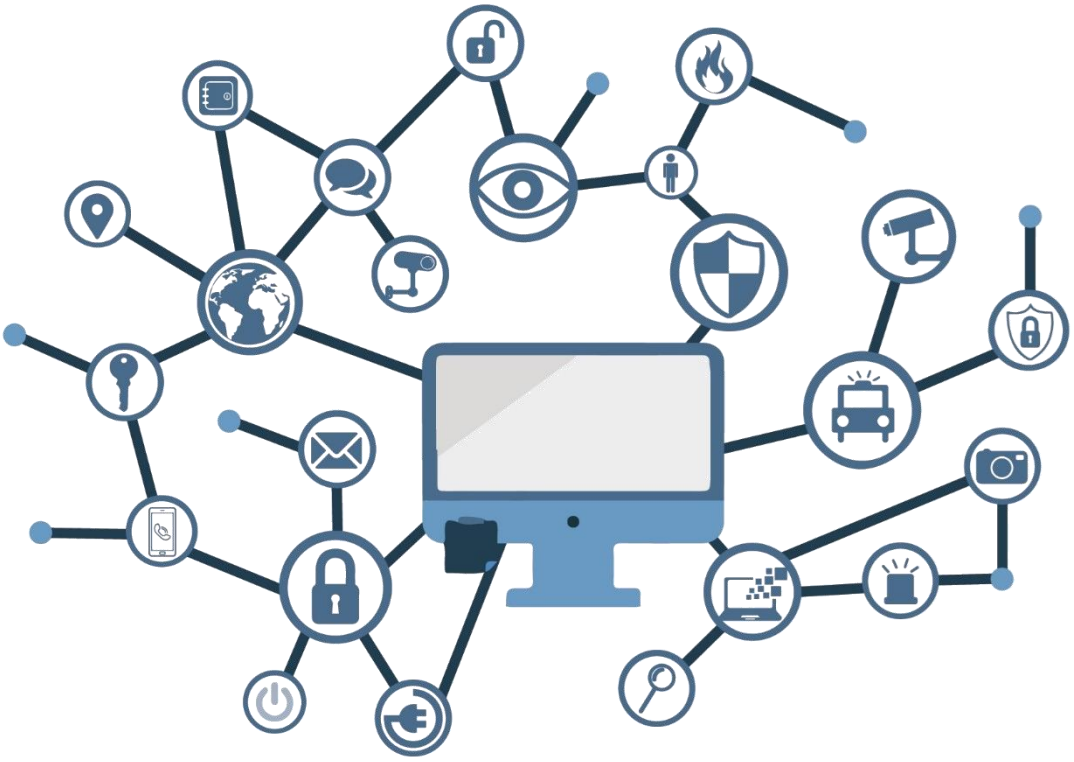
centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC-576A21

# GUÍA DE APLICACIÓN DE PERFILADO DE SEGURIDAD PARA MICROSOFT EXCHANGE 2019



AGOSTO 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

CCN 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
2022.09.09 10:30:23 +02'00'

P.º de la Castellana 109, 28046 Madrid

NIPO: 083-22-219-X

Fecha de Edición: agosto de 2022
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

# ÍNDICE

# 1. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN STIC 500), siendo de aplicación 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 configurando.

La aplicación de la presente guía requerirá la aplicación previa de la guía CCN-STIC 570A21 Guía de aplicación de perfilado de seguridad para Windows Server 2019.

# 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 sistemas que implementen Microsoft Exchange 2019.

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 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 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 Microsoft Exchange 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, 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 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 los escenarios planteados. En particular, se incluirá la configuración para aplicar un perfilado de seguridad de un servidor con “Microsoft Exchange 2019” instalado en español.

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.

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 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 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 de adecúan a cada realidad.

d) Perfilado de seguridad. En este punto se establecen las medidas de seguridad que se deberán aplican al producto o tecnología del 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 Microsoft Exchange 2019 bajo Windows Server 2019.

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 del 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 resultante 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.

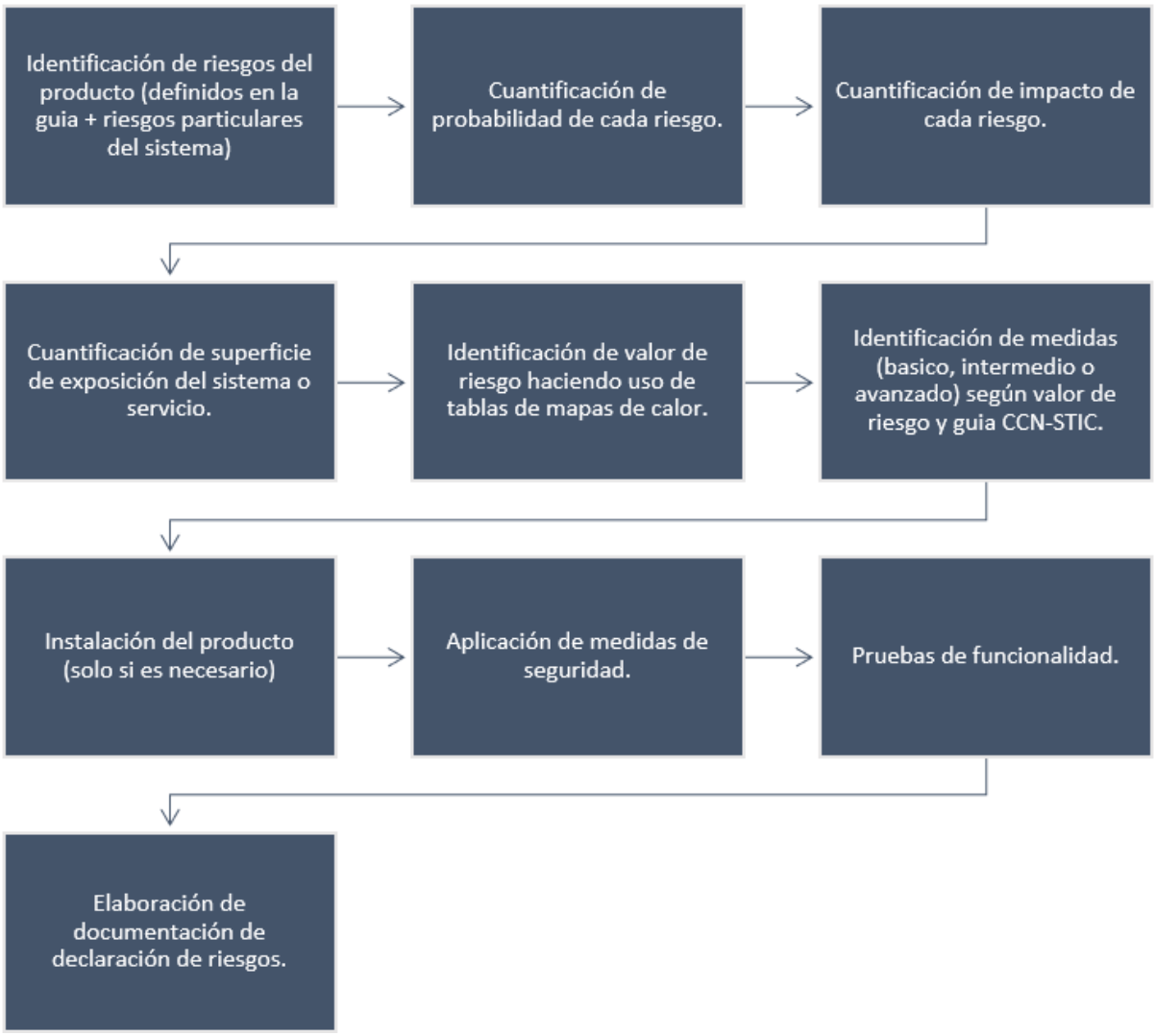
   Cada organización deberá determinar cómo configurar el sistema para el cumplimiento de la medida correspondiente. De esta forma, se ofrece un mayor grado de flexibilidad a la hora de proteger el sistema, necesario sobre todo en sistemas que ya están en funcionamiento o en producción. Es decir, en esta 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 riegos y las medidas de mitigación de éstos, se procederá a la instalación del sistema operativo en el caso de nuevas implementaciones. En caso de que el sistema ya se encuentre 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 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 Microsoft Exchange 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, quiere 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, quiere decir que tendría la capacidad de establecer conexiones con elementos de red externos de una organización o entidad.

## 5.1 RIESGOS ASOCIADOS AL SERVICIO MICROSOFT EXCHANGE 2019

A continuación, se identifican los resultados de este análisis, los cuales forman parte de la declaración de riesgos y constituyen, 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.24] Denegación de servicio. | | | |

## 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 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. 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 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 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 si 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 AL SERVICIO MICROSOFT EXCHANGE 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 al servicio Microsoft Exchange 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 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, se 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 mitigan, 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-EX1: 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 MICROSOFT EXCHANGE 2019 | ALCANCE | | |
|---|---|---|---|---|
| | | B | I | A |
| [A.3] Manipulación de los registros de actividad (log). | [A.3.SEC-EX1] Se auditan los buzones de los usuarios. | | | |
| | [A.3.SEC-EX2] Se controla el uso de privilegios. | | | |
| | [A.3.SEC-EX3] Se garantiza al menos 90 días de registros de actividad. | | | |
| | [A.3.SEC-EX4] Se auditan la administración de cuentas. | | | |
| [A.4] Manipulación de los ficheros de configuración | [A.4.SEC-EX1] Los usuarios estándar no disponen de permisos de administrador local ni se encuentran incluidos en un grupo "Administradores". | | | |
| [A.5] Suplantación de la identidad. | [A.5.SEC-EX1] Se han deshabilitado los algoritmos de cifrado inseguros. | | | |
| | [A.5.SEC-EX2] Se controlan los permisos de inicio de sesión y suplantación de identidad. | | | |
| | [A.5.SEC-EX3] Se deshabilitan protocolos inseguros de autenticación. | | | |
| [A.24] Denegación de servicio. | [A.3.SEC-EX4] Se auditan la administración de cuentas. | | | |
| | [A.24.SEC-EX1] Los servicios de Exchange deben encontrarse en un modo de inicio adecuado y tener establecidos los permisos mínimos requeridos. | | | |

# ANEXO A. PASO A PASO CONFIGURACIÓN BASE DE SEGURIDAD SOBRE MICROSOFT EXCHANGE 2019

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento del servicio Microsoft Exchange 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.

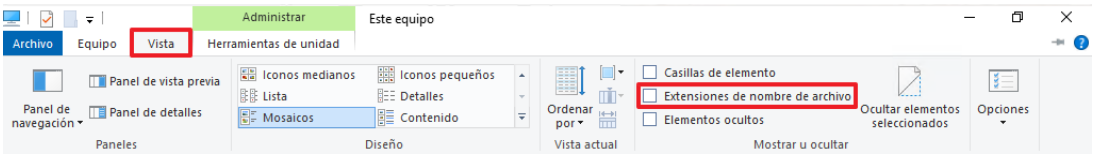
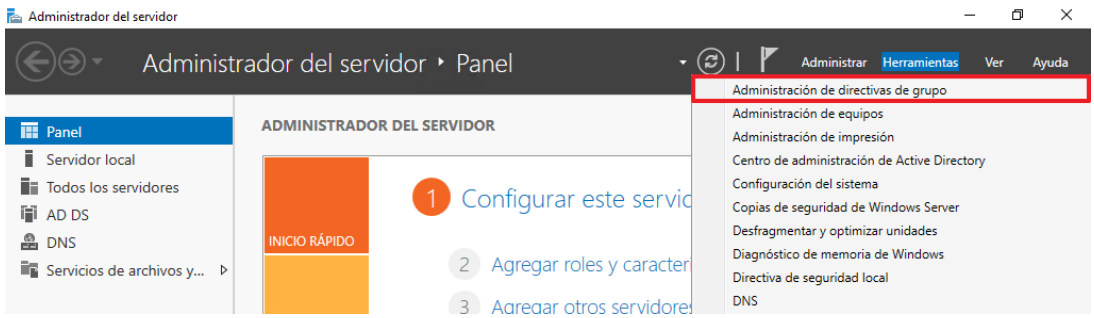
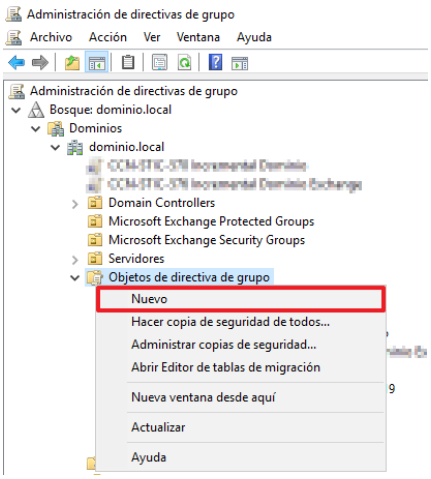
A modo de ejemplo, se procede a realizar un perfilado intermedio de seguridad, aplicado a un servicio Microsoft Exchange 2019. Antes de aplicar esta guía, se deben haber aplicado las configuraciones de seguridad necesarias sobre el servidor miembro Windows Server 2019, para la correcta aplicación de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

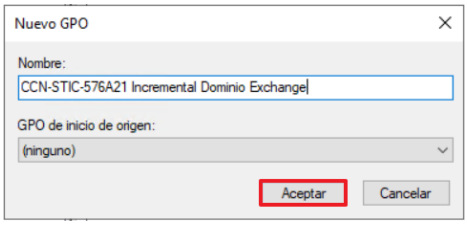
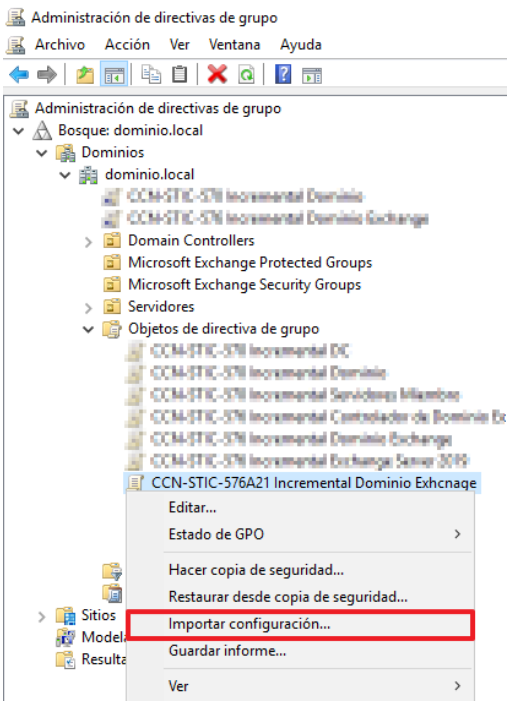
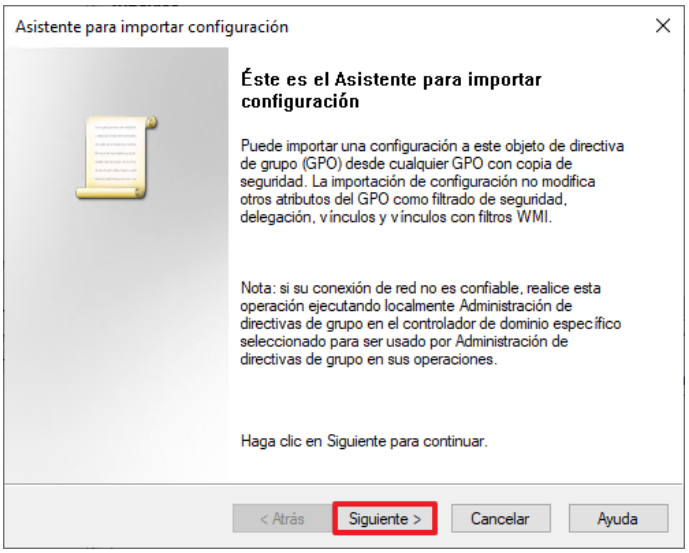
## ANEXO A.1. PREPARACION DEL DOMINIO

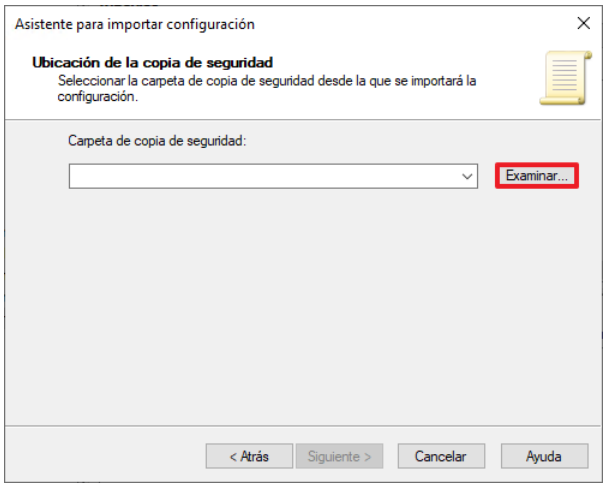
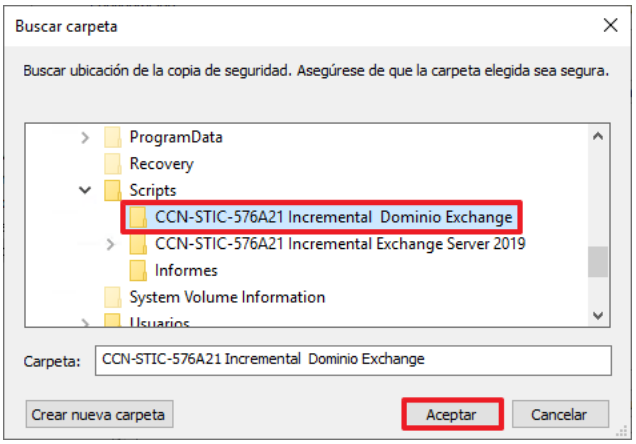
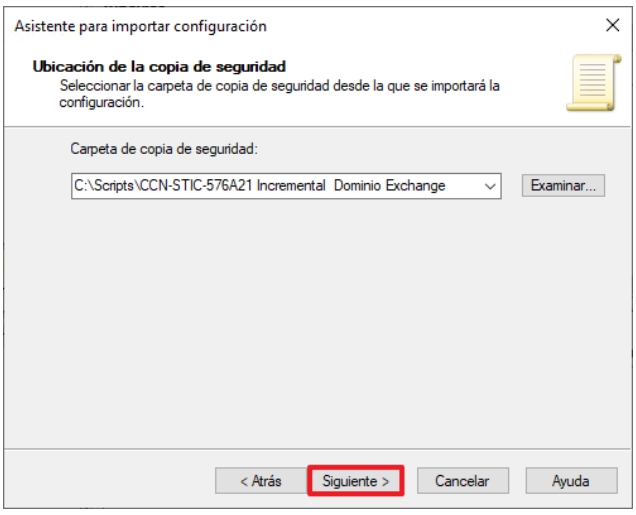
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

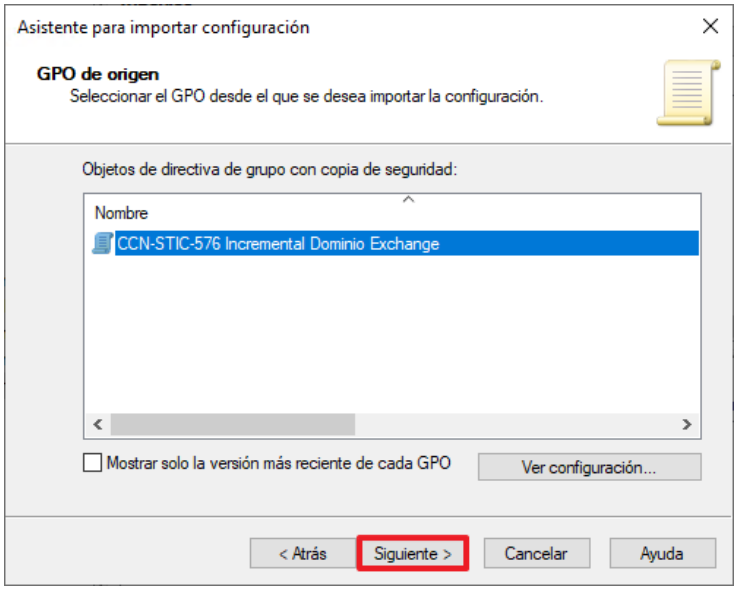
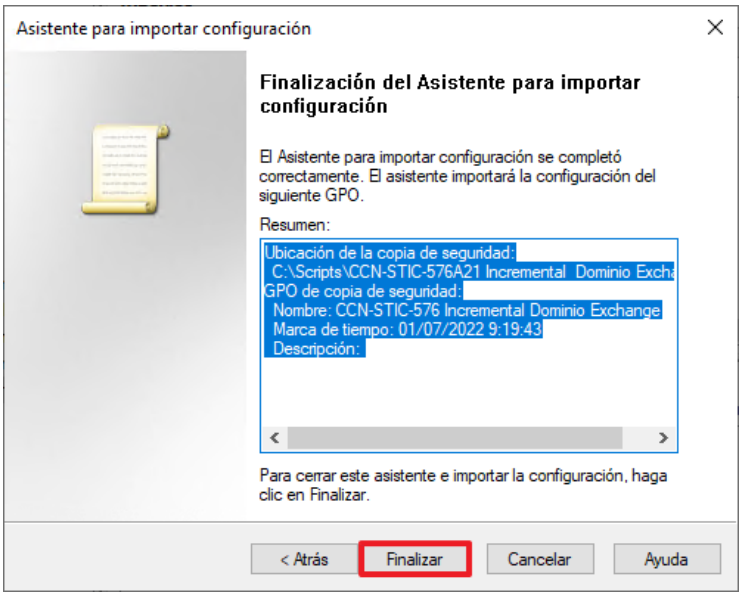
a) **[A.5.SEC-EX3]** Se deshabilitan protocolos inseguros de autenticación. Mediante la aplicación de directivas incluidas en la GPO “CCN-STIC-576A21 Incremental Dominio Exchange”, se procede a la deshabilitación de los protocolos inseguros u obsoletos de autenticación.

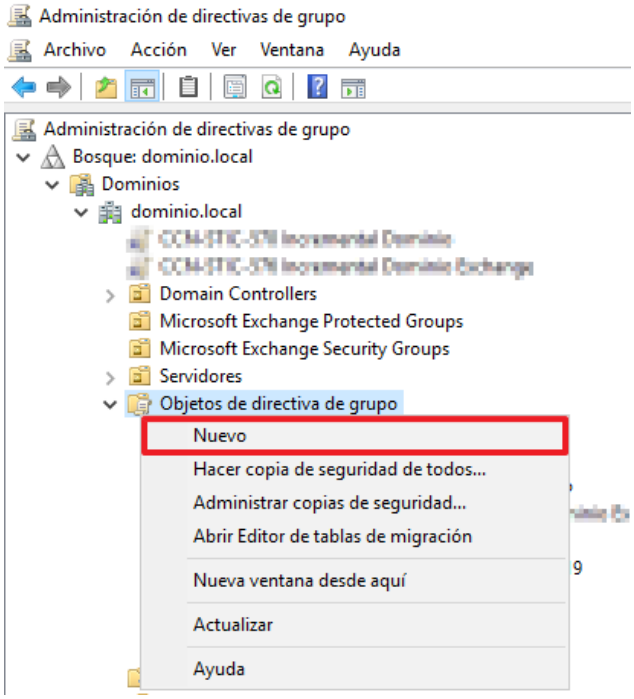
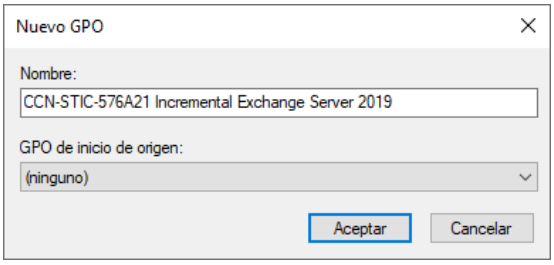
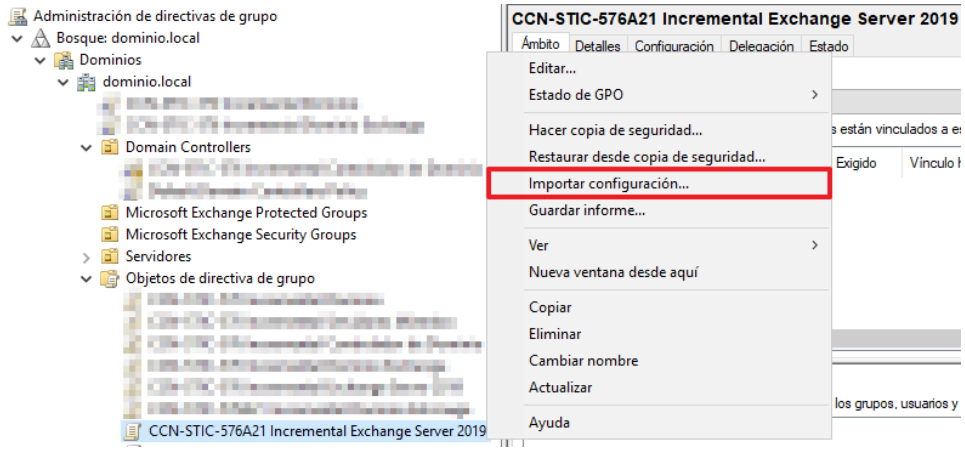
| Paso | Descripción |
|---|---|
| 1. | Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de la guía CCN-STIC-576A21. |
| 2. | Debe iniciar sesión con una cuenta que sea Administrador del Dominio. |
| 3. | Cree el directorio “**Scripts**” en la unidad C:\. |

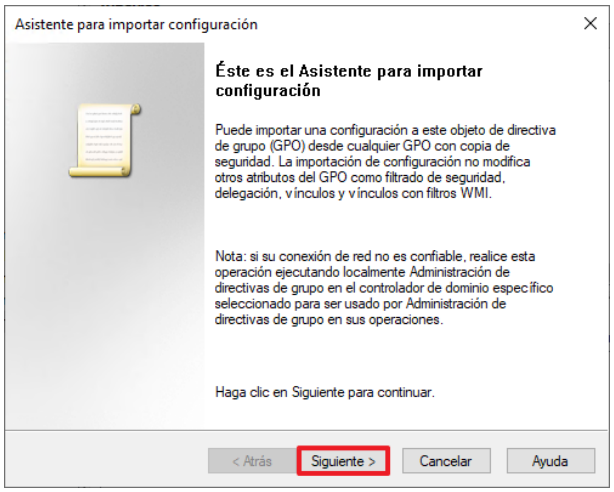
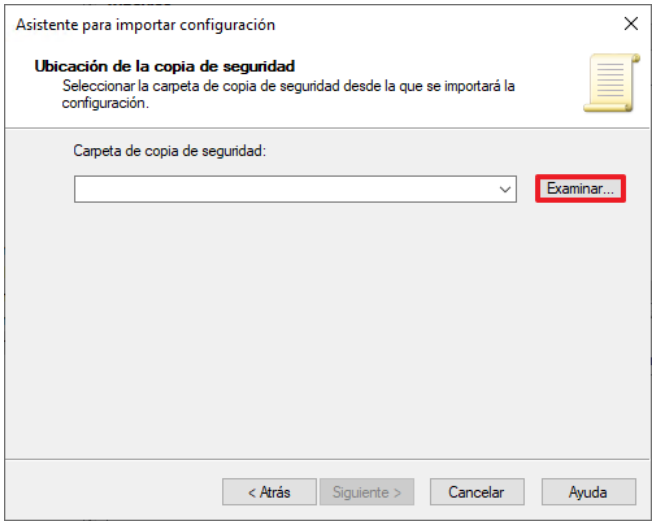
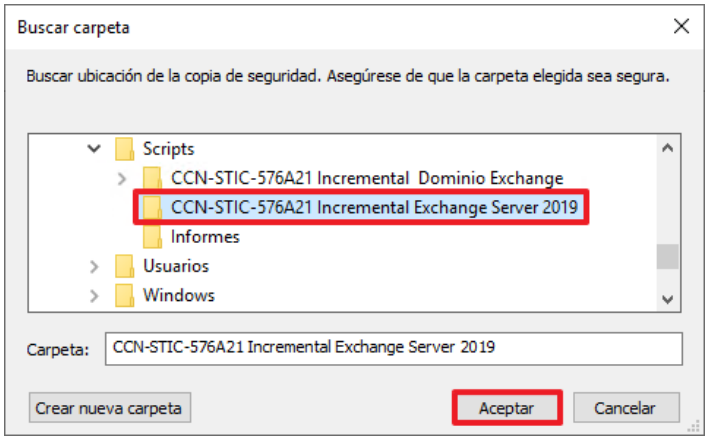
| Paso | Descripción |
|---|---|
| 4. | Copie los ficheros y directorios que acompañan a esta guía al directorio "**C:\Scripts**". |
| 5. | Configure el "**Explorador de archivos**" para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos oculta las extensiones conocidas y este hecho dificulta su identificación. Para ello, pulse sobre el icono del explorador de archivos desde la barra de tareas.<br>  |
| 6. | En el "**Explorador de archivos**" pulse sobre la pestaña "**Vista**" del menú superior y marque la casilla "**Extensiones de nombre de archivos**".<br>  |
| 7. | 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**".<br>  |
| 8. | Despliegue los contenedores y sitúese sobre el nodo "**Objetos de directiva de grupo**". |
| 9. | Pulse con el botón derecho, sobre dicho nodo y seleccione la opción "**Nuevo**".<br>  |

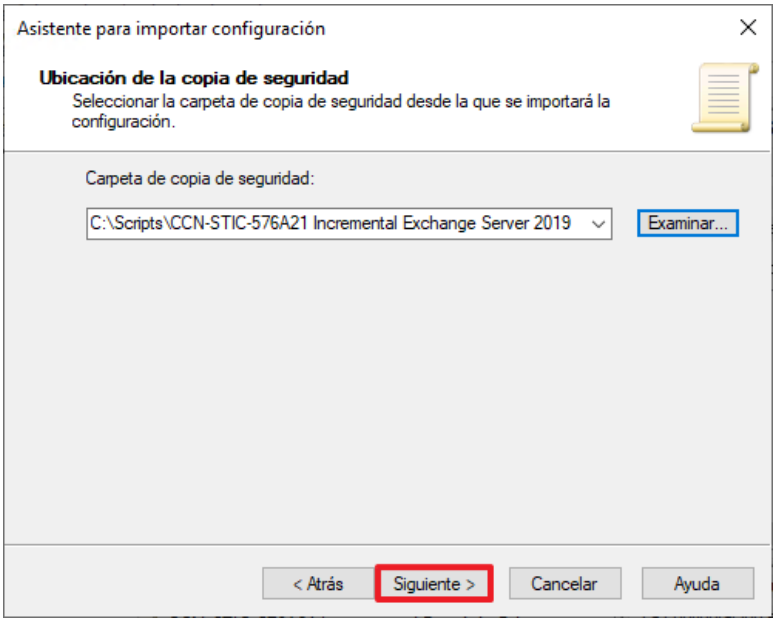
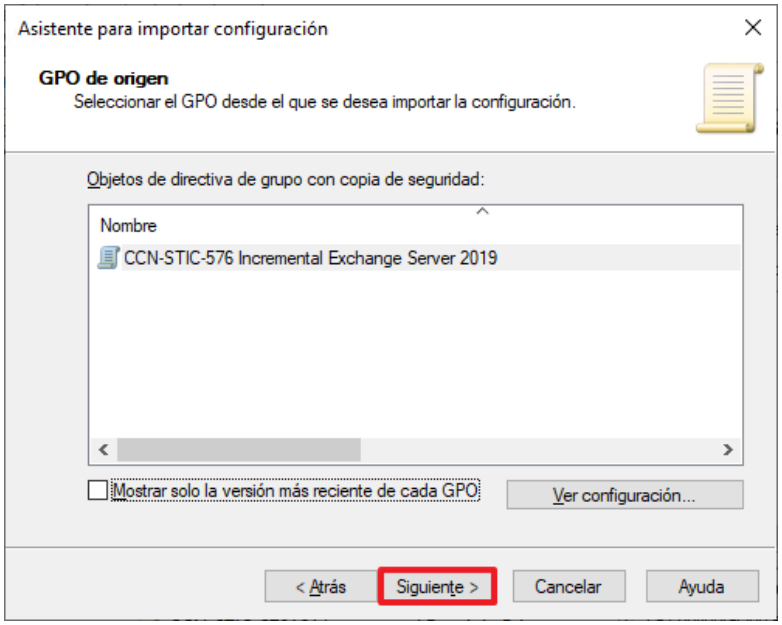
| Paso | Descripción |
|---|---|
| 10. | Introduzca como nombre “CCN-STIC-576A21 Incremental Dominio Exchange” y pulse el botón “**Aceptar**”.<br>  |
| 11. | Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “**Importar configuración...**”.<br>  |
| 12. | En el asistente de importación de configuración, pulse el botón “**Siguiente >**”.<br>  |

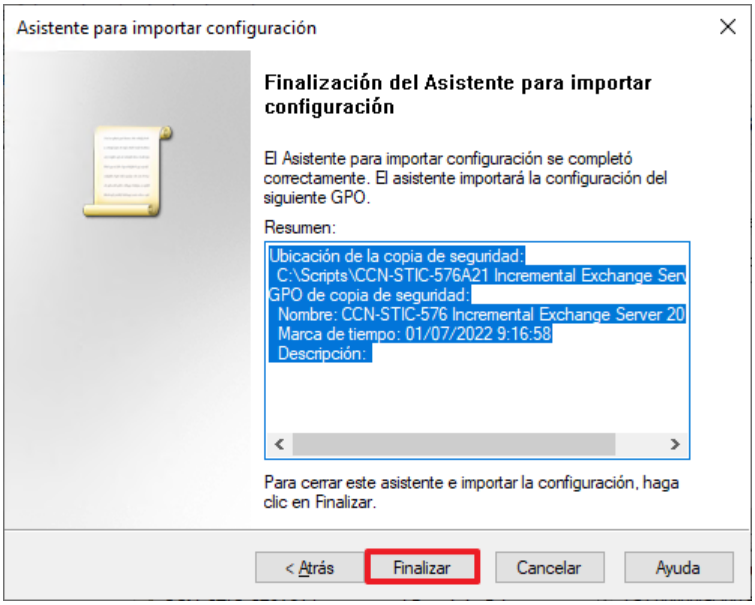
| Paso | Descripción |
|---|---|
| 13. | En la selección de copia de seguridad pulse el botón "**Siguiente >**". No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. |
| 14. | En "**Carpeta de copia de seguridad**", pulse el botón "**Examinar...**".<br>  |
| 15. | Seleccione la carpeta "CCN-STIC-576A21 Incremental Dominio Exchange" que encontrará en el directorio "**C:\Scripts**" y pulse el botón "**Aceptar**".<br>  |
| 16. | Pulse el botón "**Siguiente >**" una vez seleccionada la carpeta adecuada.<br>  |

| Paso | Descripción |
|---|---|
| 17. | En la pantalla siguiente compruebe que aparece la política de seguridad "CCN-STIC-576A21 Incremental Dominio Exchange" y pulse el botón "**Siguiente >**".<br>  |
| 18. | Para completar el asistente pulse el botón "**Finalizar**".<br>  |
| 19. | 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. |

| Paso | Descripción |
|---|---|
| 20. | Nuevamente, pulse con el botón derecho, sobre "**Objetos de directiva de grupo**" y seleccione la opción "**Nuevo**".<br>  |
| 21. | Introduzca como nombre "CCN-STIC-576A21 Incremental Exchange Server 2019" y pulse el botón "**Aceptar**".<br>  |
| 22. | Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción "**Importar configuración...**".<br>  |

| Paso | Descripción |
|---|---|
| 23. | En el asistente de importación de configuración, pulse el botón "**Siguiente >**". No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.<br>  |
| 24. | En "Carpeta de copia de seguridad", pulse el botón "**Examinar...**".<br>  |
| 25. | Seleccione la carpeta "CCN-STIC-576A21 Incremental Exchange Server 2019" que encontrará en el directorio "**C:\Scripts**" y pulse el botón "**Aceptar**".<br>  |

| Paso | Descripción |
|---|---|
| 26. | Pulse el botón "**Siguiente >**" una vez seleccionada la carpeta adecuada.<br>  |
| 27. | En la pantalla siguiente compruebe que aparece la política de seguridad "CCN-STIC-576A21 Incremental Exchange Server 2019" y pulse el botón "**Siguiente >**".<br>  |

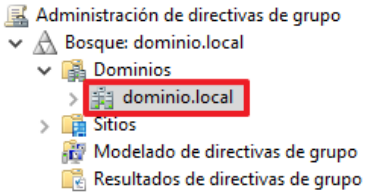
| Paso | Descripción |
|---|---|
| 28. | Para completar el asistente pulse el botón "**Finalizar**".<br>  |
| 29. | Pulse el botón "**Aceptar**" para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración y continúe con el siguiente paso. |

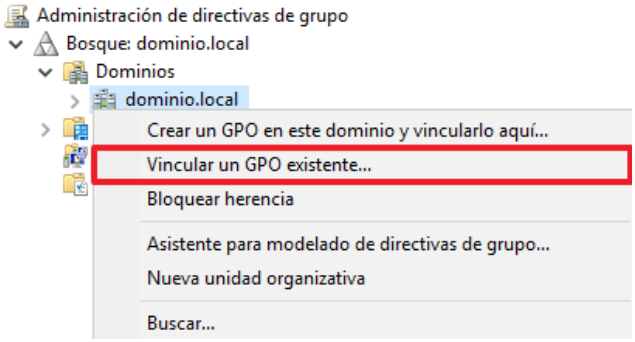
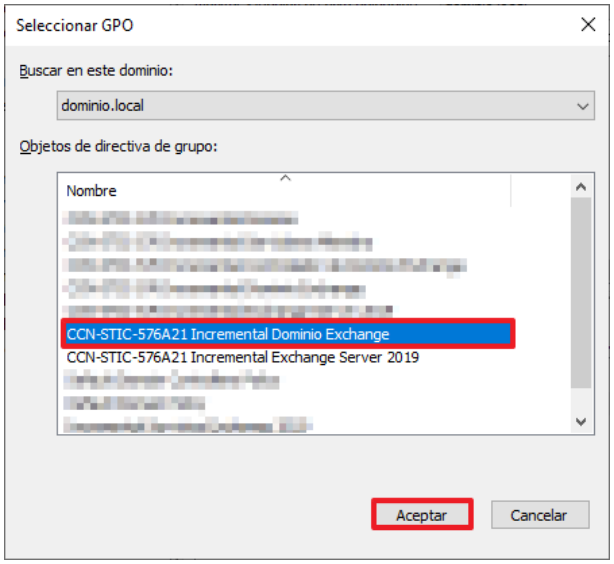
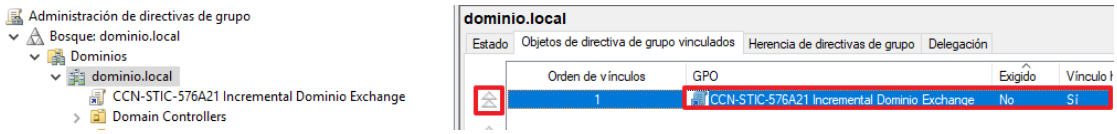
## ANEXO A.2. IMPLEMENTACION DE POLITICAS DE SEGURIDAD

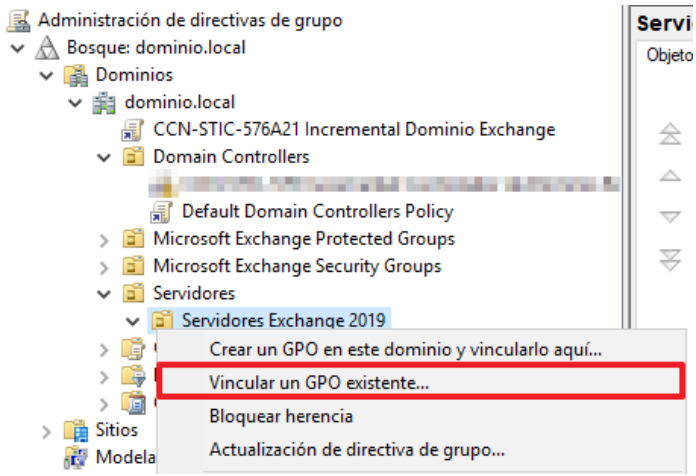
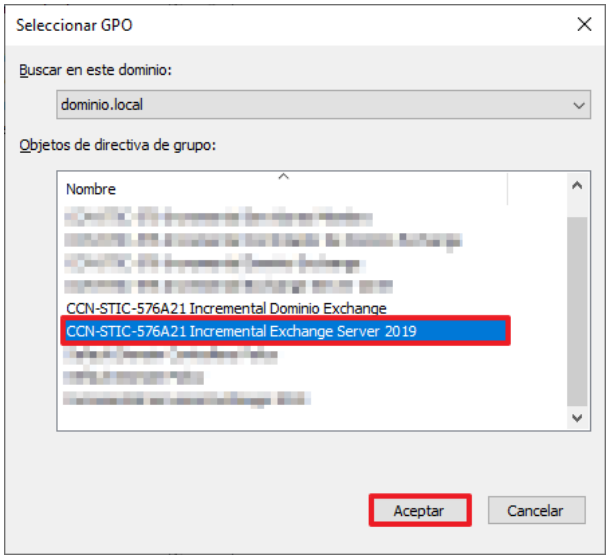
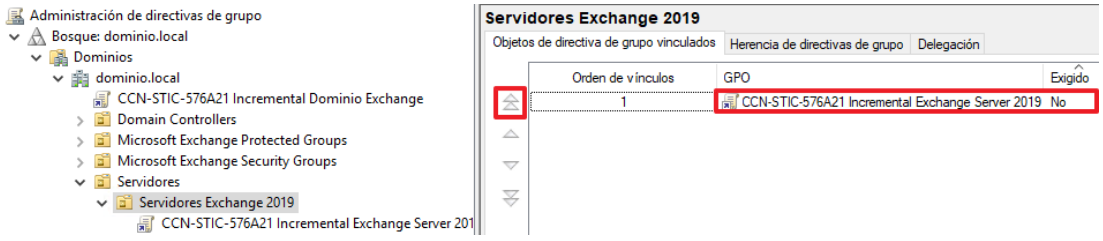
El presente punto establece la aplicación de las políticas de seguridad una vez que se han tenido en consideración las condiciones definidas en el punto previo.

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

a) **[A.24.SEC-EX1]** Los servicios de Exchange deben encontrarse en un modo de inicio adecuado y tener establecidos los permisos mínimos requeridos. La aplicación de directivas incluidas en la GPO "CCN-STIC-576A21 Incremental Exchange Server 2019" permiten el cumplimiento de esta medida de seguridad.

| Paso | Descripción |
|---|---|
| 30. | Si previamente ha cerrado la consola, inicie la herramienta de administración de directivas de grupo. |
| 31. | Despliegue el nodo y posiciónese sobre su dominio.<br>  |

| Paso | Descripción |
|---|---|
| 32. | Pulse con el botón derecho sobre el mismo y seleccione la opción "**Vincular un GPO existente...**".<br>  |
| 33. | Seleccione la política "CCN-STIC-576A21 Incremental Dominio Exchange" y pulse el botón "**Aceptar**".<br>  |
| 34. | Una vez agregado, en el panel derecho seleccione la pestaña "**Objetos de directiva de grupo vinculados**" y seleccione la política "CCN-STIC-576A21 Incremental Dominio Exchange". |
| 35. | Pulse el botón con la flecha que apunta hacia arriba hasta situar la política "CCN-STIC-576A21 Incremental Dominio Exchange" en primer lugar dentro del orden de vínculo.<br>  |

| Paso | Descripción |
|---|---|
| 36. | Para continuar con la aplicación de las directivas anteriormente creadas, seleccione la Unidad Organizativa donde esté alojado su Servidor de Exchange 2019 y seleccione la opción "**Vincular un GPO existente...**".<br>  |
| 37. | Seleccione la política "CCN-STIC-576A21 Incremental Exchange Server 2019" y pulse el botón "**Aceptar**".<br>  |
| 38. | Una vez agregado, en el panel derecho seleccione la política "CCN-STIC-576A21 Incremental Exchange Server 2019" y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo.<br>  |

## 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 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 Exchange 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.3.1. ASIGNACION DE PERMISOS Y ROLES

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

a) **[A.3.SEC-EX2]** Se controla el uso de privilegios. El usuario debe disponer de los permisos exclusivamente necesarios para el correcto desempeño de su actividad laboral, evitando la asignación de privilegios no necesarios.

b) **[A.4.SEC-EX1]** Los usuarios estándar no deben disponen de permisos de administrador local ni encontrarse incluidos en un grupo con permisos de administrador. La pertenencia a grupos de administración debe ser restringida sólo al personal responsable de la administración del servidor, nunca al usuario estándar.

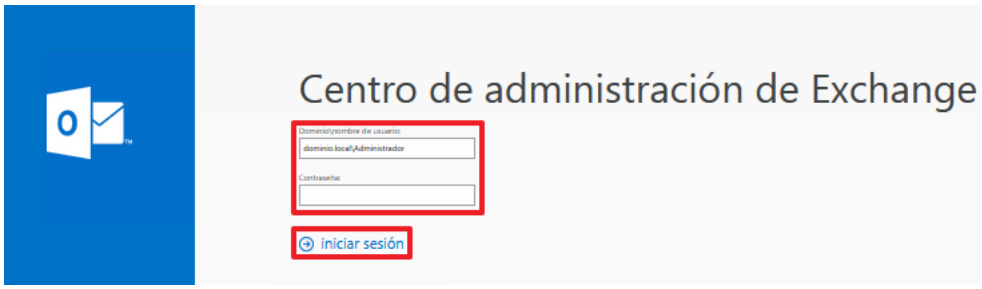
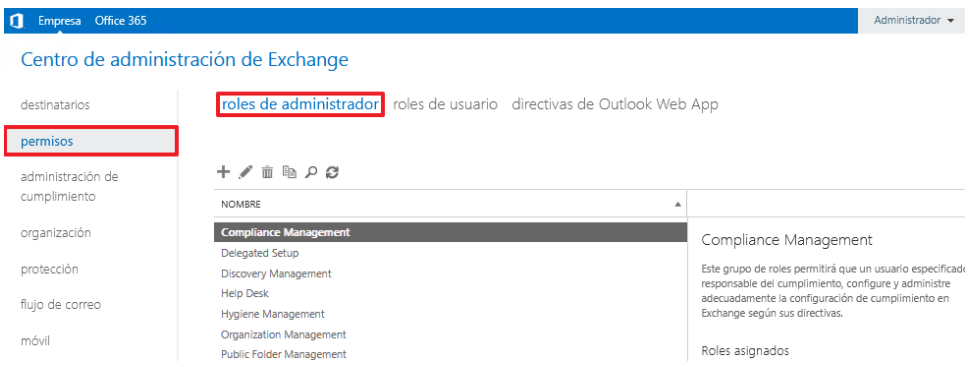
c) **[A.5.SEC-EX2]** Se controlan los permisos de inicio de sesión. La creación del buzón de usuario incluye la asignación de los permisos de inicio de sesión.

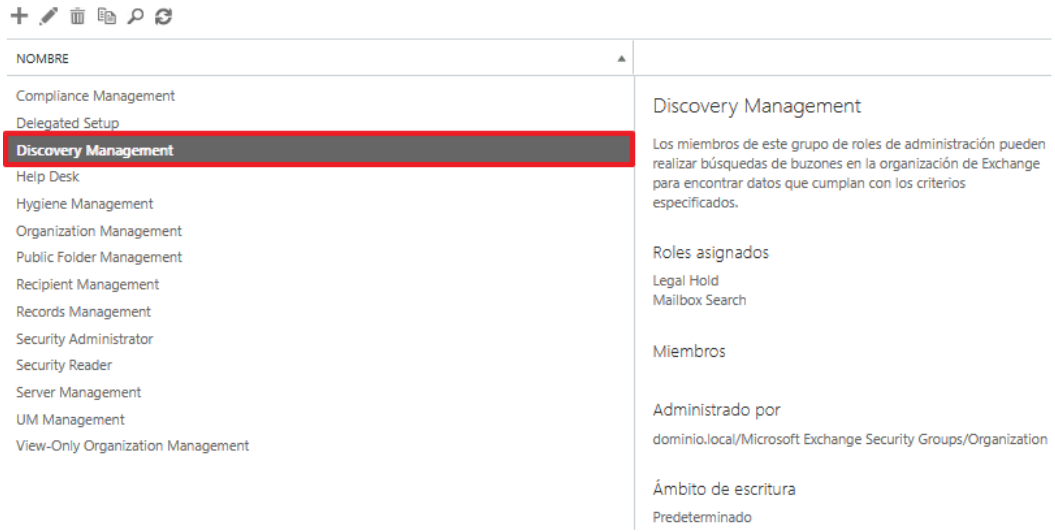
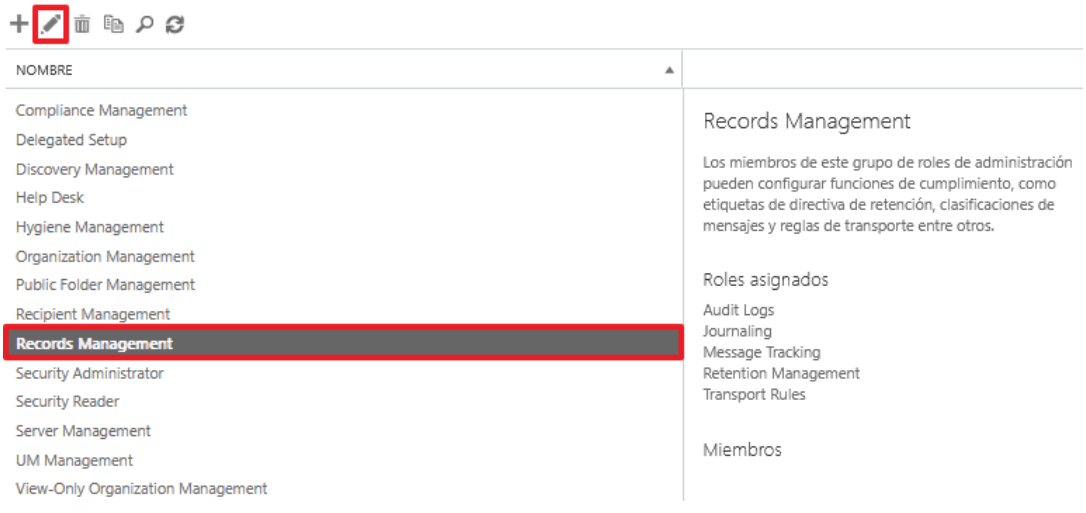
Antes de poder aplicar diferentes mecanismos de auditoría y conformidad, debe tener presente que determinadas funcionalidades requieren de la obtención de permisos específicos para la realización de las operaciones. La asignación de dichos permisos se basa en el modelo RBAC (Role Based Access Control). Dicho modelo tiene su base fundamental en la pertenencia a grupos y la aplicación de directivas sobre dichos grupos.

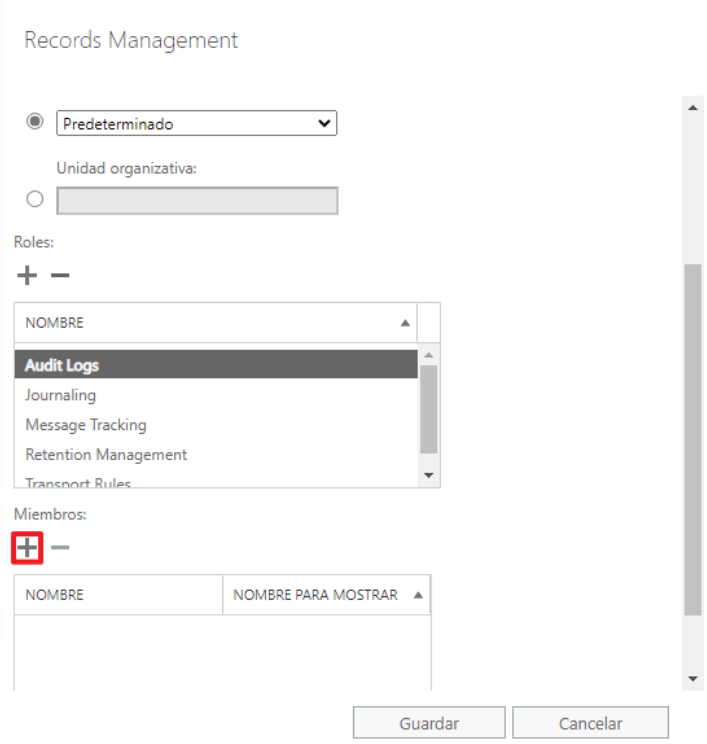
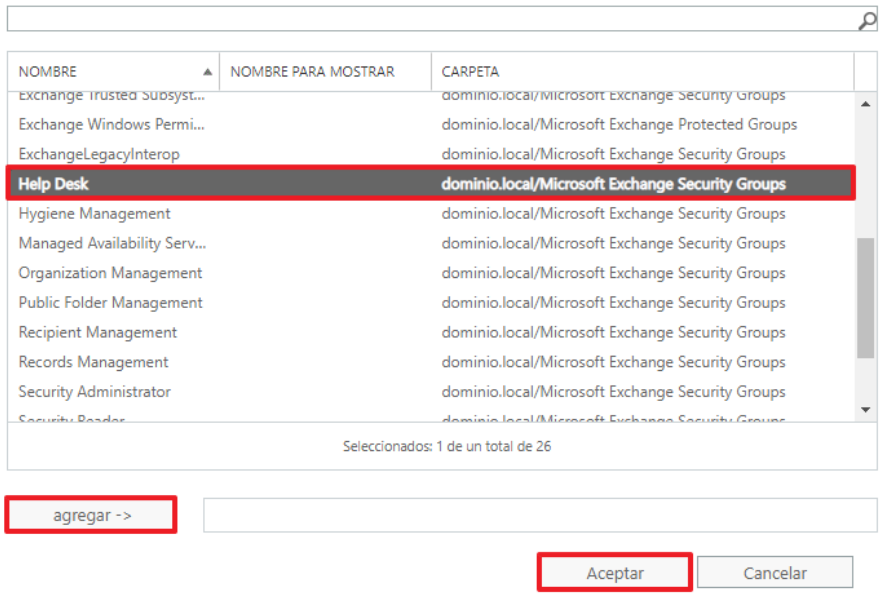
Así mismo, este modelo permite establecer una jerarquía de roles segregados, de tal forma que algunos usuarios de la organización pueden realizar tareas de administración del servidor, a la vez que otros pueden asumir la funcionalidad de auditores del sistema.

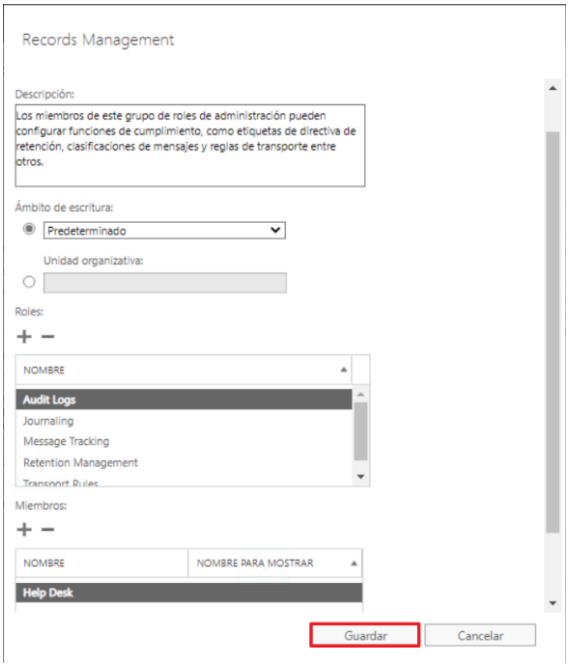
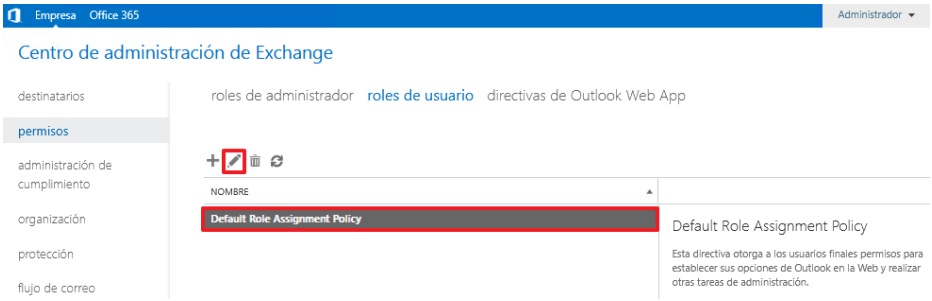
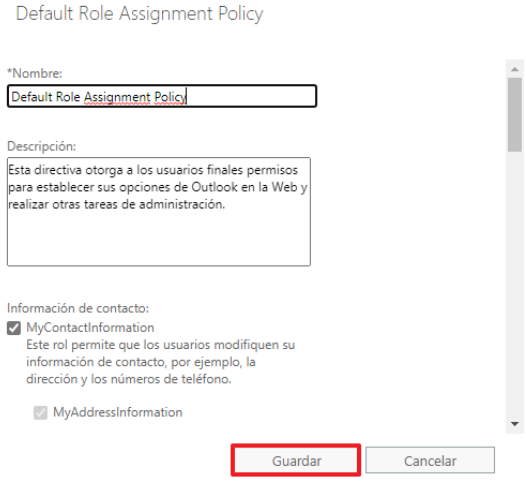
La administración de roles y permisos se puede realizar a través de la consola Web de administración (Exchange Control Panel) o bien a través de cmdlets de PowerShell. Para una mejor comprensión, este anexo mostrará cómo realizar dichas acciones a través del entorno gráfico vía Web.

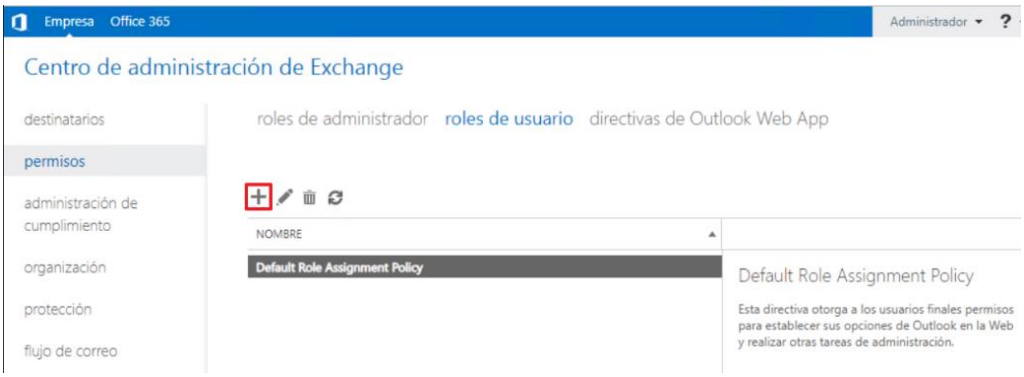
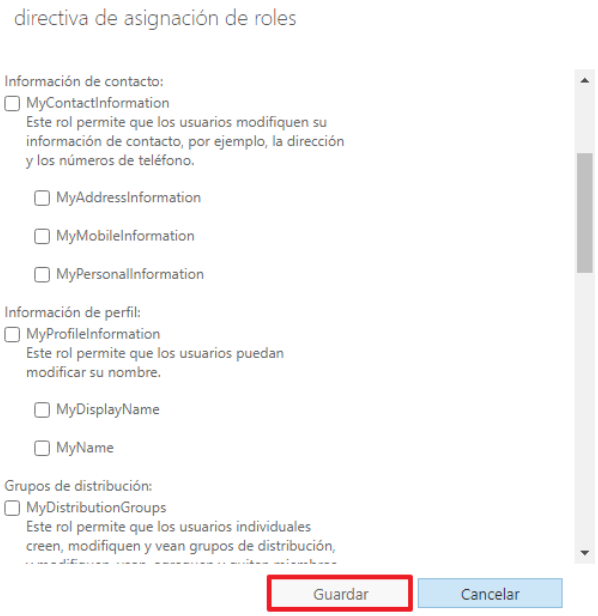
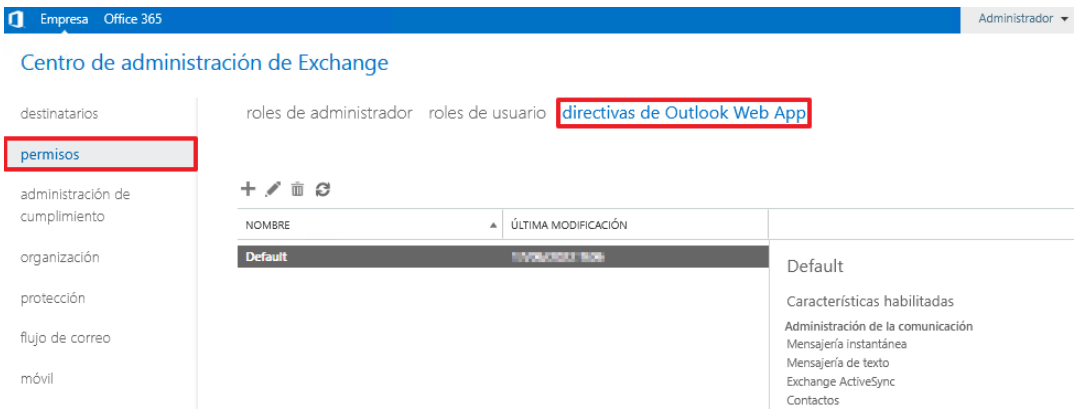
**Nota:** Si desea conocer más sobre la administración de roles y permisos visite la siguiente URL: https://technet.microsoft.com/es-es/library/jj657511(v=exchg.150).aspx.

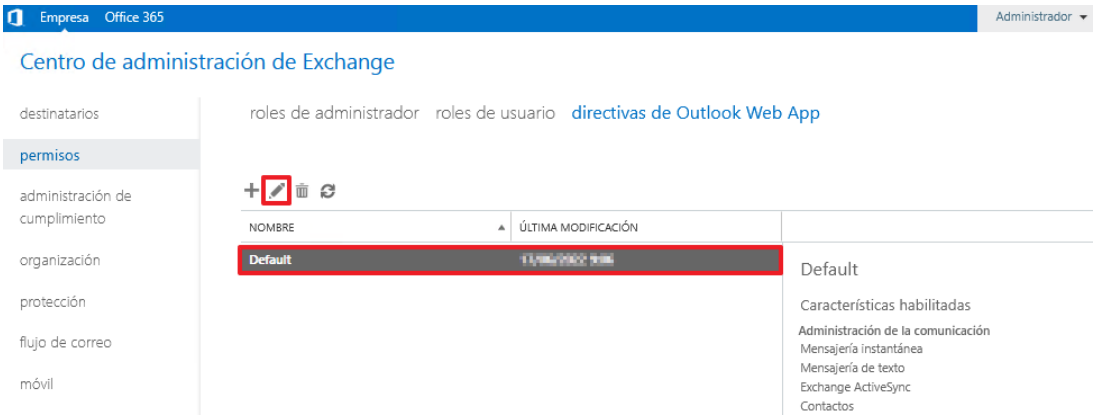
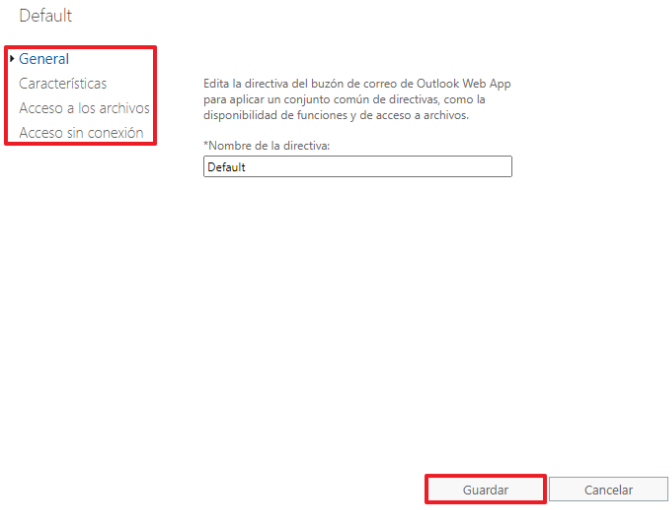
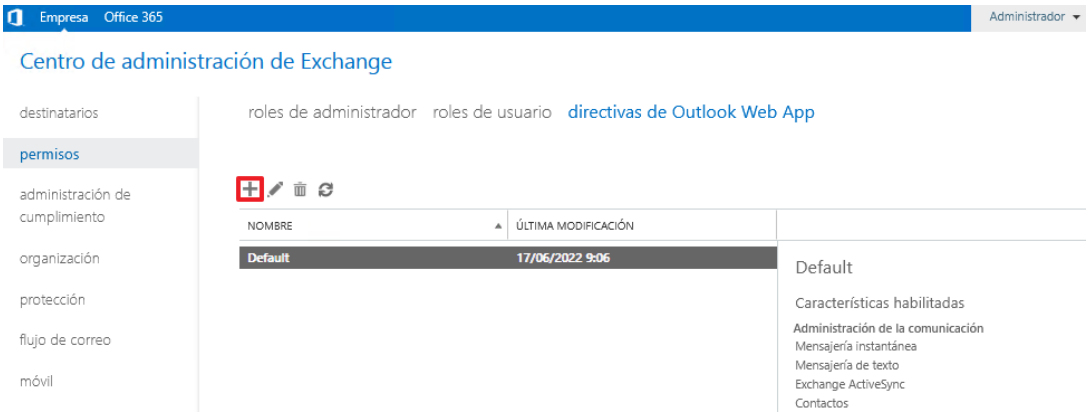
| Paso | Descripción |
|---|---|
| 39. | A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2019 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2019. |
| 40. | Abra el explorador web de su organización, en este caso se usará Microsoft Edge.<br>  |
| 41. | Introduzca la URL para acceder al "**Exchange Administrative Center**" de su organización.<br>  |
| 42. | Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.<br>  |
| 43. | Seleccione el enlace "**Permisos**" para configurar los permisos RBAC.<br>  <br>**Nota:** Desde este menú se pueden asignar roles de administrador predeterminados a grupos nuevos o existentes en la organización, o también se pueden crear nuevos roles de administrador con permisos específicos. |

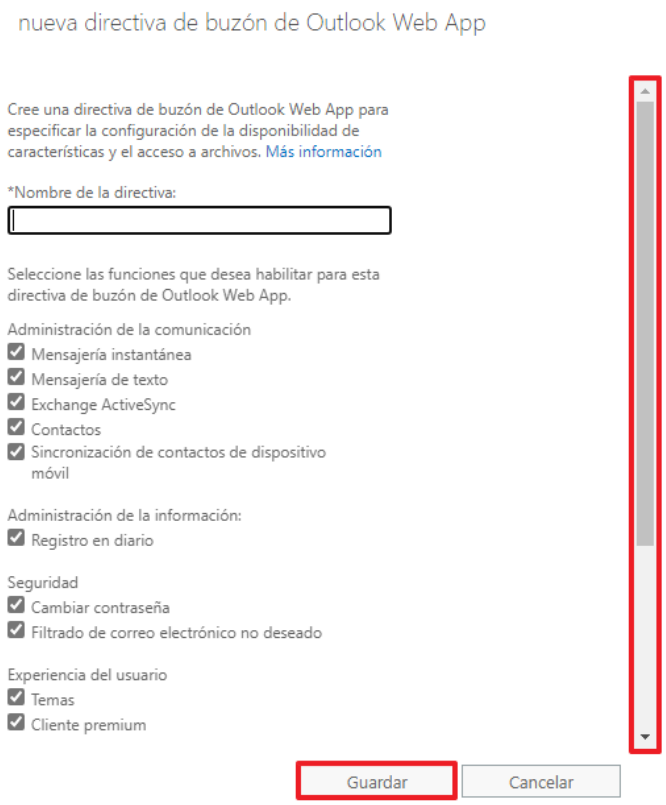
| Paso | Descripción |
|---|---|
| 44. | Por ejemplo, el rol denominado "**Discovery Management**" o administración de la detección, tiene asignados los permisos necesarios para trabajar con la retención legal, así como la suspensión y exhibición de datos electrónicos. Estos permisos incluyen la realización de búsquedas de buzones en la organización para obtener datos que cumplan determinados criterios y la configuración de retenciones legales en los diferentes buzones de correo.<br>  |
| 45. | Por otro lado, el rol denominado "**Records Management**" o administración de registros, incluye otra serie de permisos asignados relativos a las capacidades de auditoría. A continuación, a modo de ejemplo, se va a asignar dicho rol a un grupo de seguridad de Directorio Activo. Para ello, seleccione el rol "**Records Management**" y pulse el botón "**Modificar**".<br>  |

| Paso | Descripción |
|---|---|
| 46. | A continuación, en la sección "**Miembros**", podrá agregar un grupo de seguridad de Directorio Activo pulsando en el botón "**+**".   |
| 47. | En la pantalla de selección, localice las cuentas de usuarios o grupos de seguridad universales que se desean añadir y pulse el botón "**Agregar**". Por ejemplo, seleccione el grupo "**Help Desk**" y pulse en el botón "**agregar**" y "**Aceptar**".   |

| Paso | Descripción |
|---|---|
| 48. | A continuación, pulse sobre el botón "**Guardar**" para hacer efectivos los cambios.<br>  |
| 49. | Es posible modificar el grupo de roles de usuario por defecto, pulse sobre el grupo "**Default Role Assignment Policy**" y a continuación, seleccione "**Modificar**".<br>  |
| 50. | A continuación, se pueden modificar los campos que sean necesarios para adaptarlos a los requerimientos de su organización y pulse "**Guardar**".<br>  |

| Paso | Descripción |
|---|---|
| 51. | Del mismo modo es posible crear un grupo de roles de usuario nuevo, para ello seleccione la pestaña "**roles de usuario**" pulse sobre la opción nuevo o "**+**".<br>  |
| 52. | A continuación, cumplimente los campos en función de las necesidades de su organización y pulse "Guardar".<br>  |
| 53. | Del mismo modo puede cambiar las directivas de Outlook Web App, para ello diríjase a la opción "**directivas de Outlook Web App**".<br>  |

| Paso | Descripción |
|---|---|
| 54. | A continuación, seleccione la opción que viene creada por defecto, para ello seleccione "**Default**" y pulse el icono "**Modificar**".<br>  <br>**Nota:** El valor predeterminado de directiva de buzón de correo de Outlook Web App tiene todas las opciones habilitadas de forma predeterminada. |
| 55. | Cumplimente los campos en función de las necesidades de su organización y pulse "**Guardar**".<br>  |
| 56. | Si desea crear un grupo de directivas nuevo, debe pulsar sobre nuevo o "**+**".<br>  |

| Paso | Descripción |
|---|---|
| 57. | Rellene los campos en función de las necesidades de su organización y pulse "**Guardar**".   |

## ANEXO A.3.2. CERTIFICADOS

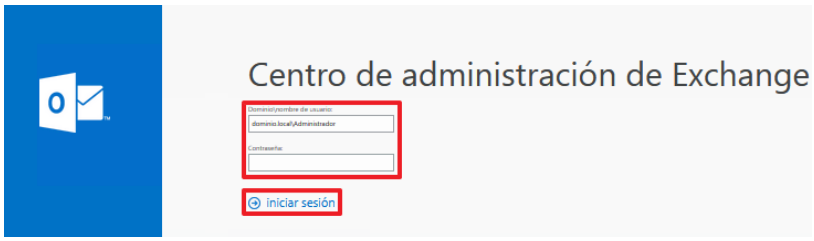
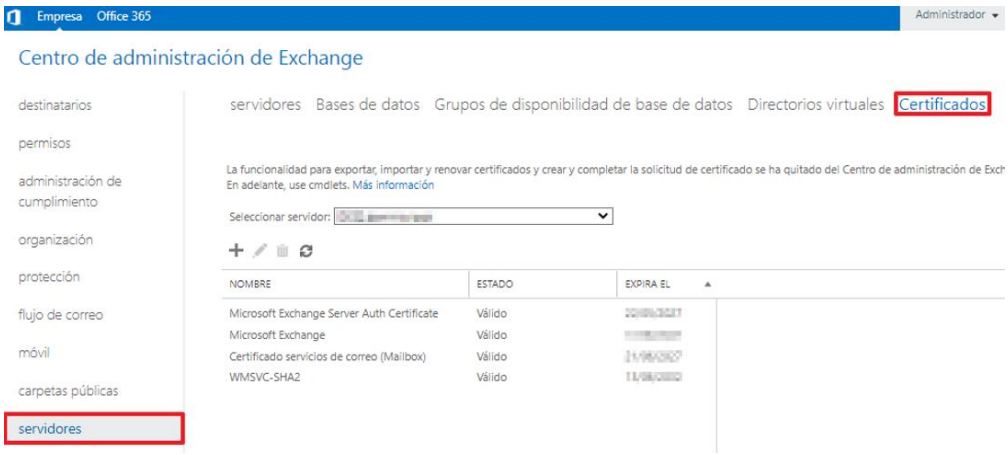
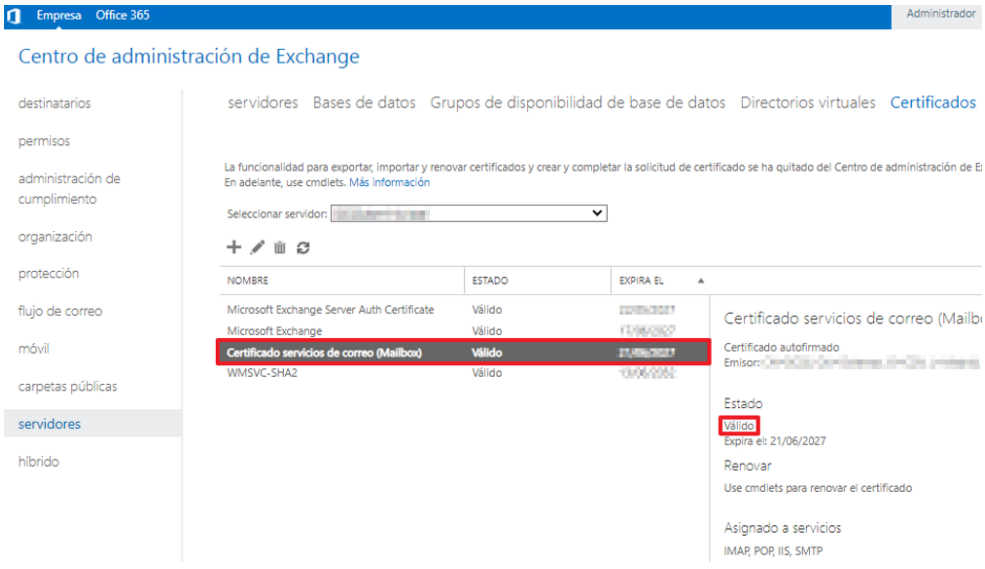
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.5.SEC-EX1]** Se han deshabilitado los algoritmos de cifrado inseguros. El uso de certificados emitidos por una entidad certificadora de confianza (de aquí en adelante, CA de confianza), permitirá a los usuarios el cifrado de sus comunicaciones evitando el uso de algoritmos de cifrado inseguros.

b) **[A.5.SEC-EX2]** Se debe evitar la suplantación de identidad del usuario. La instalación de un certificado emitido por una CA de confianza, permitirá la correcta identificación del usuario evitando la suplantación del mismo.

A continuación, se muestra un ejemplo de cómo instalar un certificado emitido por una CA autorizada. En este paso a paso se da por hecho que ya se ha solicitado un certificado a una CA autorizada y se ha obtenido el certificado, por lo que se explicará únicamente cómo instalarlo.

**Nota**: Se utiliza en este ejemplo un certificado autofirmado, se recomienda el uso de certificados emitidos por una CA de confianza.

| Paso | Descripción |
|---|---|
| 58. | Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.<br>  |
| 59. | Seleccione en el menú lateral izquierdo la opción "**servidores**" y a continuación seleccione "**Certificados**".<br>  <br>**Nota:** En este ejemplo se da por hecho que se ha solicitado y obtenido previamente un certificado emitido por una entidad certificadora autorizada para este servidor. |
| 60. | Seleccione el certificado obtenido previamente de la entidad certificadora, su estado debe ser válido para el correcto funcionamiento de Microsoft Exchange 2019.<br>  <br>**Nota:** Es necesario vincular el certificado con el servidor web correspondiente adecuándose a las necesidades de su organización. |

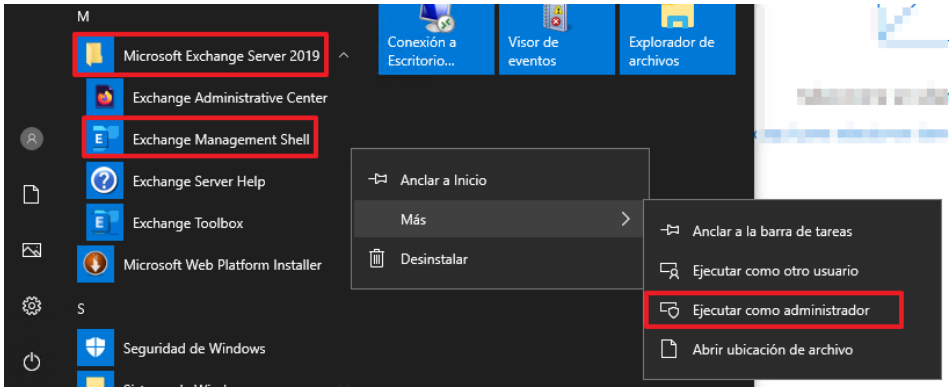
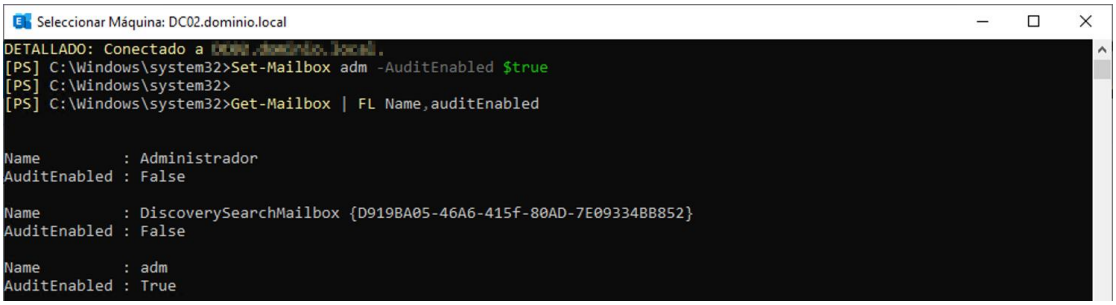
## ANEXO A.3.3. REGISTRO DE ACTIVIDAD

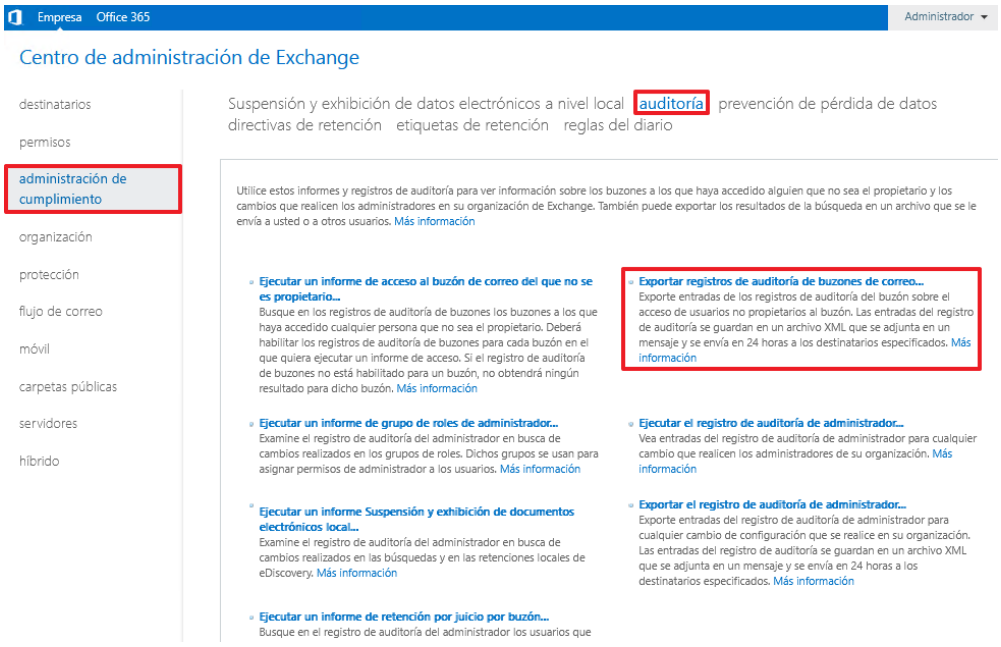
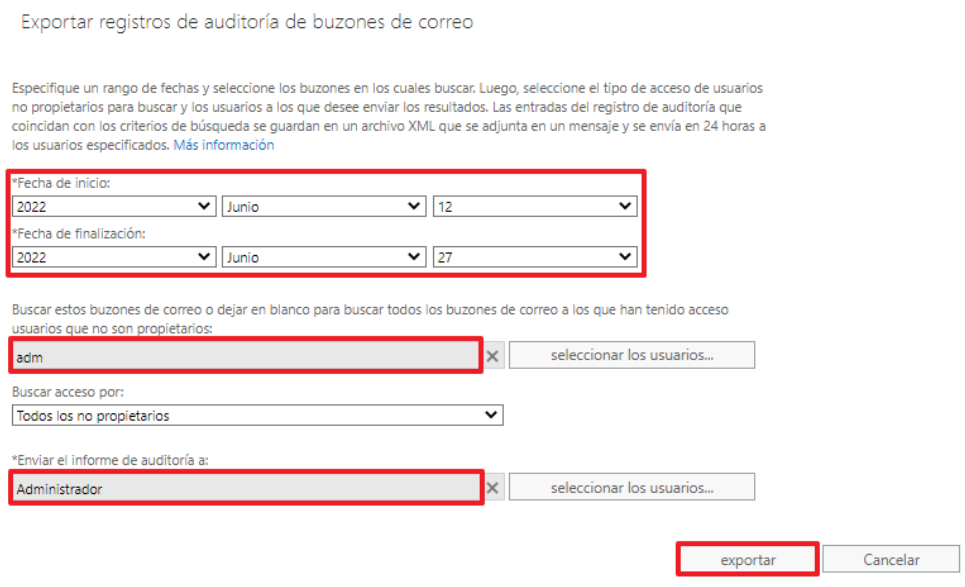
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.3.SEC-EX3]** Se garantiza al menos 90 días de registros de actividad. La generación de los registros de actividad y su posterior almacenamiento permitirán garantizar la existencia de evidencias temporales suficientes.

Es recomendable que la ubicación de los registros sea diferente a la del sistema, además de tener limitado el acceso únicamente a los usuarios autorizados.

Mediante el registro de auditoría de buzón, se puede registrar el acceso y controlar los inicios de sesión a los buzones de correo por parte de sus propietarios, delegados (incluidos los administradores con permisos de acceso total al buzón) y administradores.

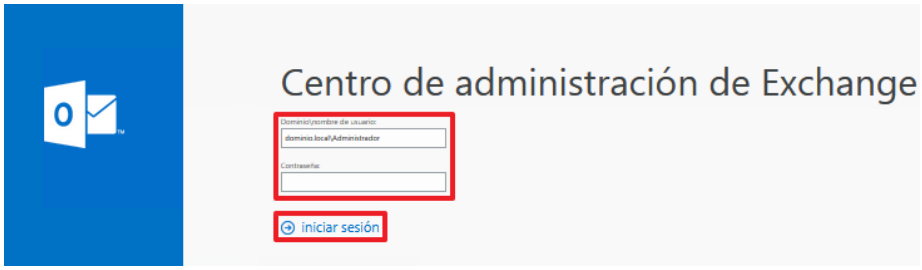
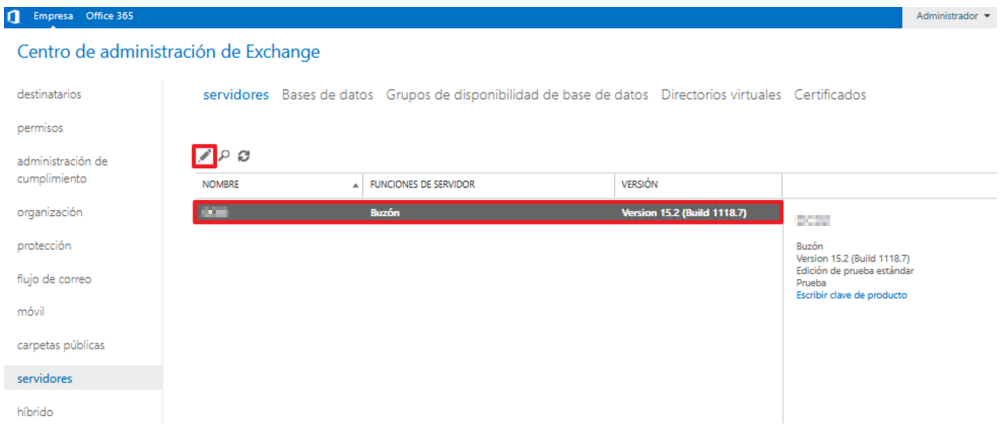
| Paso | Descripción |
|---|---|
| 61. | Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2019 con un usuario con permisos de administrador. |
| 62. | Pulse sobre el menú inicio, despliegue la carpeta “Microsoft Exchange Server 2019” y pulsando con botón derecho en “**Exchange Management Shell**”, seleccione “**Ejecutar como administrador**”.<br>  <br><br>**Nota:** El sistema le solicitará elevación de privilegios. |
| 63. | Una vez conectado al Shell, ejecute la siguiente sintaxis:<br>**> Set-Mailbox <identity> -AuditEnabled $true**<br>**> Get-Mailbox \| FL Name,auditEnabled**<br>  <br><br>**Nota:** En este ejemplo se habilita la auditoría para el buzón de “adm”. |

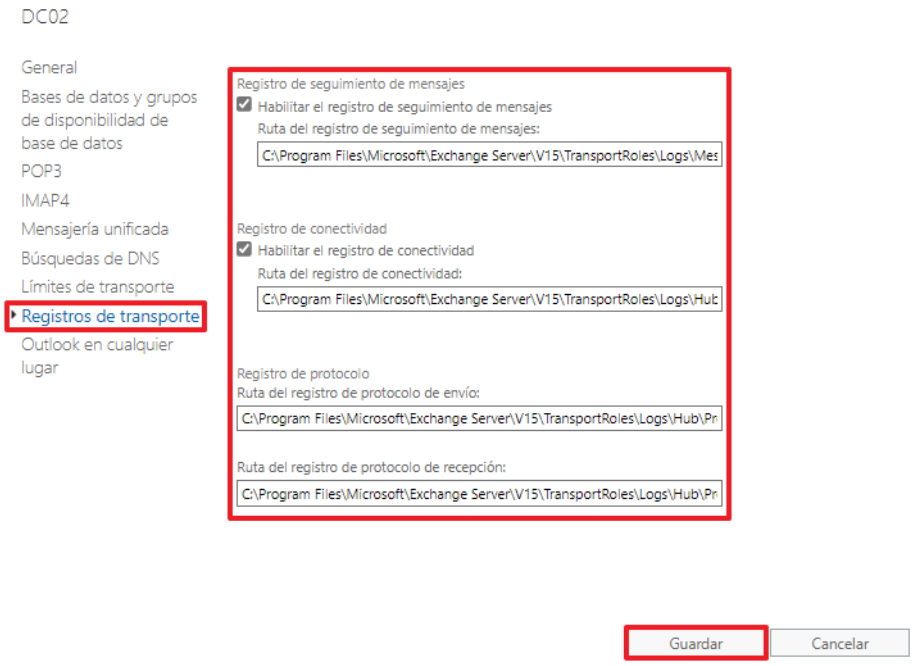
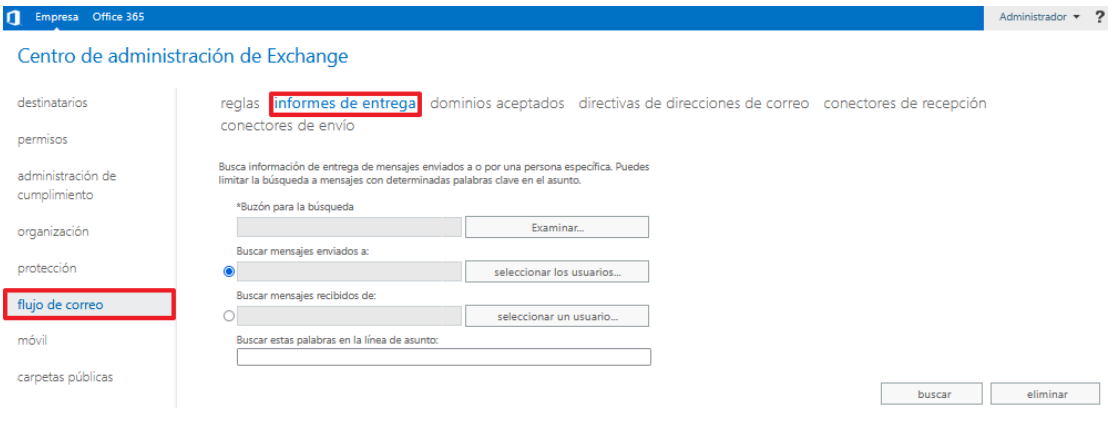
| Paso | Descripción |
|---|---|
| 64. | Es posible exportar los registros de auditoría de buzones desde la consola Web de administración de Exchange, desde el menú "**administración de cumplimiento**" seleccionando la opción "**Auditoría**" y pulsando en "**Exportar registros de auditoría de buzones de correo…**".<br>  <br>**Nota:** Exchange puede tardar hasta 24 horas en generar el informe y enviarlo al destinatario seleccionado. |
| 65. | Deberá indicar el intervalo de fechas, los buzones donde realizar la búsqueda y el buzón de destino del informe. Una vez elegidos los campos, pulse "**exportar**".<br>  |

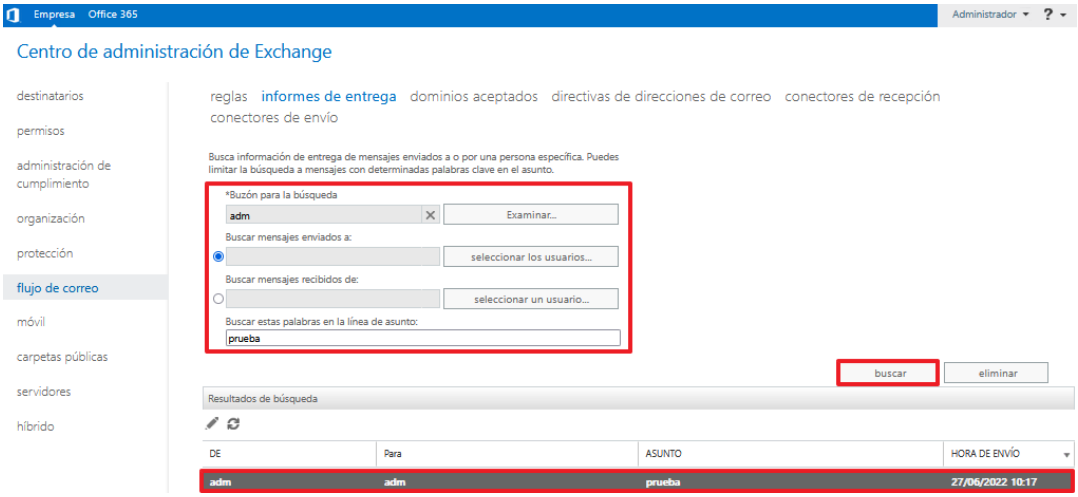
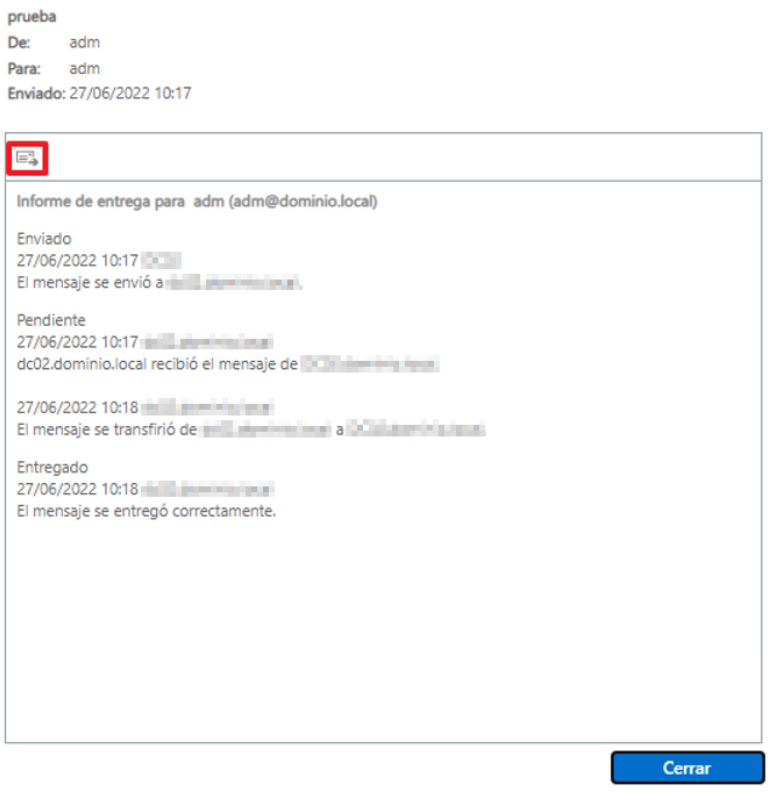
## ANEXO A.3.4. REGISTRO DE SEGUIMIENTO DE MENSAJES

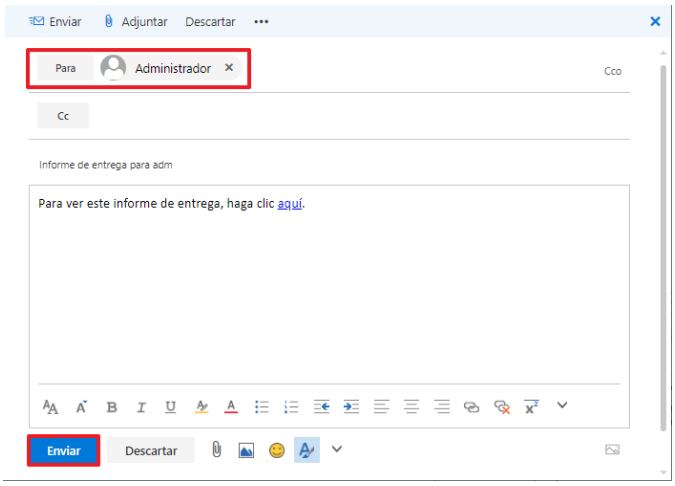
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.3.SEC-EX1]** Se auditan los buzones de los usuarios. La habilitación del seguimiento de mensajes permitirá, mediante el uso del apartado de "flujos de correo", realizar búsquedas precisas sobre los buzones de usuario. Estas búsquedas permitirán identificar, entre otros, tanto comportamientos anómalos como el origen de posibles ataques de phising.

| Paso | Descripción |
|---|---|
| 66. | Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.<br>  |
| 67. | Dentro de la consola de administración de Exchange, seleccione el menú "**servidores**". A continuación, seleccione "**servidores**".<br>  |
| 68. | Seleccione el servidor con el rol "**Buzón**" y a continuación pulse el botón de "**Modificar**" para dicho servidor.<br>  |

| Paso | Descripción |
|---|---|
| 69. | En la sección "**Registros de transporte**" puede modificar la configuración de almacenamiento de cada uno de los registros, así como habilitar y deshabilitar el "**Registro de seguimiento de mensajes**" y el "**Registro de conectividad**", tal y como se muestra a continuación. Pulse "**Guardar**" para finalizar.<br>  |
| 70. | El registro de seguimiento de mensajes puede ejecutarlo desde la propia consola Web de administración de Exchange Server 2019. Para ello, pulse sobre "**flujo de correo**" y posteriormente en "**informes de entrega**".<br>  |

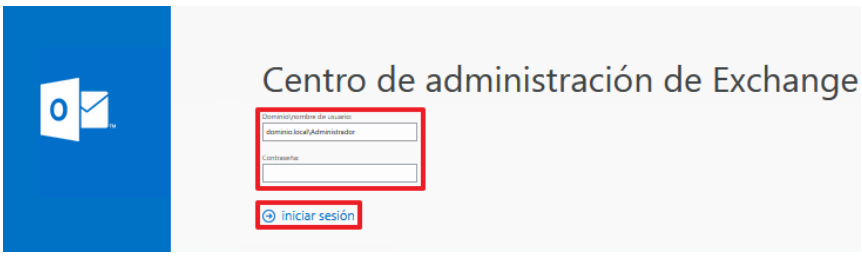
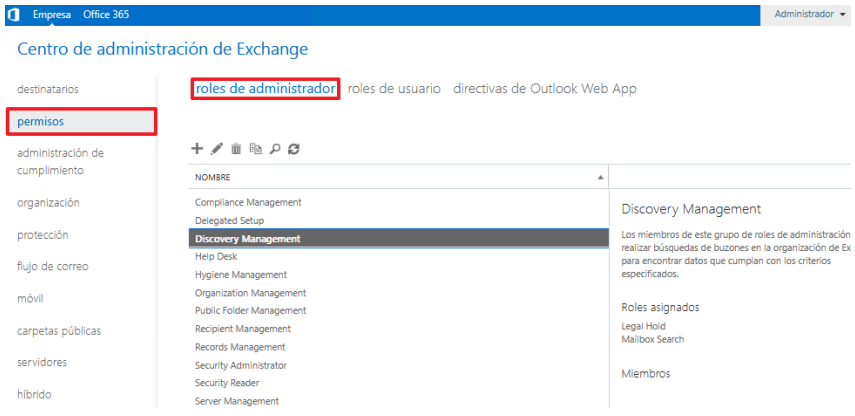
| Paso | Descripción |
|---|---|
| 71. | Puede seleccionar el buzón en el que se desea buscar un mensaje, así como el remitente y/o el destinatario. Con la finalidad de reducir el número de resultados, se pueden escribir palabras clave en la línea de asunto (recuerde que esta funcionalidad sólo permite buscar por el asunto del mensaje y no su contenido). Puede ver más detalles pulsando dos veces sobre el mensaje.<br>  |
| 72. | Es posible que necesite enviar el informe de seguimiento al usuario afectado. Para ello, pulse sobre el botón de envío y se generará un mensaje con un enlace para que el propio usuario lo pueda visualizar.<br>  |

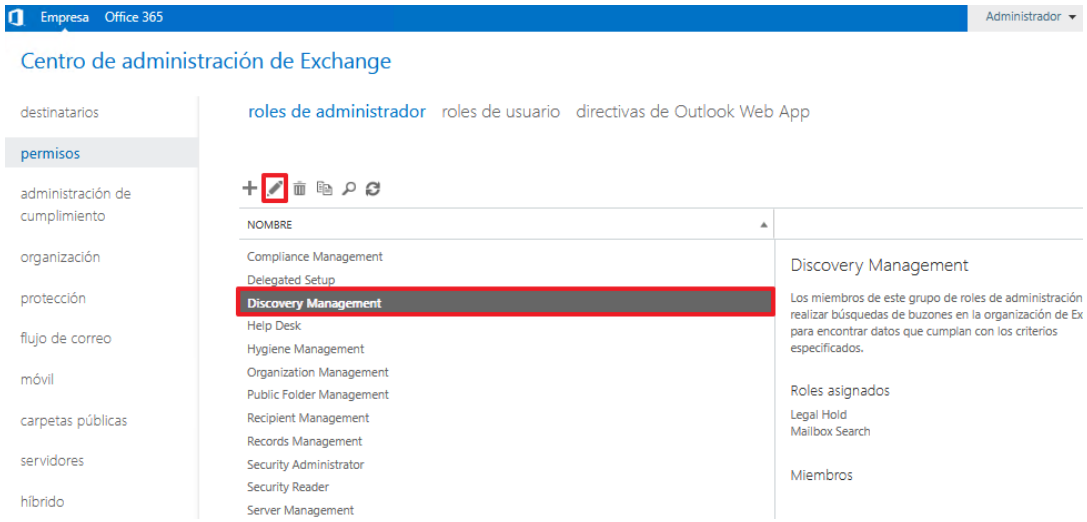
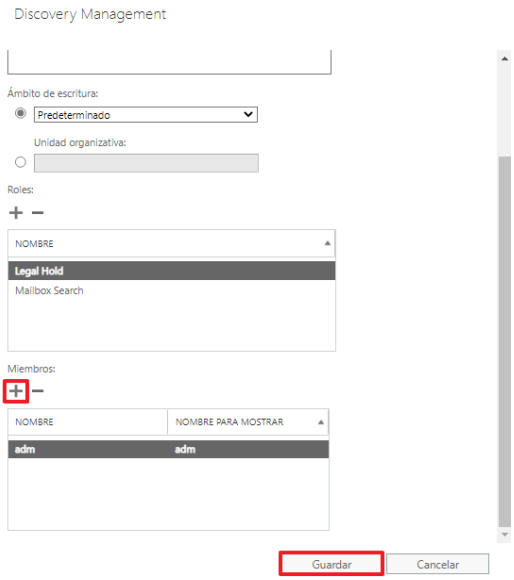
| Paso | Descripción |
|---|---|
| 73. | Especifique el destinatario y pulse sobre el botón "**Enviar**" para enviar el informe de entrega.<br>  |

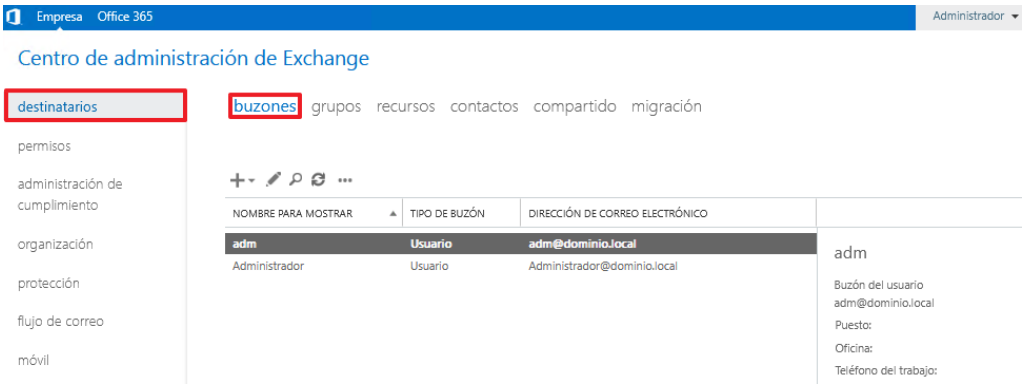
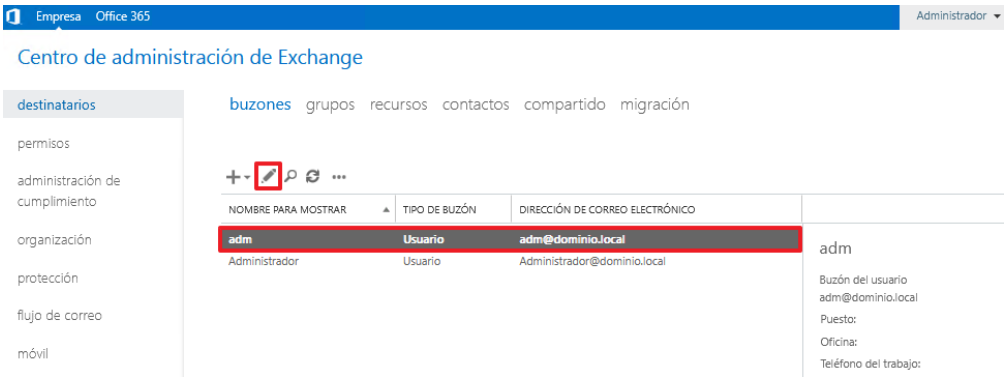
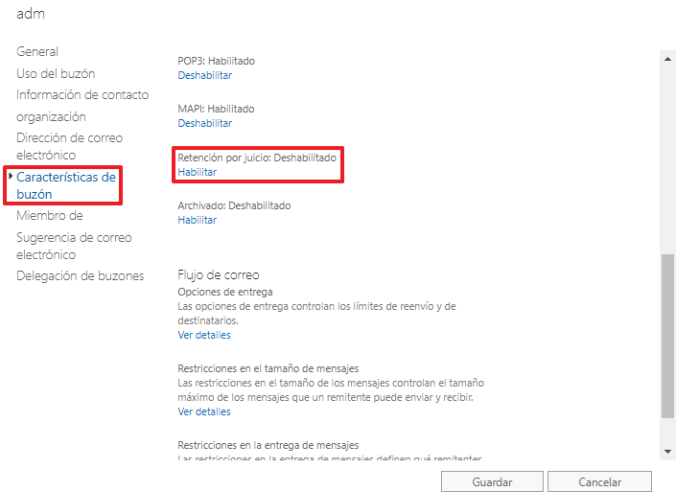
## ANEXO A.3.5. REGISTRO DE LA GESTION DE INCIDENTES

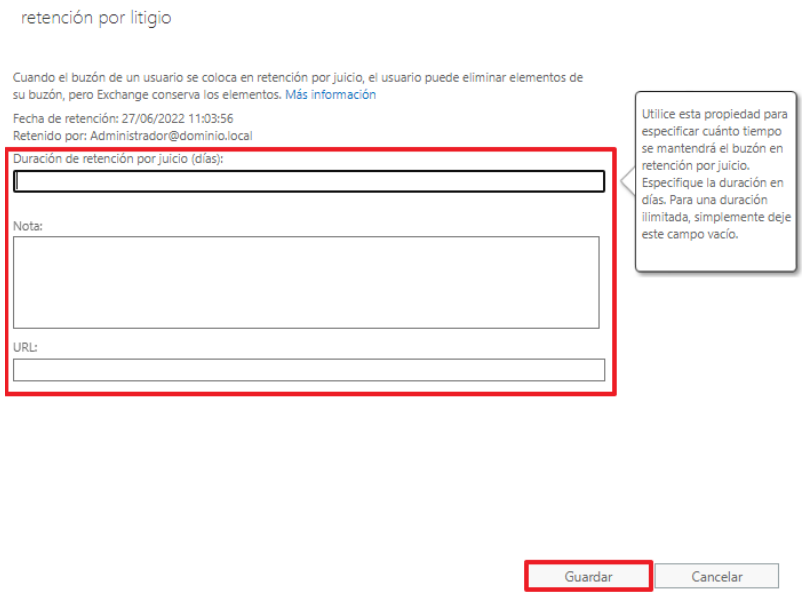
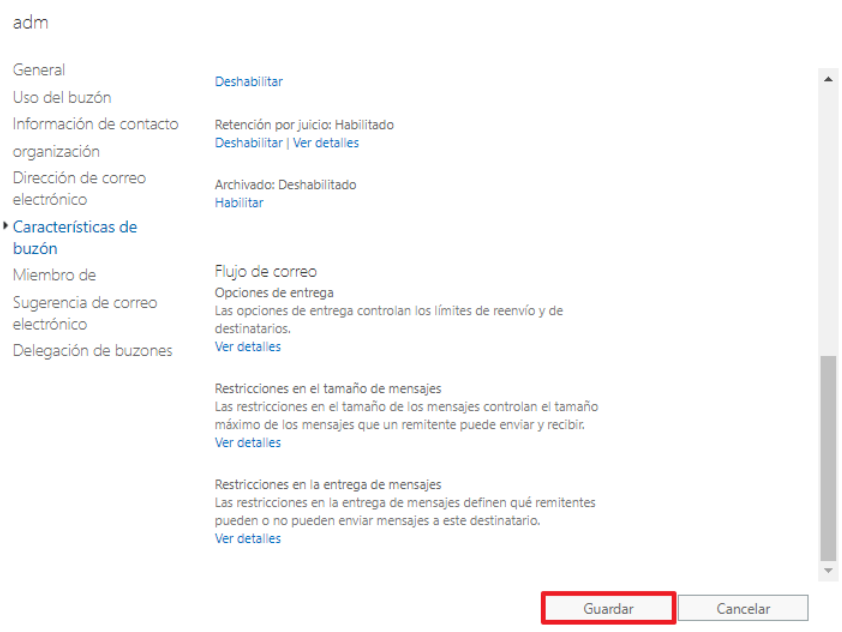
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

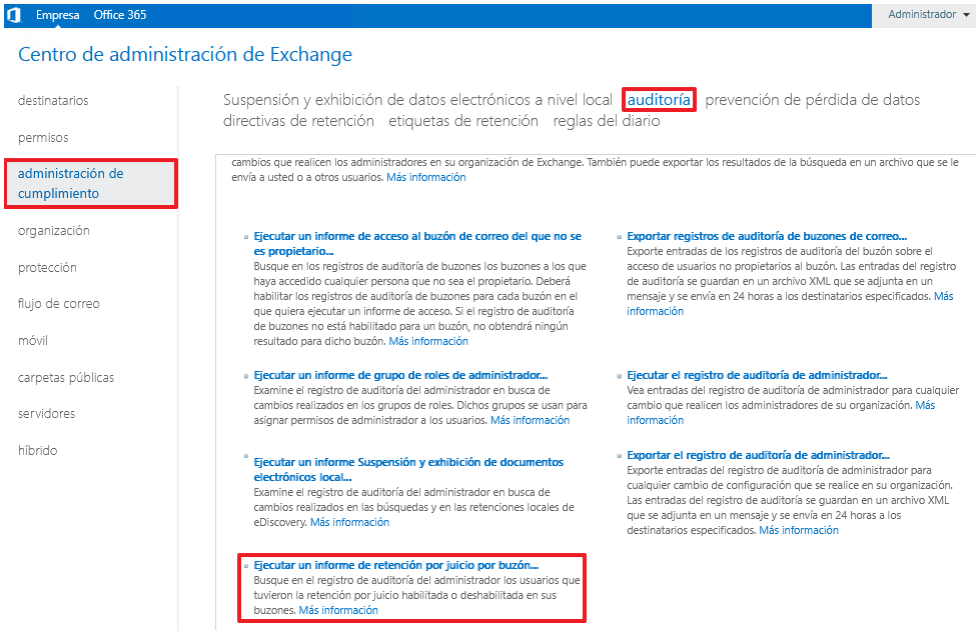
a) **[A.3.SEC-EX4]** Se auditan la administración de cuentas. De esta manera se tiene trazabilidad a la hora de gestionar cualquier tipo de incidencia.

| Paso | Descripción |
|---|---|
| 74. | Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.<br>  |
| 75. | Seleccione "**permisos**" y a continuación sitúese en "**roles de administrador**".<br>  |

| Paso | Descripción |
|---|---|
| 76. | A continuación, seleccione el grupo de roles "**Discovery Management**" y pulse "**Editar**".<br>  |
| 77. | En la sección "**Miembros**", pulse sobre el botón "**+**" para agregar las cuentas de los usuarios a los cuales se les quiere otorgar este grupo de roles, para finalizar pulse sobre "**Guardar**".<br>  <br>**Nota:** En este ejemplo se agrega la cuenta dominio.local\adm creada previamente, debe adaptar estos pasos a su organización. Además, cabe señalar que los administradores de la organización Exchange, de forma predeterminada, no disponen de los permisos para realizar búsquedas en los buzones de tipo suspensión y exhibición de datos electrónicos, aunque sí disponen del permiso para establecer un buzón en modo de retención legal. |

| Paso | Descripción |
|---|---|
| 78. | A continuación, para habilitar la retención por juicio en un buzón de usuario, diríjase a la sección "**destinatarios → buzones**".<br>  |
| 79. | Seleccione el buzón de usuario en el cual desea habilitar la retención por juicio y pulse sobre "**Modificar**".<br>  <br>**Nota:** En este ejemplo se activará la retención por juicio al "adm". |
| 80. | En la sección "**Características de buzón**", pulse sobre el botón "**Habilitar**" en "**Retención por juicio**" para activar la retención por juicio sobre el buzón de usuario previamente seleccionado.<br>  |

| Paso | Descripción |
|---|---|
| 81. | A continuación, complete la siguiente ventana adecuándola a las necesidades de su organización y pulse sobre "**Guardar**".<br>  |
| 82. | Una vez finalizada la configuración pulse sobre "**Guardar**" para cerrar la ventana.<br>  |

| Paso | Descripción |
|---|---|
| 83. | Una vez habilitada la retención legal en los buzones correspondientes, es posible obtener un informe sobre los elementos que han sido modificados o eliminados desde el menú "**Administración del cumplimiento → Auditoría → Ejecutar un informe de retención por juicio de buzón**" en la consola Web de administración de Exchange Server 2019.   |

PUBLICACIONES DE DEFENSA

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