

Guía de Seguridad de las TIC CCN-STIC 885B

Guía de configuración segura para SharePoint Online



JUNIO 2024





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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-248-9

Fecha de Edición: junio de 2024

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1. SHAREPOINT ONLINE	4
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA	4
1.2 DEFINICIÓN DEL SERVICIO.....	4
1.3 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL	6
2. DESPLIEGUE DE SHAREPOINT ONLINE.....	6
2.1 ADMINISTRADOR – CONFIGURACIÓN INICIAL.....	6
2.2 USUARIO FINAL – PRIMEROS PASOS.....	9
2.2.1 CREAR UN SITIO.....	10
3. CONFIGURACIÓN DE SHAREPOINT ONLINE	17
3.1 MARCO OPERACIONAL.....	17
3.1.1 CONTROL DE ACCESO	17
3.1.2 EXPLOTACIÓN	27
3.1.3 MONITORIZACIÓN DEL SISTEMA.....	29
3.2 MEDIDAS DE PROTECCIÓN.....	29
3.2.1 PROTECCIÓN DE LAS COMUNICACIONES.....	29
3.2.2 PROTECCIÓN DE LA INFORMACIÓN	30
3.2.3 PROTECCIÓN DE LOS SERVICIOS	37
4. SCRIPTS DE CONFIGURACIÓN	38
5. OTRAS CONSIDERACIONES DE SEGURIDAD	39
5.1 CONTROL DE VERSIONES	39
5.2 PAPELERA DE RECICLAJE	41
5.3 DIRECTIVAS DE USO COMPARTIDO.....	43
5.4 BLOQUEAR LA INTEGRACIÓN CON YAMMER	45
6. GLOSARIO Y ABREVIATURAS	46
7. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD	47

1. SHAREPOINT ONLINE

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es indicar los pasos a seguir para la configuración del servicio *SharePoint Online* cumpliendo con los requisitos necesarios del *Esquema Nacional de Seguridad* en su categoría ALTA.

Esta guía debe usarse en conjunto con “CCN-STIC-885A - Guía de configuración segura para Office 365”, donde se describen generalidades de Microsoft 365 y características comunes a todos los servicios, así como un *glosario* con los términos y abreviaturas de seguridad utilizadas en estas guías.

Para la confección de esta guía se han consultado las siguientes fuentes:

- Documentación oficial de Microsoft.
- CCN-STIC-823 Servicios en la Nube.
- CCN-STIC-884A - Guía de configuración segura para Azure.
- CCN-STIC-885A - Guía de configuración segura para Office 365.
- ENS Real Decreto BOE-A-2022-7191.

1.2 DEFINICIÓN DEL SERVICIO

SharePoint Online (SPO) es un servicio basado en la nube que ayuda a las organizaciones a compartir y administrar contenidos, conocimiento y aplicaciones para habilitar el trabajo en equipo y buscar información de manera eficaz. Se encuentra enmarcado dentro de *Microsoft 365*, conjunto de aplicaciones y servicios basados en la nube alojados en servidores propiedad de Microsoft y disponibles desde dispositivos con conexión a Internet. Hay que destacar también que Microsoft 365 funciona sobre *Microsoft Azure*.

Las principales características de *SharePoint Online* son:

- *Compartición sencilla y colaboración continua.*
Proporcionar a los contactos un lugar donde organizarse y colaborar en el contenido, los datos y noticias para que estén en sintonía.
- *Informar y poner en contacto a la organización.*
Compartir recursos y aplicaciones comunes y difundir mensajes con páginas dinámicas y enriquecidas.
- *Inteligencia.*
Búsqueda empresarial potente de archivos, sitios y contactos.

SharePoint Online incluye:

	<i>Almacenamiento de archivos</i>	OneDrive proporciona espacio de almacenamiento personal en la nube.
	<i>Uso compartido externo</i>	Compartir archivos y contenido de forma segura con los contactos de dentro y fuera de la organización.
	<i>Administración de contenido</i>	Organizar y administrar contenido en bibliotecas y listas con metadatos, administración de registros y directivas de retención.
	<i>Sitios de grupo</i>	Proporcionar un lugar para que el equipo se organice y colabore en el contenido, los datos y noticias para que estén en sintonía.
	<i>Sitios de comunicación</i>	Difundir mensajes de un grupo y compartirlo con los miembros de la organización con sitios de comunicación atractivos y dinámicos.
	<i>Intranets</i>	Informar e involucrar a la organización con intranets y sitios para dotar de contenidos, anunciar las novedades, compartir recursos, simplificar los procesos e involucrar a los contactos.
	<i>Aplicaciones móviles</i>	Obtener acceso a las intranets, sitios de grupo y contenido con la aplicación móvil de SharePoint para Android™, iOS®, y Windows y las aplicaciones móviles de OneDrive para Android, iOS y Windows.
	<i>Automatizar el trabajo</i>	Automatizar los procesos empresariales con alertas y flujos de trabajo.
	<i>Detección</i>	Descubrir los contactos relevantes y el contenido importante cuando más se necesite.
	<i>Búsqueda</i>	Personalización de la búsqueda empresarial y los resultados con características mejoradas para que aparezcan los recursos en Microsoft 365.
	<i>eDiscovery</i>	Buscar contenido en formato electrónico para escenarios de retención o auditoría.
	<i>Funcionalidades DLP</i>	Usar las funcionalidades de prevención de pérdida de datos (DLP) avanzadas para identificar, supervisar y proteger la información sensible.
	<i>Conservación local</i>	Usar la conservación local para prevenir la eliminación o edición de contenido mediante programación.

1.3 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL

PowerShell de Microsoft 365 permite gestionar y configurar SharePoint Online desde la línea de comandos, con un usuario con derechos de administración. Consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]

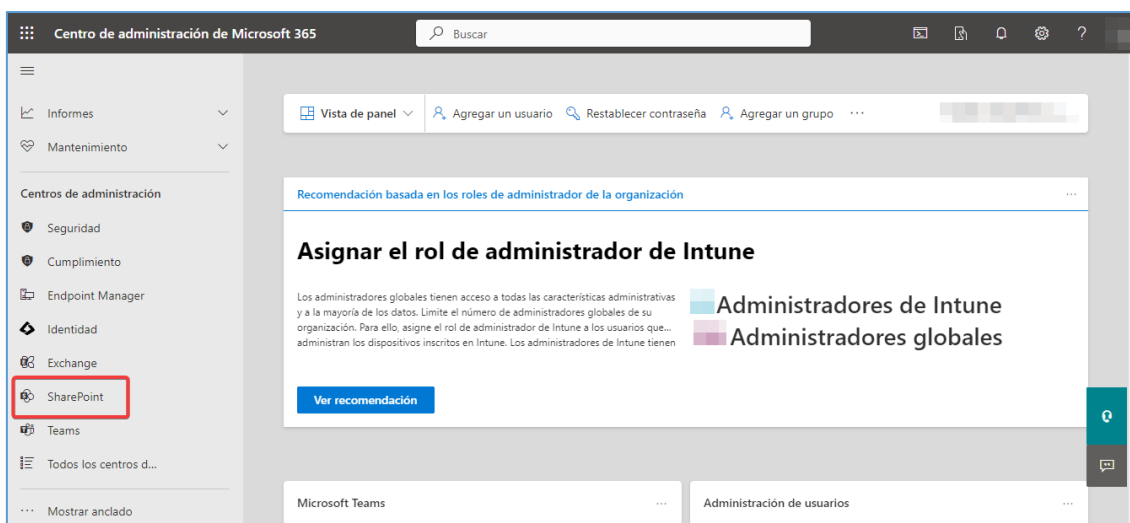
2. DESPLIEGUE DE SHAREPOINT ONLINE

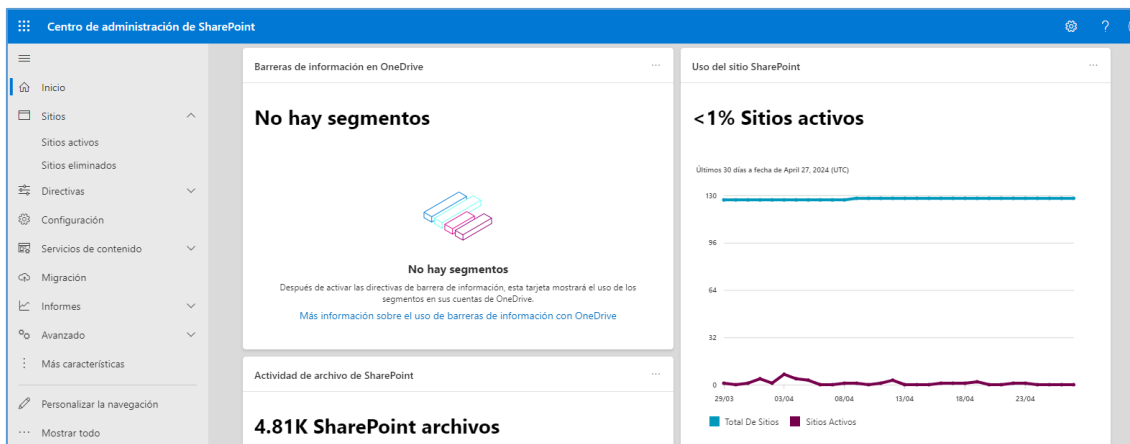
SharePoint Online no necesita instalación previa en el entorno on-premise del cliente, ya que es un servicio on-line accesible desde Internet y alojado en el tenant de Microsoft 365 de la organización. Utiliza la infraestructura de “Nube pública” referida en la guía [823-Cloud Computing].

SharePoint Online, así como el conjunto de Microsoft 365, se encuentra englobado en la categoría de servicio **SaaS** (Software as a Service). El CSP (Microsoft) es el encargado de ofrecer al cliente el software como un servicio.

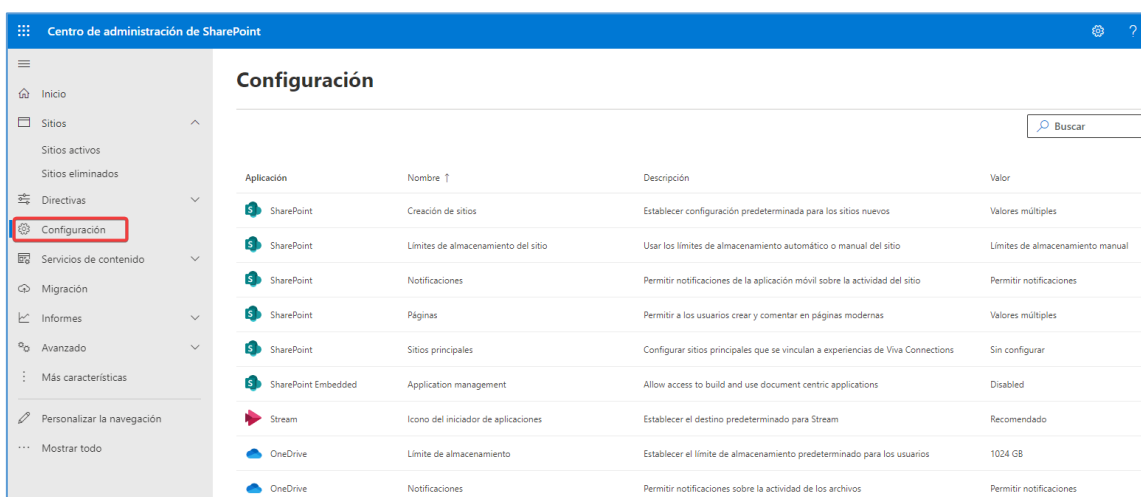
2.1 ADMINISTRADOR – CONFIGURACIÓN INICIAL

El usuario *administrador* podrá acceder al portal de administración de SharePoint Online a través del portal de administración de Microsoft 365 (<https://admin.microsoft.com>).





En el menú [Configuración] se puede controlar qué características están disponibles para los usuarios de la organización tanto a nivel de OneDrive, Stream y SharePoint.



Aplicación	Nombre ↑	Descripción	Valor
SharePoint	Creación de sitios	Establecer configuración predeterminada para los sitios nuevos	Valores múltiples
SharePoint	Límites de almacenamiento del sitio	Usar los límites de almacenamiento automático o manual del sitio	Límites de almacenamiento manual
SharePoint	Notificaciones	Permitir notificaciones de la aplicación móvil sobre la actividad del sitio	Permitir notificaciones
SharePoint	Páginas	Permitir a los usuarios crear y comentar en páginas modernas	Valores múltiples
SharePoint	Sitios principales	Configurar sitios principales que se vinculan a experiencias de Viva Connections	Sin configurar
SharePoint Embedded	Application management	Allow access to build and use document centric applications	Disabled
Stream	Icono del iniciador de aplicaciones	Establecer el destino predeterminado para Stream	Recomendado
OneDrive	Límite de almacenamiento	Establecer el límite de almacenamiento predeterminado para los usuarios	1024 GB
OneDrive	Notificaciones	Permitir notificaciones sobre la actividad de los archivos	Permitir notificaciones

Creación de sitios

Creación de sitios

Establecer configuración para los sitios nuevos.

[Más información sobre la creación de sitios](#)

☒ Los usuarios pueden crear sitios de SharePoint

Controle si los usuarios pueden crear sitios desde SharePoint, OneDrive, el cmdlet pnP de PowerShell y la API de REST. Esta configuración no impide que los usuarios puedan crear equipos o grupos de Microsoft 365 y sus sitios conectados

☒ Mostrar las opciones para crear un sitio en SharePoint y crear una biblioteca compartida desde OneDrive

Crear sitios de grupo en

Zona horaria predeterminada

Límite de almacenamiento predeterminado para sitios nuevos

Permite elegir la ubicación de los *sites* de grupo de la organización.

Configurar la zona horaria.

Activar o desactivar la creación de sitios por parte de los usuarios.

***Recomendación:** elegir la zona horaria adecuada y dejar resto de valores por defecto.

Límites de almacenamiento del sitio

Límites de almacenamiento del sitio

Comparta el almacenamiento entre todos los sitios o controle los límites de almacenamiento por sitio con facilidad.

☒ Automático

Los sitios usarán el almacenamiento que necesiten hasta un máximo de 25 TB.

☐ Manual

Establecer límites específicos para cada sitio

Guardar

Cancelar

Automático para compartir el almacenamiento entre todos los sitios.

Manual: establecer límites específicos para cada sitio.

*Recomendación: dejar valor por defecto. No afecta a la seguridad.

Notificaciones

Notificaciones

Seleccione esta opción para permitir que los usuarios de la aplicación móvil de SharePoint reciban notificaciones sobre la actividad del sitio de SharePoint. Los usuarios pueden desactivar las notificaciones si no quieren recibirlas.

[Más información sobre las notificaciones de SharePoint](#)

☒ Permitir notificaciones

Para **permitir las notificaciones en las aplicaciones móviles** relacionadas con SharePoint.

*Recomendación: dejar valor por defecto. No afecta a la seguridad.

Sincronizar

Sincronizar

Use esta configuración para controlar la sincronización de archivos en OneDrive y SharePoint.

☒ Mostrar el botón Sincronizar en el sitio web de OneDrive

☐ Permitir la sincronización solo en equipos unidos a dominios específicos

☐ Bloquear la carga de tipos de archivo específicos

Para **controlar la sincronización de archivos en OneDrive y SharePoint**.

*Recomendación: dejar valor por defecto.

Retención

Retención

Especifique el período de retención predeterminado de OneDrive de un usuario cuando se elimina el usuario. El cambio de esta configuración también afecta a las cuentas de OneDrive que ya están dentro del período de retención.

[Más información sobre cómo establecer la retención de OneDrive](#)

Días para conservar OneDrive de un usuario eliminado

Escriba un valor entre 30 y 3650 días.

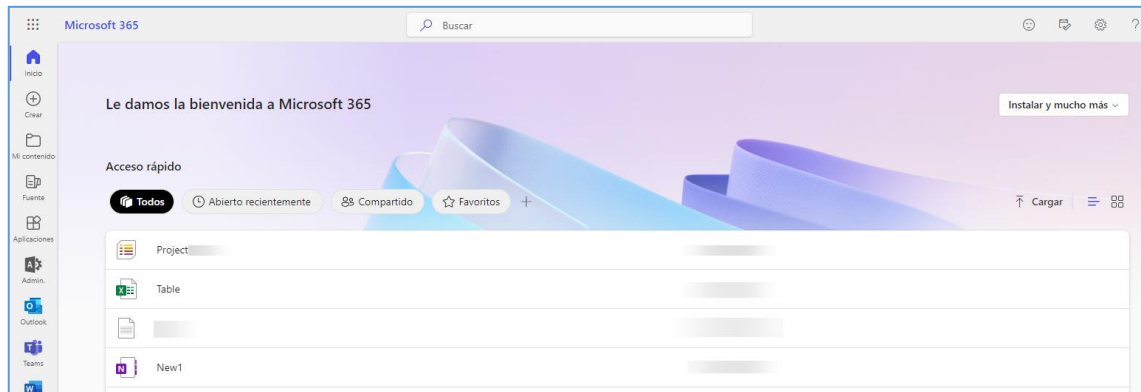
30

Para **controlar la retención predeterminada en OneDrive cuando se elimina una cuenta de usuario**.

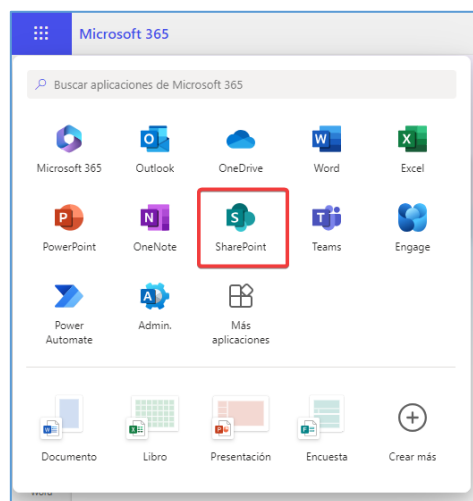
*Recomendación: dejar valor por defecto.

2.2 USUARIO FINAL – PRIMEROS PASOS

El *usuario final* podrá acceder al portal Office 365 a través de la *url*: microsoft365.com u office.com. Tras introducir las credenciales se muestra un panel con todas las aplicaciones y características a las que tiene acceso el usuario en cuestión.



Pulsando en el icono  de la parte superior izquierda de la pantalla y pulsando en el icono de SharePoint se podrá acceder al portal de SharePoint.



La pantalla de inicio de SharePoint Online se encuentra dividida en dos secciones:

- Menú lateral izquierdo. Con opciones de búsqueda, sitios que se siguen y sitios recientes.
- Panel principal. Para crear sitios y noticias y visualizar sitios frecuentes.

2.2.1 CREAR UN SITIO



Pulsando el botón “Crear sitio” del panel principal, se despliegan dos opciones:

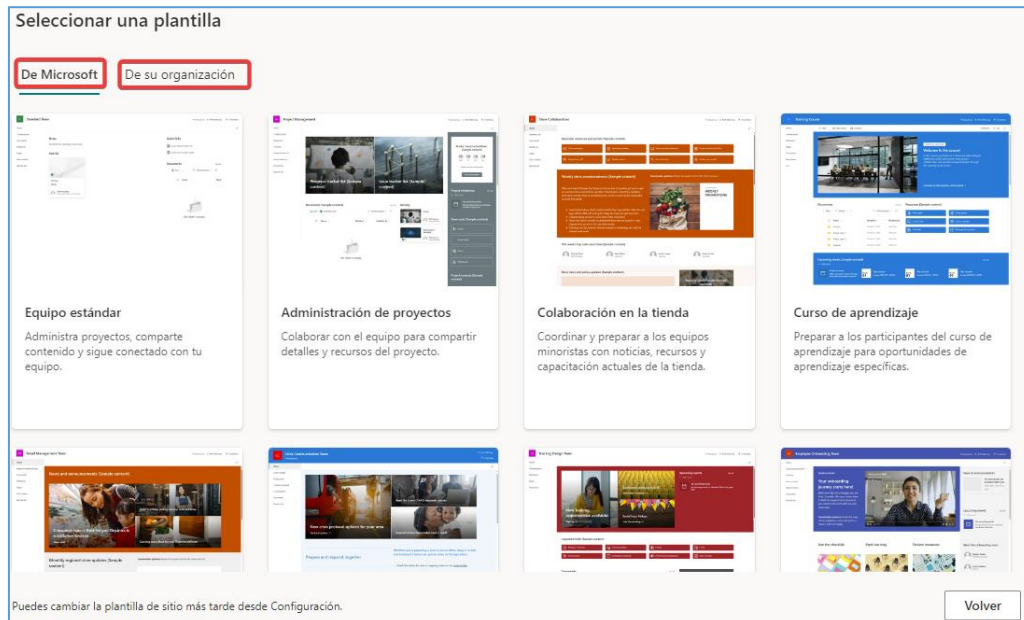
- **Sitio de comunicación:** para difundir información, compartir noticias, informes, estados, etc. a una audiencia amplia en un formato visualmente atractivo. Sólo genera contenido un pequeño conjunto de miembros y es un público mucho mayor quien lo consulta.
- **Sitio de grupo:** proporciona una ubicación concreta en la que un grupo de personas pueden trabajar en un proyecto concreto y compartir información desde cualquier lugar con cualquier dispositivo. Son grupos cerrados, la información se limita sólo a los miembros del grupo o participantes específicos.

Adicionalmente, desde el *Centro de administración de SharePoint* se muestran otras opciones desde el botón “Examinar más sitios”, donde poder crear un sitio de grupo sin un grupo de Microsoft 365, o bien un centro de documentos, una wiki empresarial, un portal de publicación, centro de contenidos y más plantillas adicionales.

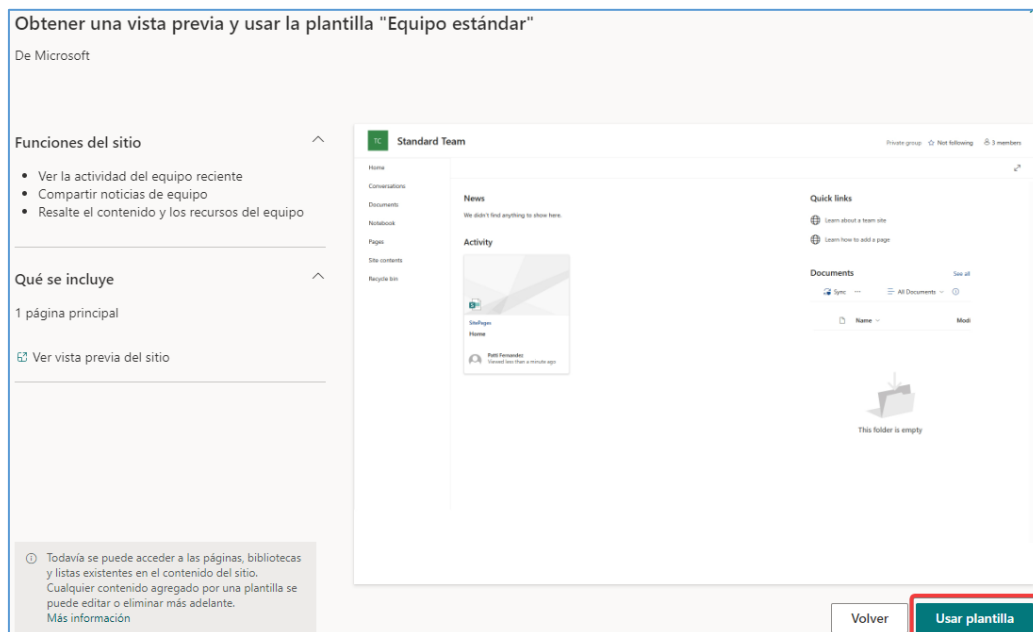


2.2.1.1 CREAR UN SITIO DE GRUPO

1. Se puede seleccionar una plantilla de las que proporciona Microsoft o una plantilla de la propia organización.



2. Las características de la plantilla seleccionada pueden ser visualizadas y proceder a pulsar sobre el botón 'Usar plantilla'.



3. Agregar nombre del sitio, descripción y propietario del grupo.

Asigne un nombre a su sitio

Decida un nombre único que siga los estándares de nomenclatura de su organización. La descripción es opcional, pero es útil para que los usuarios comprendan para qué sirve su sitio.

El sitio de grupo se conectará a un grupo de Microsoft 365, lo que proporciona a su sitio un bloc de notas de OneNote compartido, una dirección de correo electrónico de grupo y un calendario de equipo.



Equipo estándar  Cambiar plantilla

Nombre del sitio *
CCN-M365-Grupo2
El nombre del sitio está disponible.

Descripción del sitio
Informa a los usuarios del propósito de tu sitio

Dirección de correo electrónico del grupo *
CCN-M365-Grupo2
El alias de grupo está disponible.

Dirección del sitio *
https://.sharepoint.com/sites/ CCN-M365-Grupo2
La dirección del sitio está disponible.

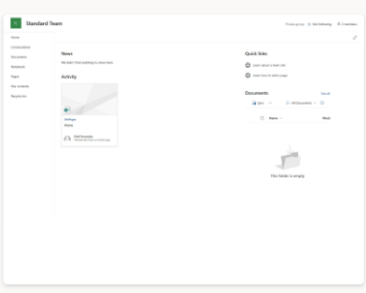
Propietario del grupo *
Comienza a escribir un nombre

Atrás 

- En este punto es donde se decide si el sitio va a ser público (accesible por cualquier persona de la organización- útil para contenido genérico) o privado (sólo los miembros pueden acceder).

Establecer idioma y otras opciones

Establece el idioma predeterminado para el sitio. Si es necesario, selecciona etiquetas y otras opciones de configuración para clasificar qué tipo de contenido se almacena en el sitio y quién puede acceder a la información.



Equipo estándar  Cambiar plantilla

Confidencialidad ⓘ
Ninguno

Configuración de privacidad
Privado: solo los miembros pueden obtener acceso a este sitio

Seleccionar un idioma
Inglés
Selecciona el idioma predeterminado del sitio. No se podrá cambiar más adelante.

Zona horaria
(UTC+01:00) Bruselas, Copenhague, Madrid, París

Límite de almacenamiento *
25600 GB

Atrás 

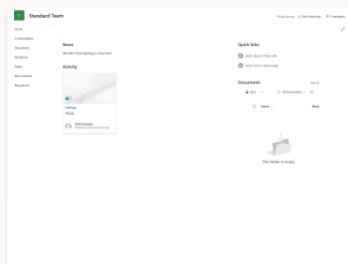
- Agregar miembros o más propietarios.

Agregar propietarios y miembros del sitio

Considere la posibilidad de asignar un propietario de sitio adicional o un grupo para ayudar a administrar el contenido del sitio. [Obtenga más información sobre los permisos.](#)

Propietarios del sitio tener control total sobre el contenido del sitio, el tema, los permisos, las asociaciones del centro y otras configuraciones del sitio.

Miembros del sitio puede editar y ver el contenido del sitio, incluidos archivos, páginas, listas y navegación.



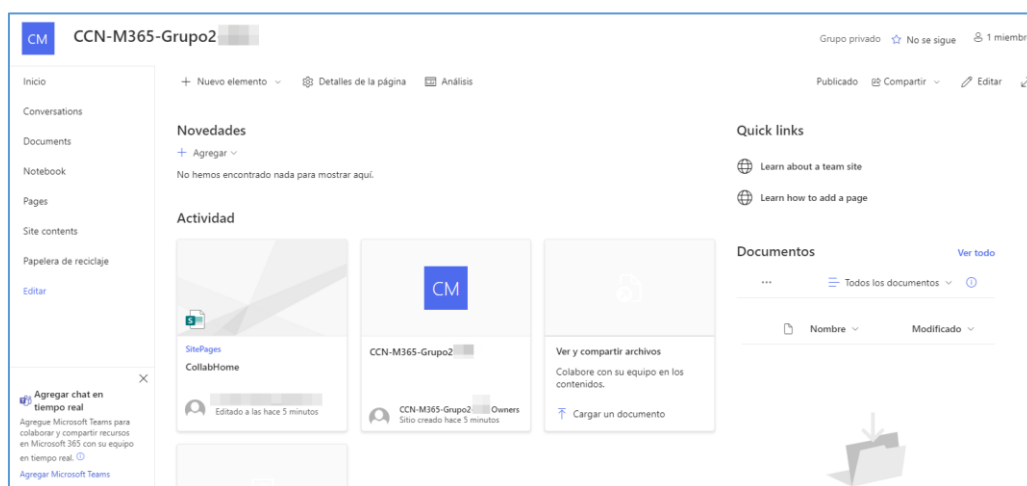
Equipo estándar

Agregar miembros

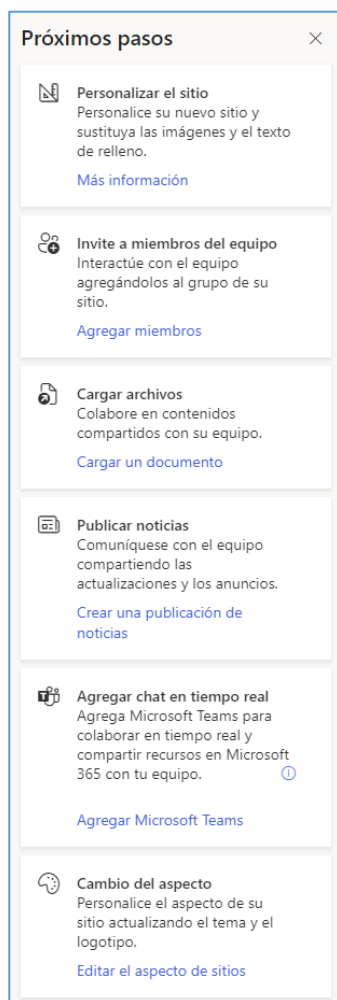
Comience a escribir un nombre

Finalizar

- Al pulsar el botón “Finalizar” se crea el sitio de grupo y se navega a la página del sitio recién creado.



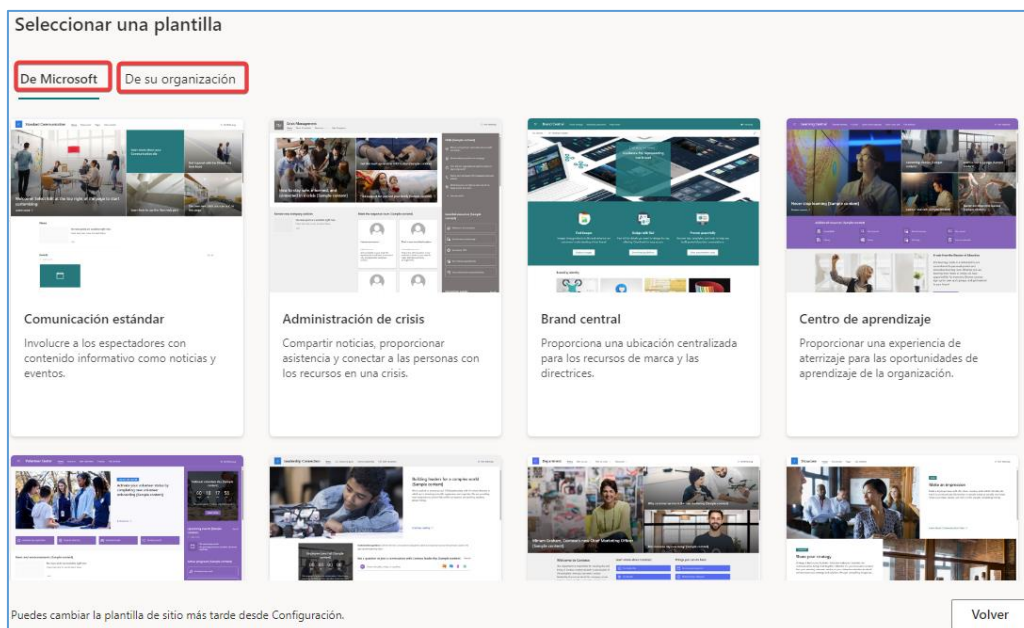
- Los siguientes pasos para el usuario podrían ser:



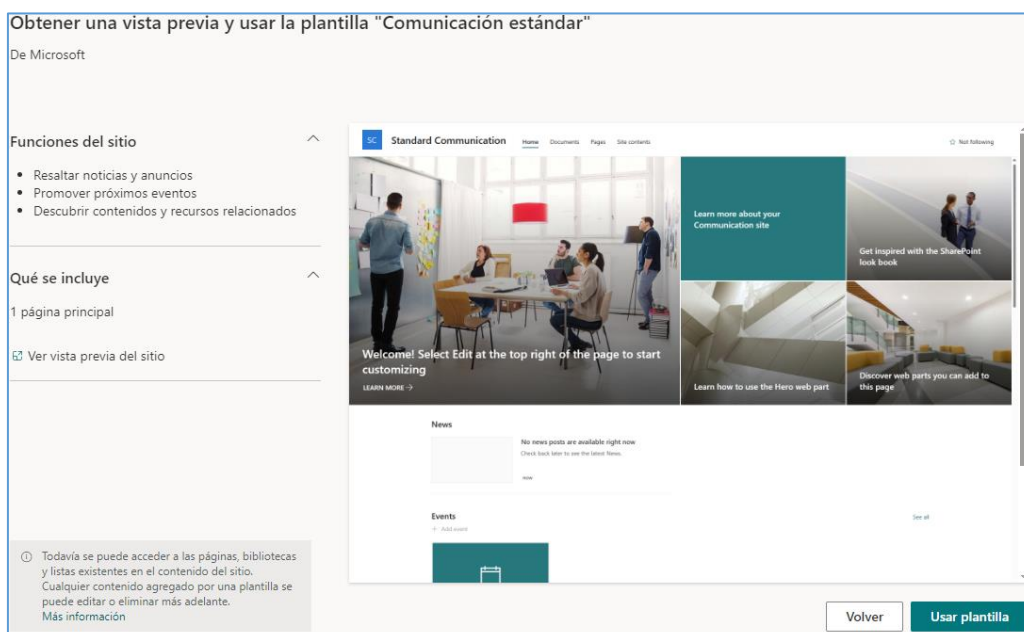
- Personalizar el sitio
- Invitar miembros
- Cargar archivos en el sitio
- Publicar noticias
- Agregar chat en Teams
- Cambiar aspecto

2.2.1.2 CREAR UN SITIO DE COMUNICACIÓN

1. Se puede seleccionar una plantilla de las que proporciona Microsoft o una plantilla de la propia organización.



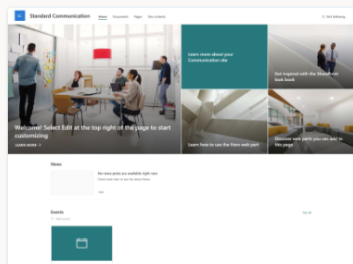
2. Las características de la plantilla seleccionada pueden ser visualizadas y proceder a pulsar sobre el botón 'Usar plantilla':



3. Agregar nombre del sitio, descripción y propietario del grupo.

Asigne un nombre a su sitio

Decida un nombre único que siga los estándares de nomenclatura de su organización. La descripción es opcional, pero es útil para que los usuarios comprendan para qué sirve su sitio.



Comunicación estándar

 Cambiar plantilla

Nombre del sitio *

CCN-SPO-COMUNICACION

El nombre del sitio está disponible.

Descripción del sitio

Sitio de comunicación CCN

Dirección del sitio *

../sites/

CCN-SPO-COMUNICACION

La dirección del sitio está disponible.

<https://plain823.sharepoint.com/sites/CCN-SPO-COMUNICACION>

Propietario del sitio *



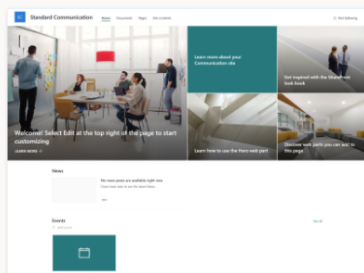
Atrás

Siguiente

4. Establecemos idioma y otras opciones.

Establecer idioma y otras opciones

Establece el idioma predeterminado para el sitio. Si es necesario, selecciona etiquetas y otras opciones de configuración para clasificar qué tipo de contenido se almacena en el sitio y quién puede acceder a la información.



Comunicación estándar

 Cambiar plantilla

Confidencialidad ⓘ

Ninguno

Seleccionar un idioma

Inglés

Selecciona el idioma predeterminado del sitio. No se podrá cambiar más adelante.

Zona horaria

(UTC+01:00) Bruselas, Copenhague, Madrid, París

Límite de almacenamiento *

25600

GB

Atrás

Crear sitio

5. Al pulsar “Crear sitio”, se crea el *sitio de comunicación*.

3. CONFIGURACIÓN DE SHAREPOINT ONLINE

A continuación, se abordará la configuración del servicio SharePoint Online centrándose en el cumplimiento de los requisitos del Esquema Nacional de Seguridad (ENS) establecidas en el BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo que aplican exclusivamente a este servicio:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

3.1 MARCO OPERACIONAL

3.1.1 CONTROL DE ACCESO

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

Microsoft Entra ID es la herramienta principal para la gestión de accesos y privilegios sobre los recursos de Azure dentro de una organización. Al ser **SharePoint Online** un recurso de Azure, el proveedor de identidad será **Microsoft Entra ID**.

Si bien esta guía trata únicamente la gestión de cuentas de usuarios en nube Microsoft Entra ID, también permite configuraciones híbridas. Se puede consultar la documentación de identidades híbridas en el enlace:

<https://docs.microsoft.com/es-es/azure/active-directory/hybrid/index>

Para cumplir con los requisitos exigidos dentro del ámbito del ENS, se recomienda consultar la guía [CCN-STIC-884A Guía de Configuración segura para Azure].

3.1.1.1 IDENTIFICACIÓN

La gestión de identidades de SharePoint Online es común a todas las aplicaciones de la solución Microsoft 365 y se describe en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

3.1.1.2 REQUISITOS DE ACCESO

SharePoint Online establece un conjunto de *niveles de permisos* para proteger el acceso a los recursos.

El modelo de objetos en SharePoint Online

SharePoint proporciona distintas alternativas para controlar el acceso a los objetos:

- Los objetos pueden usar, bien los mismos permisos que el sitio web, la lista o la carpeta primarios al heredar tanto los roles como los usuarios disponibles en el objeto primario, o bien permisos únicos.

- SharePoint incluye los cuatro grupos siguientes de forma predeterminada, con un nivel de permisos asociado:
 - **Administradores:** Tienen los mismos permisos de Control total que el propietario de un sitio, y pueden realizar acciones como administrar la búsqueda, la papelera de reciclaje y las características de la colección de sitios. También tienen acceso a todos los elementos del sitio, incluidos los subsitios, aún si se ha roto la herencia de permisos.
 - **Propietarios:** Tienen un control total del sitio de SharePoint. Si el sitio tiene un grupo o equipo de Microsoft 365 asociado, los propietarios del grupo o del equipo se incluyen automáticamente como propietarios del sitio.
 - **Miembros:** Tienen permisos de edición para el sitio de SharePoint y pueden agregar y quitar archivos, listas y bibliotecas. Si el sitio tiene un grupo o equipo de Microsoft 365 asociado, los miembros del grupo o del equipo se incluyen automáticamente como miembros del sitio.
 - **Visitantes:** Tienen permisos de solo vista para el sitio de SharePoint. Este nivel de permisos solo se usa en SharePoint y no está relacionado con los permisos de un grupo o equipo de Microsoft 365 asociado.

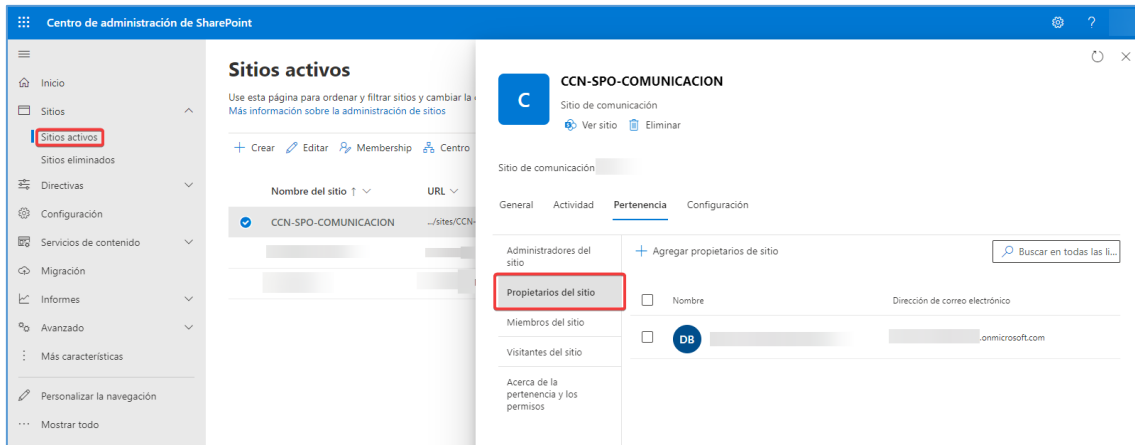
Estos grupos son independientes de los grupos de Microsoft 365 y Microsoft Entra ID (anteriormente conocido como Azure Active Directory) y constituyen la base para asignar permisos a los recursos del sitio.

Cuando se crea un sitio web con permisos únicos (no heredados del sitio *padre*) con la interfaz de usuario, se navega a una página donde puede asignar usuarios a estos grupos como parte del aprovisionamiento del sitio. Ver apartado [2.2 Usuario final - primeros pasos] y [3.1.1.4 Proceso de gestión de derechos de acceso].

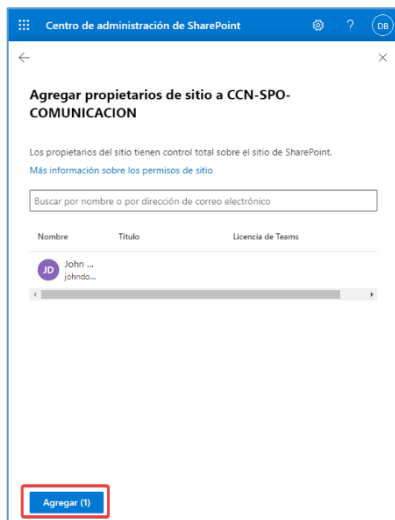
Agregar un nuevo propietario a un sitio de grupo desde el Centro de administración de SharePoint

Como administrador de SharePoint es posible asignar nuevos *propietarios (owners)* a un sitio. Esta opción es interesante si se desea compartir tareas de administración.

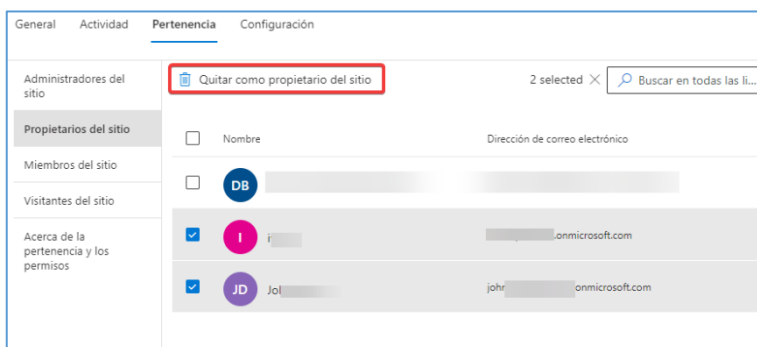
1. Desde el *Centro de administración de SharePoint*, menú [Sitios\Sitios activos] y accediendo a las propiedades del sitio seleccionado. Pulsar sobre la pestaña “Pertenencia” y después sobre “Propietarios del sitio”:



2. Pulsar sobre “Agregar propietarios de sitio”.



Para agregar un nuevo propietario basta con escribir el nombre o la dirección de correo electrónico y pulsar sobre el botón “Agregar”.



Para eliminar un propietario seleccionar al usuario o usuarios y pulsar sobre el botón “Quitar como propietario del sitio”.

Siempre debe existir al menos un propietario del sitio. Al agregar o quitar usuarios de un sitio de grupo, se agregan o eliminan también del grupo de Microsoft 365, Exchange Online, Teams, etc.

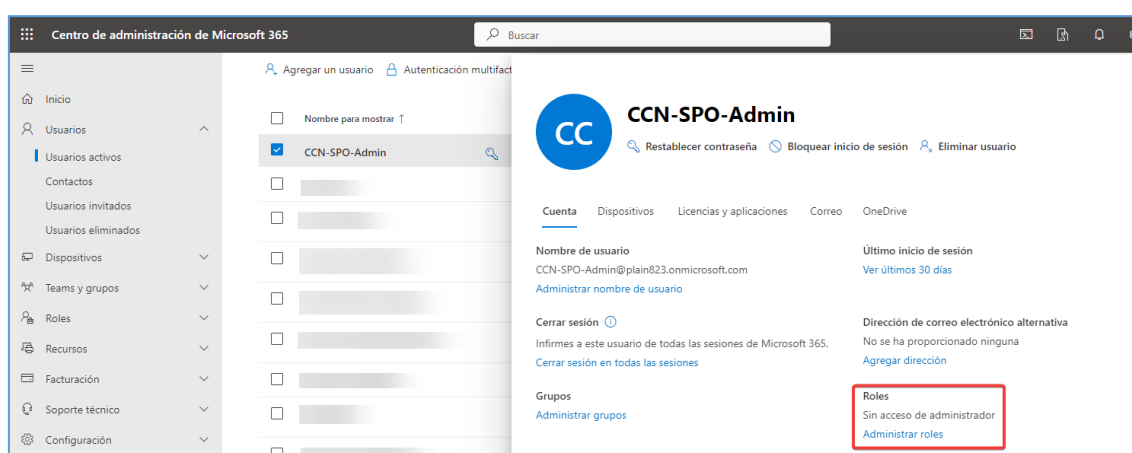
Para **proporcionar o restringir el acceso** de los usuarios a un sitio SharePoint consultar el apartado [3.1.1.4 Proceso de gestión de derechos de acceso].

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Rol de administrador

Los administradores globales de Microsoft 365 pueden asignar usuarios al **rol de administrador de SharePoint** para ayudarle con la administración de SharePoint Online. Se recomienda establecer un administrador para cada servicio de la solución de Microsoft 365. En aquellas organizaciones donde exista una delegación de tareas de administración se requiere establecer un administrador por cada servicio delegado.

1. Abrir el *Centro de administración de Microsoft 365*, menú [Usuarios\Usuarios activos], y pulsar sobre el nombre del usuario. En la ventana emergente, pulsar sobre el enlace “Administrar roles”.



2. Pulsar sobre el nombre del usuario y, en el panel derecho de propiedades, pulsar el enlace “Administrar roles”:

Administrar roles de administrador

CCN-SPO-Admin seleccionado

Los roles de administrador ofrecen permiso a los usuarios para ver los datos y completar las tareas en los centros de administración. Asigne el rol menos permisivo para que los usuarios solo tengan el acceso que necesitan.

[Más información sobre roles de administración](#)

☐ Usuario (sin acceso al centro de administración)

☒ Acceso al centro de administración

Los lectores globales tienen acceso de solo lectura en los centros de administración, mientras que los administradores globales tienen acceso ilimitado para editar toda la configuración. Los usuarios que tienen asignados otros roles están más limitados en lo que pueden ver y hacer.

☐ Administrador de Exchange ⓘ

☒ Administrador de SharePoint ⓘ

☐ Administrador de Teams ⓘ

☐ Administrador de soporte técnico de servicio ⓘ

☐ Administrador de usuarios ⓘ

Guardar cambios

Puede ser interesante asociar, junto con el rol de administrador de SharePoint, la función de **administrador de soporte técnico de servicio**. De esta forma, puede ver información relacionada con el servicio en el *Centro de administración de Microsoft 365*: crear y administrar solicitudes de soporte técnico con Microsoft relativas a servicios de Azure y Microsoft 365, consultar el centro de mensajes y el panel de servicios de Azure Portal y el Centro de administración de Microsoft 365.

Los usuarios a los que se ha asignado el rol de administrador de SharePoint tienen

acceso al centro de administración de SharePoint y pueden crear y administrar colecciones de sitios, designar administradores de colecciones de sitios, administrar perfiles de usuario, la configuración global de SharePoint y mucho más.

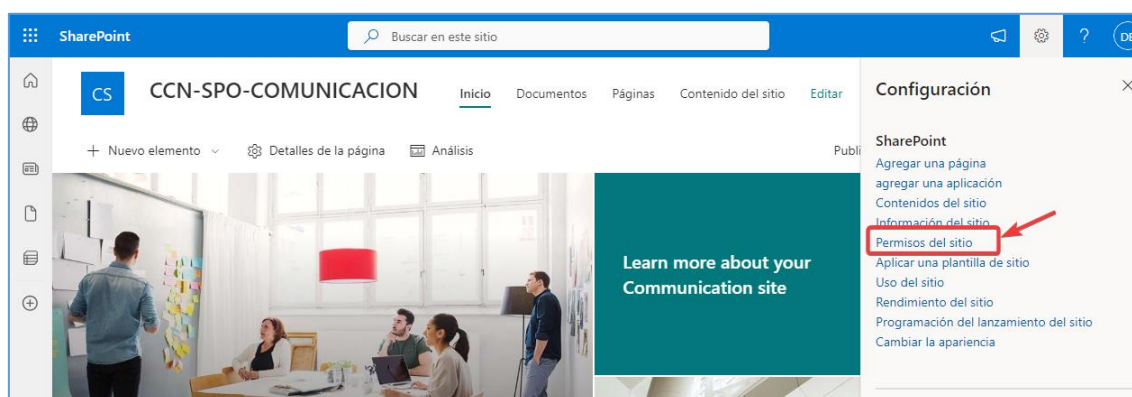
Más información sobre roles en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

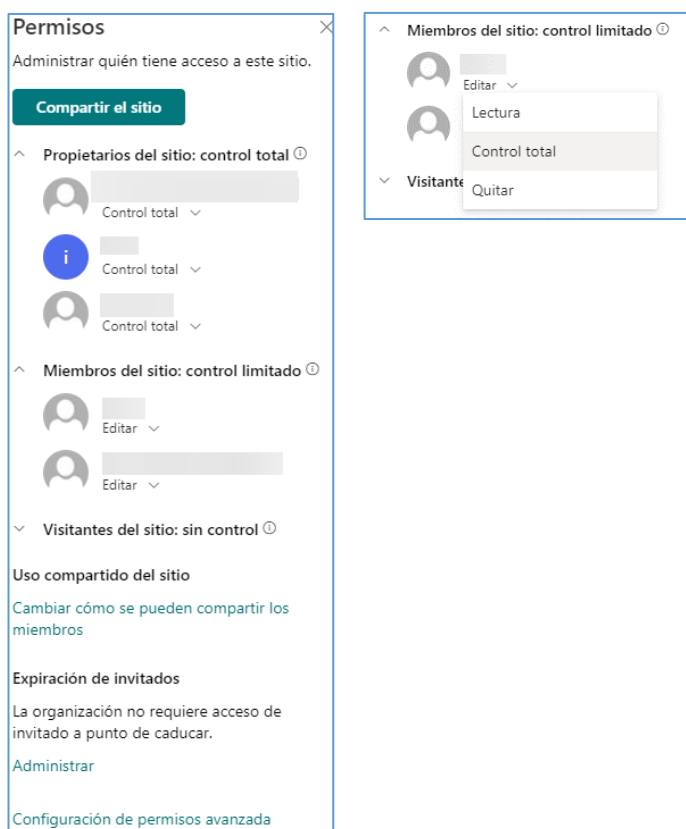
Configurar permisos del sitio por un propietario

Después de crear un sitio de SharePoint, **se debe proporcionar o restringir el acceso** de los usuarios al sitio o a su contenido. Por ejemplo, puede proporcionarse acceso solo a los miembros de un equipo, o bien a todos los usuarios, pero restringir la edición para algunos. La manera más sencilla de trabajar con permisos es usar los niveles de permisos y grupos predeterminados ofrecidos, que abarcan los escenarios más comunes.

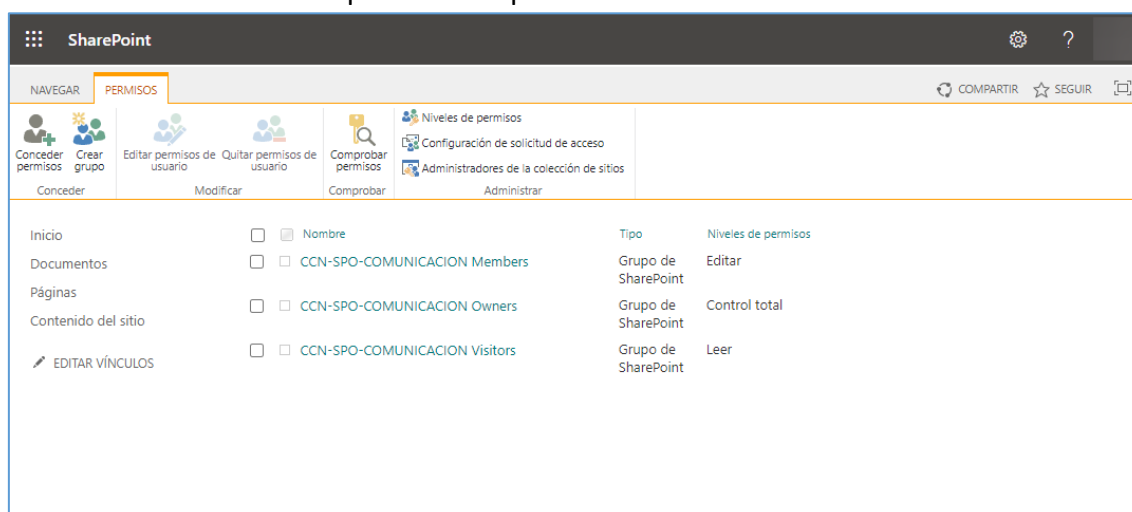
1. Desde el menú de configuración del sitio del portal de usuario de SharePoint, en la esquina superior derecha, se accede a los permisos del sitio [Configuración\Permisos del sitio]:



2. Desde aquí, un propietario puede invitar a nuevas personas y gestionar su nivel de permisos: propietarios del sitio (control total del contenido del sitio), miembros del sitio (control limitado, puede editar y ver el contenido del sitio), visitante (sin control, puede ver el contenido del sitio).



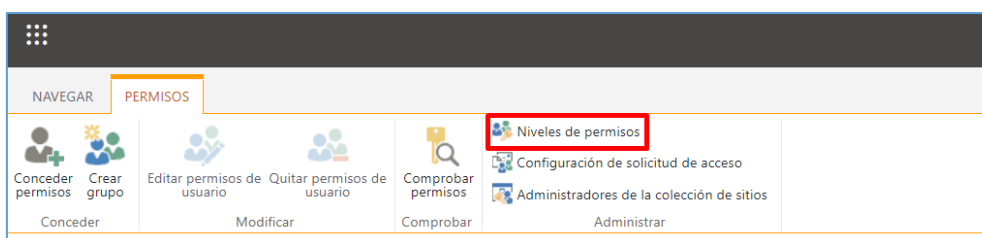
3. Pinchar sobre el enlace “Configuración de permisos avanzada”, para un control más exhaustivo de los permisos a aplicar.



4. Pulsando sobre cada uno de los grupos de SharePoint se accede a una gestión detallada, donde es posible añadir nuevos usuarios al grupo y administrar otras opciones de configuración.



Niveles de permisos



Dentro de la “Configuración de permisos avanzada”, en la pestaña “PERMISOS”, pulsar el vínculo “Niveles de Permisos”.



Un **nivel de permisos** es un conjunto de *permisos*. En este sentido, SharePoint cuenta con *niveles de permisos predeterminados* que permiten proporcionar de forma rápida y sencilla niveles de permisos comunes para un usuario o grupos de usuarios.

Se puede realizar cambios en cualquiera de los niveles de permisos predeterminados, excepto *Control total* y *Acceso limitado*.

Puede resultar conveniente establecer *niveles de permisos personalizados* para crear nuevos roles y adaptarlos a las necesidades de cada organización. Por ejemplo, un usuario con permisos para agregar documentos pero no eliminarlos.

1. Pulsar el enlace “Agregar un nivel de permisos”.

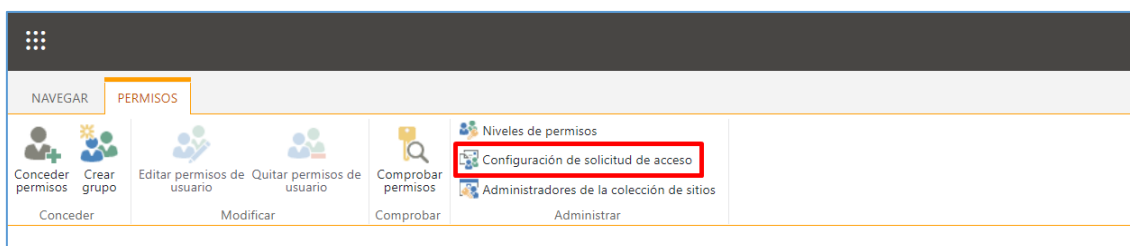


2. Asignar nombre y descripción, y la lista de permisos adecuada.

Configuración de solicitud de acceso

Es recomendable indicar cómo se configura el comportamiento para solicitar acceso a un sitio. Desde el punto de vista de la seguridad, se puede bloquear el que un usuario comparta el sitio o contenidos con otros usuarios o enviar invitaciones al grupo miembros del sitio. Estos detalles son importantes para evitar fuga de información sin control. Esta configuración es independiente del “Directivas de uso compartido”, indicado en el punto 5.3.

Dentro de la “Configuración de permisos avanzada”, en la pestaña “PERMISOS”, pulsar el vínculo “Configuración de solicitud de acceso”.



Desde esta pantalla se elige quién puede solicitar acceso o invitar a otros a este sitio.

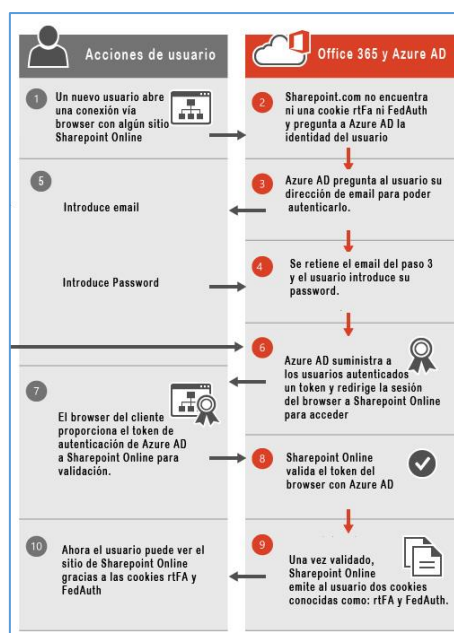
3.1.1.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS)

Los mecanismos de autenticación de SharePoint Online son comunes a todas las aplicaciones de la solución Microsoft 365 y se describen en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

Información sobre políticas de contraseñas, autenticación MFA y otros aspectos relacionados con la autenticación se describen en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

En el siguiente diagrama se describe el **proceso de autenticación de SharePoint Online**:

Se explica cómo funciona el escenario con el IdP (*Identity Provider*) predeterminado de Microsoft Entra ID.

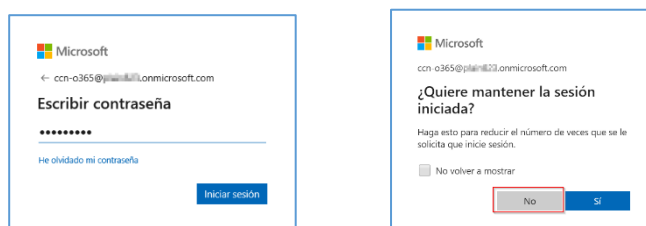


La cookie de *autenticación de Federación* (FedAuth) es para cada sitio de alto nivel de SharePoint Online, como el sitio raíz, *mySite* y el sitio de administración. La cookie de *autenticación de Federación raíz* (rtFa) se usa en todos los SharePoint Online. Cuando un usuario visita un nuevo sitio de alto nivel o la página de otra empresa, la cookie rtFa se usa para autenticarlas en modo silencioso sin que se le pregunte. Cuando un usuario cierra sesión en SharePoint Online, se elimina la cookie rtFa.

Sesión y cookies persistentes

De forma predeterminada, todas las cookies de SharePoint Online son **cookies de sesión**. Estas cookies no se guardan en la caché de cookies del explorador y, en su lugar, se eliminan siempre que se cierra el explorador.

Microsoft Entra ID muestra durante el inicio de sesión un *check*: “mantener la sesión iniciada” para habilitar las **cookies persistentes**. Estas cookies se guardan en la memoria caché del explorador y se conservan, aunque el explorador se cierre o reinicie el equipo.



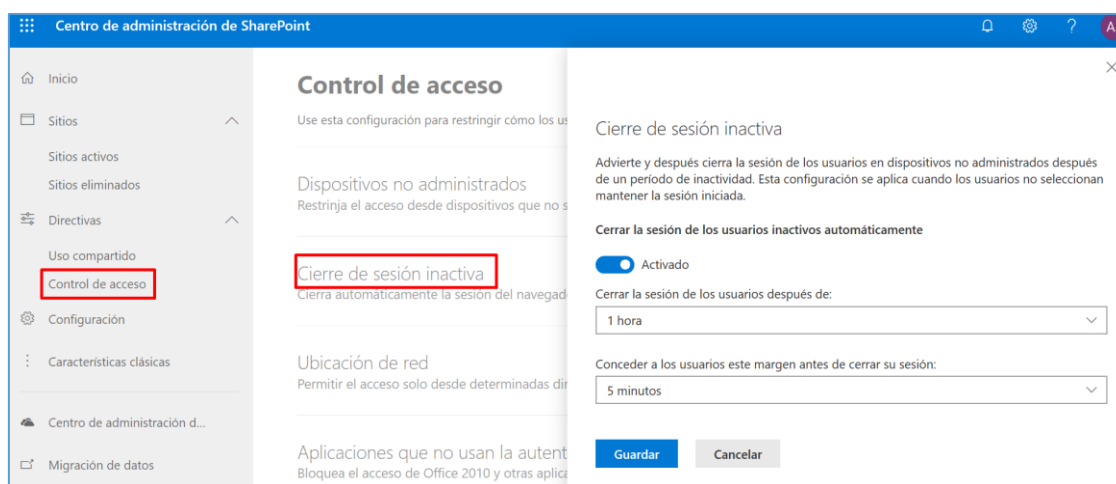
Ante la pregunta: ¿Quiere mantener la sesión iniciada?
Responder: No.

Se deben mantener deshabilitadas las cookies persistentes de inicio de sesión para evitar que se mantenga la sesión iniciada una vez se cierra el navegador y de esta forma forzar al usuario a reautenticarse siempre que utilice el servicio. Esta opción no es configurable a nivel de administración y por tanto es responsabilidad del usuario su cumplimiento.

Cierre de sesión inactiva

Conviene advertir y después cerrar la sesión de los usuarios en dispositivos no administrados después de un período de inactividad. Esta configuración se aplica cuando los usuarios no seleccionan mantener la sesión iniciada.

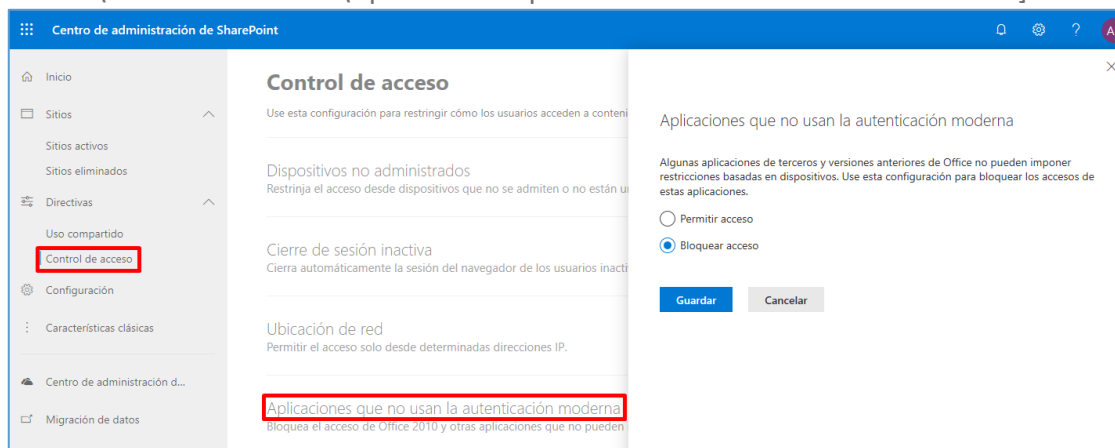
Se accede desde el *Centro de administración de SharePoint*, menú [Directivas\Control de acceso\Cierre de sesión inactiva].



Aplicaciones que no usan la autenticación moderna

Algunas aplicaciones de terceros y versiones anteriores de Office no pueden imponer restricciones basadas en dispositivos. Conviene bloquear los accesos de estas aplicaciones.

Se accede desde el *Centro de administración de SharePoint*, menú [Directiva\Control de acceso\Aplicaciones que no usan la autenticación moderna].



Se requiere establecer un “doble factor de autenticación” (MFA), tener una política adecuada de gestión de credenciales y políticas de acceso condicional. Así mismo, se requiere un registro de intentos de accesos con éxito y fallidos al sistema, descritos en el apartado [3.1.2.3 Registro de actividad]. Adicionalmente se puede controlar el acceso a Microsoft 365 mediante directivas de acceso condicional o reglas en AD FS, como se describe en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

3.1.1.6 MECANISMOS DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN)

Ídem que el apartado anterior.

3.1.2 EXPLOTACIÓN

SharePoint Online **siempre estará actualizado**. Es decir, el servicio es mantenido permanentemente por Microsoft, encargándose de las actualizaciones y parches, así como de establecer los mecanismos de detección y protección ante amenazas.

3.1.2.1 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

Si la organización dispone de *Microsoft Defender para Office 365* tendrá un explorador de detecciones en tiempo real, accesible desde el *Centro de Seguridad y cumplimiento de Office 365*. Consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

Si además se dispone de Exchange Online, se proporciona automáticamente protección contra malware para los archivos que se cargan y guardan en bibliotecas de documentos. Esta protección la proporciona el motor antimalware de Microsoft que también está integrado en Exchange.

Permitir o bloquear scripts personalizados

Permitir que los usuarios personalicen sitios y páginas en SharePoint mediante la inserción de una secuencia de comandos puede dar la flexibilidad necesaria para satisfacer las distintas necesidades de la organización. Sin embargo, debe tenerse en cuenta las implicaciones de seguridad de los scripts personalizados.

Cuando se permite a los usuarios ejecutar scripts personalizados, ya no se puede exigir la gobernanza, el ámbito de las capacidades del código insertado. En lugar de permitir un script personalizado, se recomienda usar *SharePoint Framework*. Todos los scripts que se ejecutan en una página de SharePoint (ya sea una página HTML en una biblioteca de documentos o un JavaScript en un elemento Web de editor de scripts) siempre se ejecutan en el contexto del usuario que visita la página y la aplicación de SharePoint.

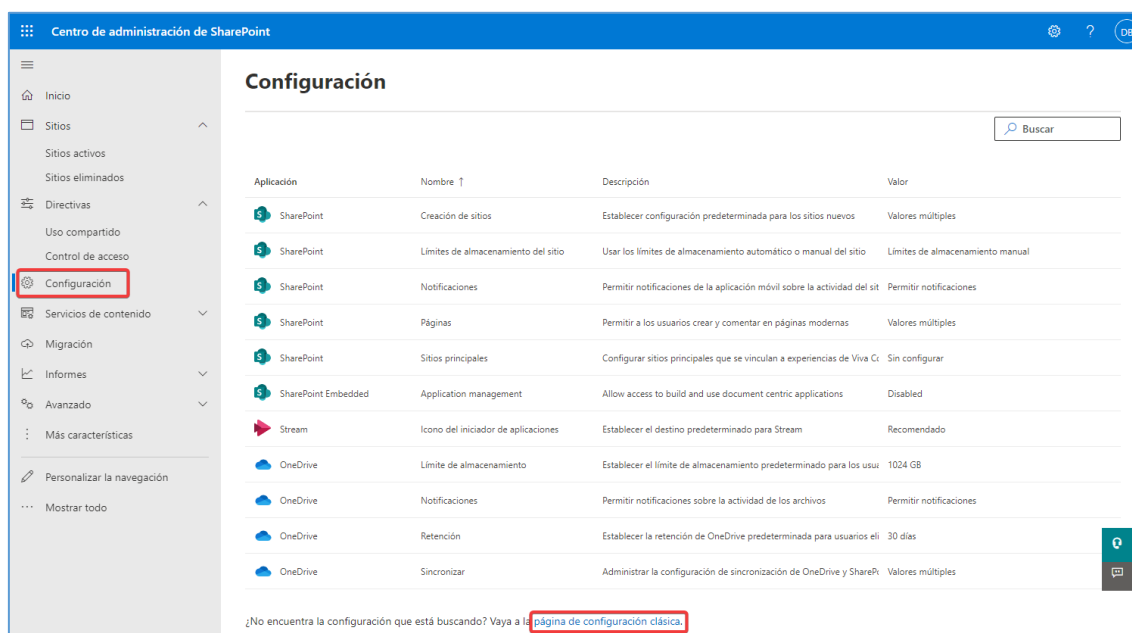
Una vez que permita el scripting, no se podrá identificar:

- Qué código se ha insertado.
- Dónde se ha insertado el código.
- Quién insertó el código.

Si se insertó un script peligroso o malintencionado, la única forma de detenerlo es eliminar la página que lo hospeda. Esto puede provocar la pérdida de datos.

Para permitir o bloquear scripts personalizados:

1. Acceder al Centro de administración de SharePoint, menú [Configuración], y acceder al link de la parte inferior de la página “*página de configuración clásica*”.



Centro de administración de SharePoint

Configuración

Aplicación	Nombre ↑	Descripción	Valor
SharePoint	Creación de sitios	Establecer configuración predeterminada para los sitios nuevos	Valores múltiples
SharePoint	Límites de almacenamiento del sitio	Usar los límites de almacenamiento automático o manual del sitio	Límites de almacenamiento manual
SharePoint	Notificaciones	Permitir notificaciones de la aplicación móvil sobre la actividad del sitio	Permitir notificaciones
SharePoint	Páginas	Permitir a los usuarios crear y comentar en páginas modernas	Valores múltiples
SharePoint	Sitios principales	Configurar sitios principales que se vinculan a experiencias de Viva Gl	Sin configurar
SharePoint Embedded	Application management	Allow access to build and use document centric applications	Disabled
Stream	Icono del iniciador de aplicaciones	Establecer el destino predeterminado para Stream	Recomendado
OneDrive	Límite de almacenamiento	Establecer el límite de almacenamiento predeterminado para los usuarios	1024 GB
OneDrive	Notificaciones	Permitir notificaciones sobre la actividad de los archivos	Permitir notificaciones
OneDrive	Retención	Establecer la retención de OneDrive predeterminada para usuarios eli	30 días
OneDrive	Sincronizar	Administrar la configuración de sincronización de OneDrive y ShareP	Valores múltiples

¿No encuentra la configuración que está buscando? Vaya a la [página de configuración clásica](#).

2. En la pantalla de configuración, navegar a la sección de “Script personalizado” y establecer los valores deseados.

Script personalizado

Permite controlar si los usuarios pueden ejecutar scripts personalizados en sitios personales y en sitios creados por ellos mismos. Nota: pueden transcurrir hasta 24 horas antes de que los cambios realizados a esta configuración tengan efecto.

Para obtener más información, consulte <http://go.microsoft.com/fwlink/?linkid=397546>

- ☒ Impedir que los usuarios ejecuten scripts personalizados en sitios personales
- ☐ Permitir que los usuarios ejecuten scripts personalizados en sitios personales
- ☒ Impedir que los usuarios ejecuten scripts personalizados en sitios creados por los mismos usuarios
- ☐ Permitir que los usuarios ejecuten scripts personalizados en sitios creados por los mismos usuarios

3.1.2.2 GESTIÓN DE INCIDENTES

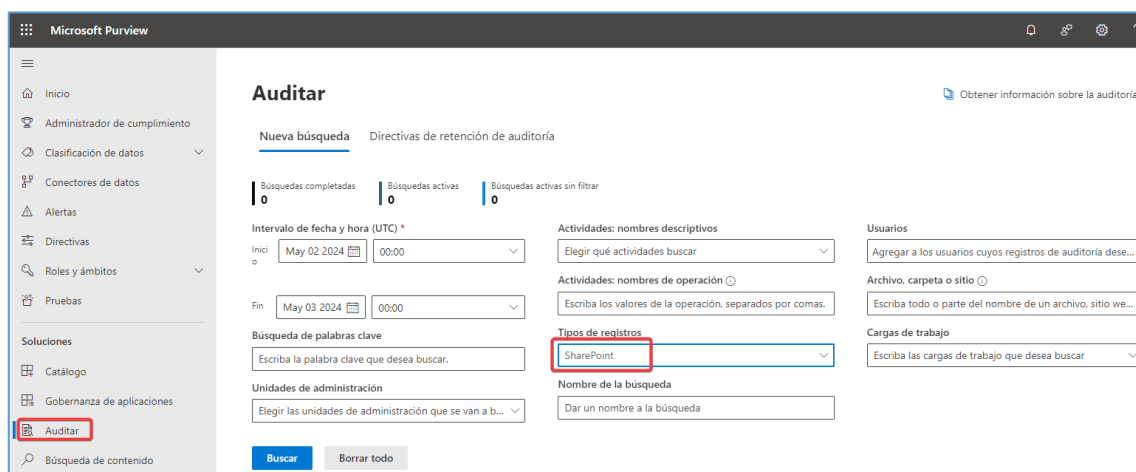
Ver apartado [3.1.2.1 Protección frente a código dañino] de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365] donde se explica cómo acceder a los informes de “Administración de Amenazas”.

3.1.2.3 REGISTRO DE LA ACTIVIDAD

Para configurar el registro de actividad del servicio de SharePoint, será necesario hacer uso de la funcionalidad de Auditoría disponible a través del portal de Microsoft Purview, anteriormente conocido como *Centro de Seguridad y cumplimiento de Office*

365. Más información en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

Mencionar además que existen muchas actividades relacionadas con Teams en el registro de auditoría, accesibles desde el portal de Microsoft Purview, en el menú [Auditar/Nueva búsqueda]:



3.1.3 MONITORIZACIÓN DEL SISTEMA

Consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365] para ver los distintos mecanismos de monitorización del servicio.

Conviene destacar que, a nivel de configuración de directivas de alertas, existen muchas actividades relacionadas con los sitios y objetos almacenados en SharePoint de manera predeterminada. Aunque dichas directivas están en desuso en función de los comentarios de los clientes como falsos positivos. Para conservar la funcionalidad de estas directivas de alerta, se pueden crear directivas de alerta personalizadas con la misma o distinta configuración. Reseñamos la que aún está en vigor:

- Volumen inusual de uso compartido de archivos externos. Genera una alerta cuando se comparte un número inusualmente grande de archivos en SharePoint o OneDrive con usuarios fuera de la organización. Esta directiva tiene una configuración de gravedad media.

3.2 MEDIDAS DE PROTECCIÓN

3.2.1 PROTECCIÓN DE LAS COMUNICACIONES

En cuanto a la protección de las comunicaciones, cabe reseñar que se usan los protocolos criptográficos para conexiones TLS, integrados en Microsoft 365 de manera automática (Todas las conexiones SSL se establecen con claves de 2048 bits). Esto es así cuando:

- Los usuarios trabajan con archivos guardados en *OneDrive for Business* o SharePoint Online.
- Los usuarios comparten archivos en reuniones en línea y conversaciones de mensajería instantánea.

En realidad, todas las comunicaciones de Microsoft 365 están cifradas: Clientes de correo (POP, IMAP, SMTP-TLS), Clientes Outlook (MAPI-HTTPS), Navegadores (Web HTTPS), Dispositivos móviles (ActiveSync HTTPS), Teams y Skype (SIP-TLS). No es necesario realizar ninguna configuración adicional, pero es importante indicar que, a partir de junio 2020, se eliminó soporte de TLS 1.0 y 1.1. Esto tiene implicaciones directas en los clientes.

3.2.2 PROTECCIÓN DE LA INFORMACIÓN

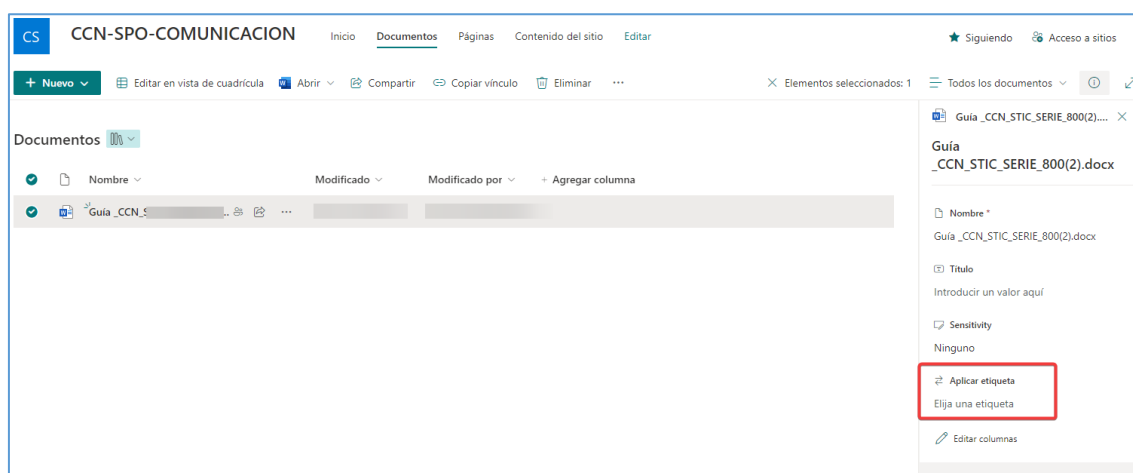
3.2.2.1 CALIFICACIÓN DE LA INFORMACIÓN

Microsoft 365 cuenta con diversos mecanismos para calificar la información, como se explican en el apartado [3.2.2.1 Calificación de la información] de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]. A continuación se describen varios desde el punto de vista de SharePoint Online.

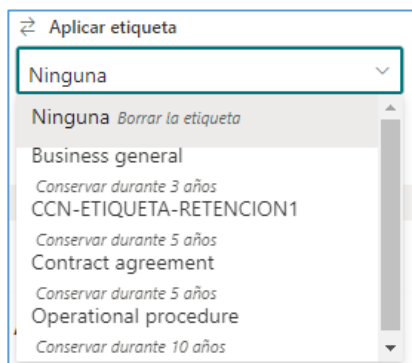
3.2.2.1.1 ETIQUETAS DE RETENCIÓN

Se puede definir el tiempo que un documento debe retenerse, o el tiempo después del cual debe borrarse. Más información sobre la **creación** de etiquetas de retención en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

1. Para aplicar una directiva de retención en un documento, navegar por el panel derecho de propiedades del documento, y seleccionar la opción “Aplicar etiqueta de retención”:

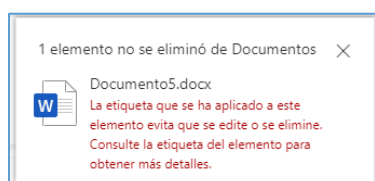


2. Se muestra un desplegable para seleccionar la etiqueta de retención a aplicar al documento.



Es posible seleccionar varios documentos a la vez y aplicar “en masa” la etiqueta.

Aplicar etiqueta
CCN-ETIQUETA-RETENCION1



Si, por ejemplo, se ha aplicado una etiqueta de retención de un documento que impida su borrado durante 5 años al intentar eliminar el documento aparecerá este mensaje.

3.2.2.1.2 SENSITIVITY LABELS

Esta característica está disponible en las aplicaciones de escritorio de Windows y Web (Word, Excel, PowerPoint y Outlook), así como en aplicaciones de otras plataformas (Mac, iOS y Android).

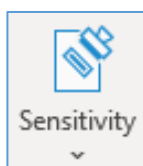
¿Cómo se usan las sensitivity labels desde un documento?

A fecha de edición de esta guía, ya no es necesario la instalación de ningún complemento para usar esta característica. Dicha característica está integrada directamente en las aplicaciones de Office (Word, Excel PowerPoint y Outlook) y el complemento que anteriormente era necesario instalarse ha sido deprecado con fecha de abril de 2024. Se deberá implementar una edición de suscripción de Office (ahora denominada Microsoft 365 Apps), ya que el etiquetado integrado no está disponible con las ediciones independientes de Office (a veces denominadas "Office Perpetual").

En las aplicaciones de Office está el icono:

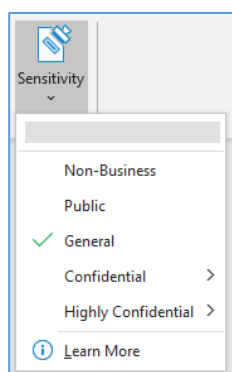


1. En la pestaña Inicio , seleccionar el botón “Sensitivity”.



Importante: La *confidencialidad* no está visible si la cuenta de Office no es una cuenta profesional con al menos licencia de Office 365 E3/E5 asignada, si el administrador no ha configurado *etiquetas de confidencialidad* y ha habilitado la característica.

2. Elegir la *sensitivity label* que se aplicará en el documento.



Para quitar una etiqueta que ya se ha aplicado al documento, anular la selección en el menú.

Nota: Si la organización tiene etiquetas configuradas en el portal de Azure Information Protection (AIP), es necesario migrarlas. [URL](#).

¿Qué sucede al aplicar una *sensitivity label* a un documento?

Al aplicar una *sensitivity label*, la información de la etiqueta se conservará con el documento o correo electrónico, incluso a medida que se comparte entre dispositivos, aplicaciones y servicios en la nube. Al aplicar una *sensitivity label* también se pueden producir cambios en el documento o correo electrónico según la configuración de la organización, por ejemplo:

- El cifrado con *Azure Rights Management* se puede aplicar al correo electrónico, invitaciones de reuniones o documentos.
- Puede aparecer un encabezado o pie de página en el documento o correo electrónico.
- Puede aparecer una marca de agua en el documento

3.2.2.2 LIMPIEZA DE DOCUMENTOS

Al compartir una copia electrónica de determinados documentos de Microsoft 365 o al exponer cierta documentación en Internet, es una buena práctica revisar el documento en busca de datos ocultos, información personal y en general cualquier metadato que pudiera estar asociado. Es posible eliminar esta información a través del Inspector de documentos, característica que se accede desde las propias aplicaciones de Word, Excel, PowerPoint o Visio.

3.2.2.3 COPIAS DE SEGURIDAD

No existe una solución global de respaldo de Microsoft 365. A fecha de edición de esta guía, nos encontramos con que a finales del año 2024 Microsoft tiene previsto sacar a disposición general un nuevo servicio llamado *Microsoft 365 Backup*. Dicho servicio será en modalidad de pago por uso y necesitará de una suscripción de Azure y un grupo de recursos.

Aunque existen mecanismos relacionados que se describen en el apartado [5. OTRAS CONSIDERACIONES DE SEGURIDAD] de la presente guía: control de versiones y papelera de reciclaje.

Así mismo, un mecanismo basado en “políticas de retención” en ciertos casos puede resultar suficiente para garantizar el respaldo de la información. Consultar el apartado [3.2.2.1 Calificación de la información] para ver cómo se aplican a un documento y cómo puede servir para protegerlo de ser eliminado.

3.2.2.4 DIRECTIVAS DE ADMINISTRACIÓN DE INFORMACIÓN

Las *directivas de administración de información* permiten controlar quién tiene acceso a la información de la organización, qué se puede hacer con esta y cuánto tiempo pueden conservarla. Una directiva puede ayudar a exigir el cumplimiento de normativas gubernamentales y legales, o de procesos empresariales internos. El administrador, puede configurar una directiva para controlar cómo realizar un seguimiento de los documentos, quién tiene acceso a estos y cuánto tiempo pueden conservarlos.

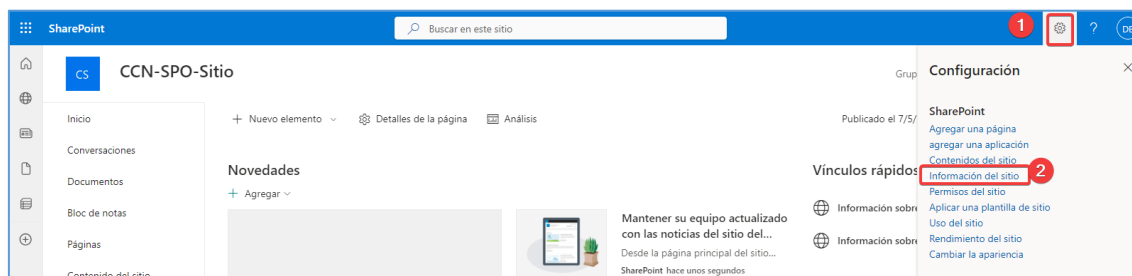
Se puede crear una *directiva de administración de información* en un sitio de tres maneras distintas:

- Crear una *directiva de administración de información* para usar en varios tipos de contenido dentro de una colección de sitios.
- Crear una *directiva de administración de información* para un tipo de contenido de sitio.
- Crear una *directiva de administración de información* para una lista o biblioteca.

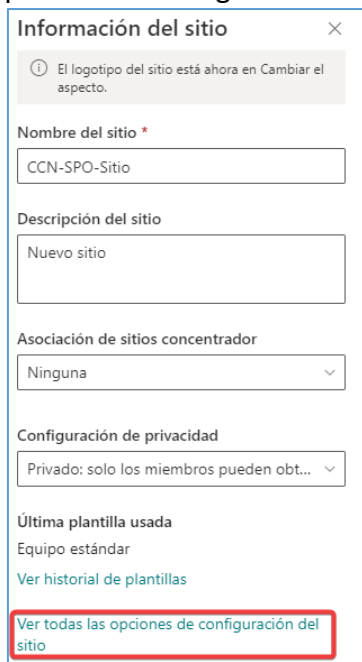
A continuación se describe cómo crear una *directiva de administración de información* para un tipo de contenido de sitio, el resto se realiza de forma análoga. [Más información.](#)

Crear una directiva de administración de información para un tipo de contenido de sitio

1. Acceder a la página principal del sitio, pulsar el icono “Configuración” y seleccionar el enlace “Información del sitio”.



2. Seleccionar “Ver todas las opciones de configuración del sitio”:



Información del sitio

El logotipo del sitio está ahora en Cambiar el aspecto.

Nombre del sitio *

CCN-SPO-Sitio

Descripción del sitio

Nuevo sitio

Asociación de sitios concentrador

Ninguna

Configuración de privacidad

Privado: solo los miembros pueden obt...

Última plantilla usada

Equipo estándar

[Ver historial de plantillas](#)

[Ver todas las opciones de configuración del sitio](#)

3. En “Configuración del sitio”, seleccionar “Características de colección de sitios”.



SharePoint

CS EDITAR VÍNCULOS

Configuración del sitio

Inicio

Conversaciones

Documentos

Bloc de notas

Páginas

Contenido del sitio

Papelera de reciclaje

EDITAR VÍNCULOS

Aspecto

Inicio rápido

Elementos de navegación

Cambiar el aspecto

Acciones del sitio

Administrar las características del sitio

Habilitar la exportación de la configuración de búsqueda

Restablecer la definición del sitio

Administración de la colección de sitios

Papelera de reciclaje

Orígenes de resultados de búsqueda

Tipos de resultados de búsqueda

Reglas de consultas de búsqueda

Esquema de búsqueda

Configuración de búsqueda

Importación de la configuración de búsqueda

Exportación de la configuración de búsqueda

Características de la colección de sitios

Jerarquía de sitios

Configuración de auditoría de la colección de sitios

Conexión del sitio del portal

Galerías del diseñador web

Columnas de sitio

Tipos de contenido de sitio

Administración de sitios

Configuración regional

Configuración de idioma

Exportar traducciones

Importar traducciones

Bibliotecas y listas del sitio

Alertas de usuario

RSS

Áreas de trabajo y sitios

Configuración del flujo de trabajo

Administración de almacenamiento de términos

Buscar

Fuentes de resultados

Tipos de resultados

Reglas de consulta

Esquema

Configuración de búsqueda

Disponibilidad de búsqueda y sin conexión

Importación de configuración

Exportación de la configuración

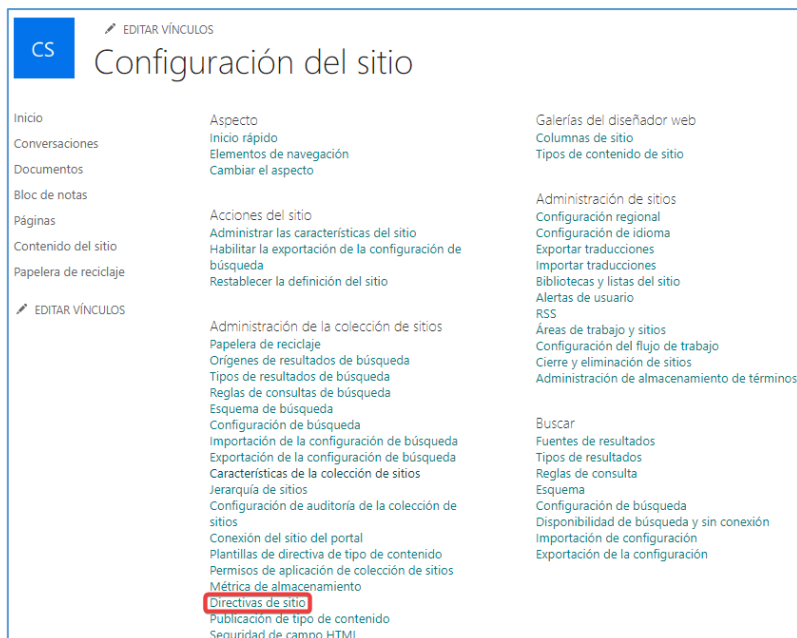
4. En la pantalla de características del sitio, navegar hasta “Directiva del sitio”, y activarlo.

**Directiva del sitio**

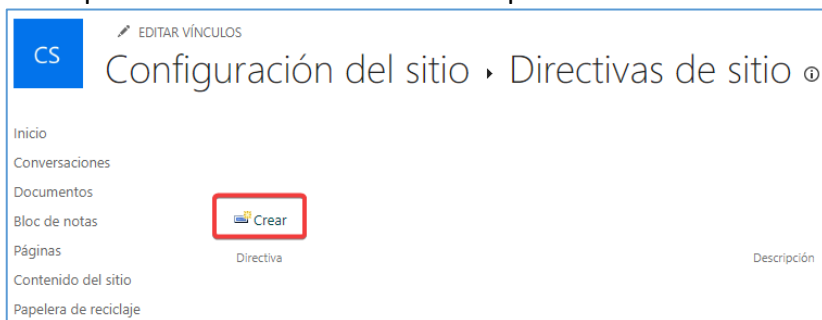
Permite a los administradores de colecciones de sitios definir programaciones de retención aplicables a un sitio y a todo su contenido.

Activar

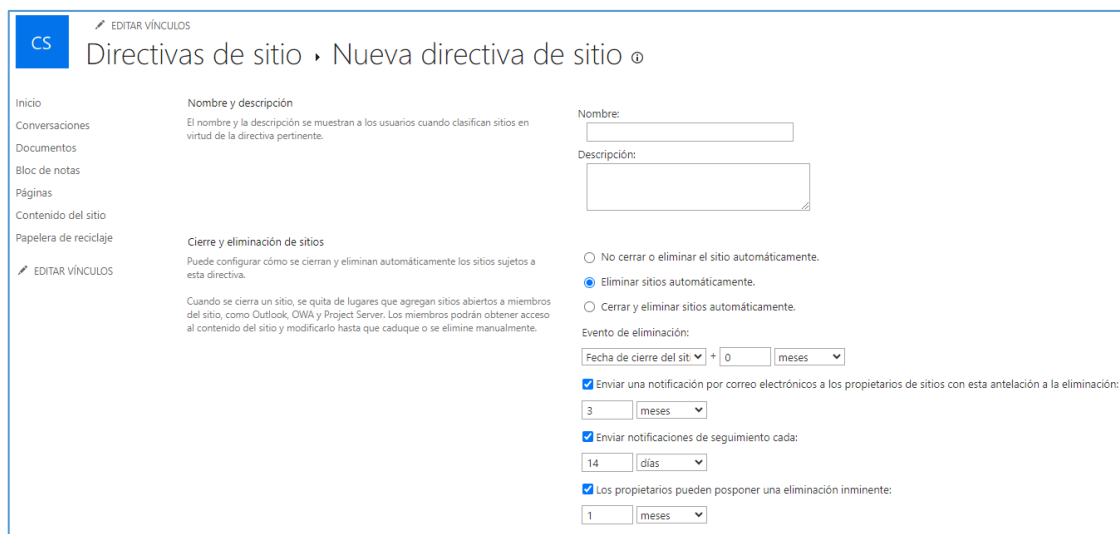
5. Volver a la pantalla de “Configuración del sitio” y pulsar el nuevo enlace “Directivas de sitio”.



6. En la pantalla de “Directivas del sitio” pulsar el botón “Crear”.



7. Establecer la política de retención adecuada.



Editar VÍNCULOS

Directivas de sitio ▸ Nueva directiva de sitio

Nombre y descripción
El nombre y la descripción se muestran a los usuarios cuando clasifican sitios en virtud de la directiva pertinente.

Cierre y eliminación de sitios
Puede configurar cómo se cierran y eliminan automáticamente los sitios sujetos a esta directiva.
Cuando se cierra un sitio, se quita de lugares que agregan sitios abiertos a miembros del sitio, como Outlook, OWA y Project Server. Los miembros podrán obtener acceso al contenido del sitio y modificarlo hasta que caduque o se elimine manualmente.

Evento de eliminación:

Fecha de cierre del sitio: 0 meses

☒ Enviar una notificación por correo electrónico a los propietarios de sitios con esta antelación a la eliminación: 3 meses

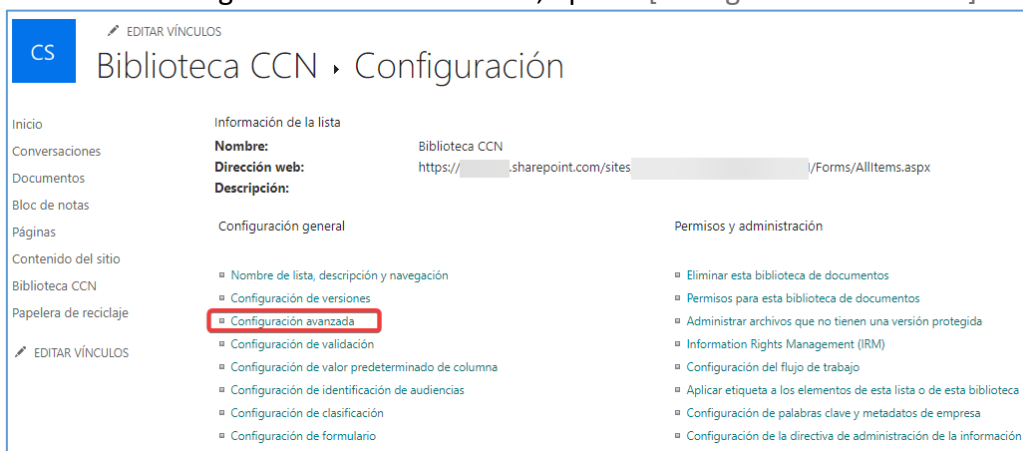
☒ Enviar notificaciones de seguimiento cada: 14 días

☒ Los propietarios pueden posponer una eliminación inminente: 1 meses

3.2.2.5 EVITAR QUE UNA BIBLIOTECA SE MUESTRA EN LOS RESULTADOS DE BÚSQUEDA

De forma predeterminada todas las bibliotecas se indizan en el buscador. Si alguna de ellas tiene contenido sensible se puede evitar que aparezca en los resultados.

1. Abrir la configuración de la biblioteca, opción [Configuración avanzada].



Editar VÍNCULOS

Biblioteca CCN ▸ Configuración

Información de la lista
Nombre: Biblioteca CCN
Dirección web: https://[redacted].sharepoint.com/sites/[redacted]/Forms/AllItems.aspx
Descripción:

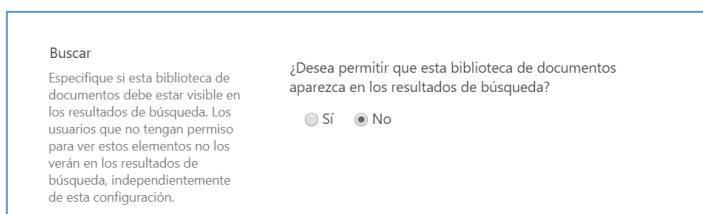
Configuración general

- Nombre de lista, descripción y navegación
- Configuración de versiones
- Configuración avanzada**
- Configuración de validación
- Configuración de valor predeterminado de columna
- Configuración de identificación de audiencias
- Configuración de clasificación
- Configuración de formulario

Permisos y administración

- Eliminar esta biblioteca de documentos
- Permisos para esta biblioteca de documentos
- Administrar archivos que no tienen una versión protegida
- Information Rights Management (IRM)
- Configuración del flujo de trabajo
- Aplicar etiqueta a los elementos de esta lista o de esta biblioteca
- Configuración de palabras clave y metadatos de empresa
- Configuración de la directiva de administración de la información

2. Desactivar la búsqueda.



Buscar
Especifique si esta biblioteca de documentos debe estar visible en los resultados de búsqueda. Los usuarios que no tengan permiso para ver estos elementos no los verán en los resultados de búsqueda, independientemente de esta configuración.

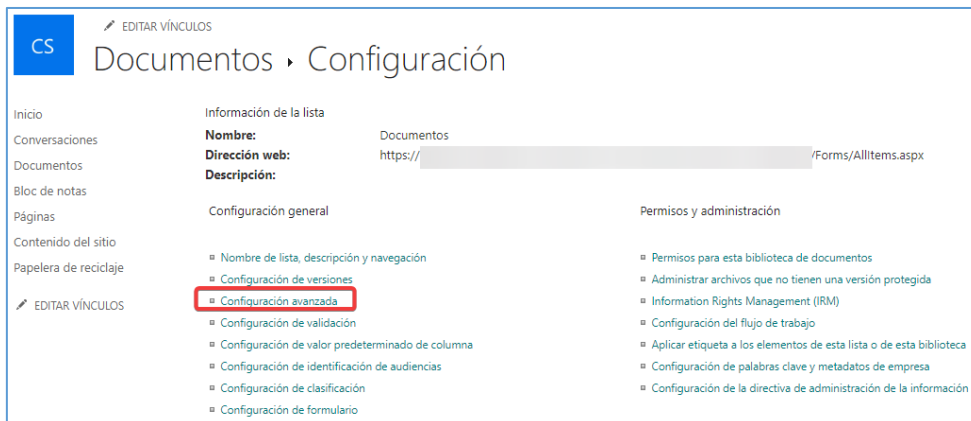
¿Desea permitir que esta biblioteca de documentos aparezca en los resultados de búsqueda?

☐ Sí ☒ No

3.2.2.6 EVITAR QUE LOS ELEMENTOS SE DESCARGUEN EN CLIENTES SIN CONEXIÓN

Si una biblioteca incluye información sensible, se puede evitar que se sincronice con clientes sin conexión como OneDrive.

1. Abrir la configuración de la biblioteca, opción [Configuración avanzada].



2. Bloquear que los elementos de esta biblioteca de documentos puedan descargarse a los clientes sin conexión.

Disponibilidad de cliente sin conexión

Indique si esta biblioteca de documentos debe estar disponible para los clientes sin conexión.

¿Desea permitir que los elementos de esta biblioteca de documentos puedan descargarse a los clientes sin conexión?

☐ Sí ☒ No

3.2.3 PROTECCIÓN DE LOS SERVICIOS

3.2.3.1 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

Microsoft 365 ofrece un sistema avanzado de **detección de amenazas** y **sistemas de mitigación** para proteger la infraestructura subyacente de los ataques de *denegación de servicio* (DoS) y prevenir la interrupción de servicio a los clientes.

El sistema de defensa DDoS de Azure está diseñado no solo para resistir ataques desde el exterior, sino también desde otros *Tenants* de Azure. Los mecanismos de limitación de peticiones de Exchange Online y SharePoint Online forman parte de un enfoque de varias capas para defenderse contra ataques DoS.

Consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure] para obtener más información sobre el *sistema de defensa DDoS de Azure*.

4. SCRIPTS DE CONFIGURACIÓN

Existen tareas de administración que pueden realizarse de manera más ágil a través del módulo de PowerShell “SharePoint Online Management Shell”. Este módulo se utiliza para administrar usuarios, sitios y colecciones de sitios. Todos los *cmdlets* del módulo comienzan con el prefijo SPO.

Los requerimientos mínimos de instalación en cuanto a Sistema operativo compatible:

Windows 11; Windows 10; Windows 7 Service Pack 1; Windows 8; Windows Server 2008 R2 SP1; Windows Server 2008 Service Pack 2; Windows Server 2012; Windows Server 2016

Y la versión de PowerShell 3.0.

1. Comprobar si ya tenemos el módulo instalado, y si no, instalarlo.

```
Get-Module -Name Microsoft.Online.SharePoint.PowerShell -ListAvailable | Select Name,Version
```

Para instalarlo:

```
Install-Module -Name Microsoft.Online.SharePoint.PowerShell
```

2. Conectarse.

2.1. Con usuario y password:

```
$adminUPN="<Dirección de correo electrónico complete de un administrador de SharePoint,
ejemplo: jdoe@contosotoycompany.onmicrosoft.com>"

$orgName="<Nombre de la organización de Microsoft 365, ejemplo: contosotoycompany>"

$userCredential = Get-Credential -UserName $adminUPN -Message "Type the password."

Connect-SPOService -Url https://$orgName-admin.sharepoint.com -Credential $userCredential.
```

2.2. Con MFA:

```
$orgName="< Nombre de la organización de Microsoft 365, ejemplo: contosotoycompany>"

Connect-SPOService -Url https://$orgName-admin.sharepoint.com
```

A continuación se muestran algunos ejemplos de cmdlets relacionados:

Obtener todas las colecciones de sitios

```
Get-SPOSite
```

Obtener información de una colección de sitio concreta

```
Get-SPOSite -Identity https://contoso.sharepoint.com
```

*Obtener información **detallada** de un sitio de grupo*

```
Get-SPOSite -Identity https://contoso.sharepoint.com/sites/groupname -detailed |fl
```

Deshabilitar la compartición de un sitio para los “no propietarios”

```
Get-SPOSite -Identity https://contoso.sharepoint.com -DisableSharingForNonOwnersStatus
```

5. OTRAS CONSIDERACIONES DE SEGURIDAD

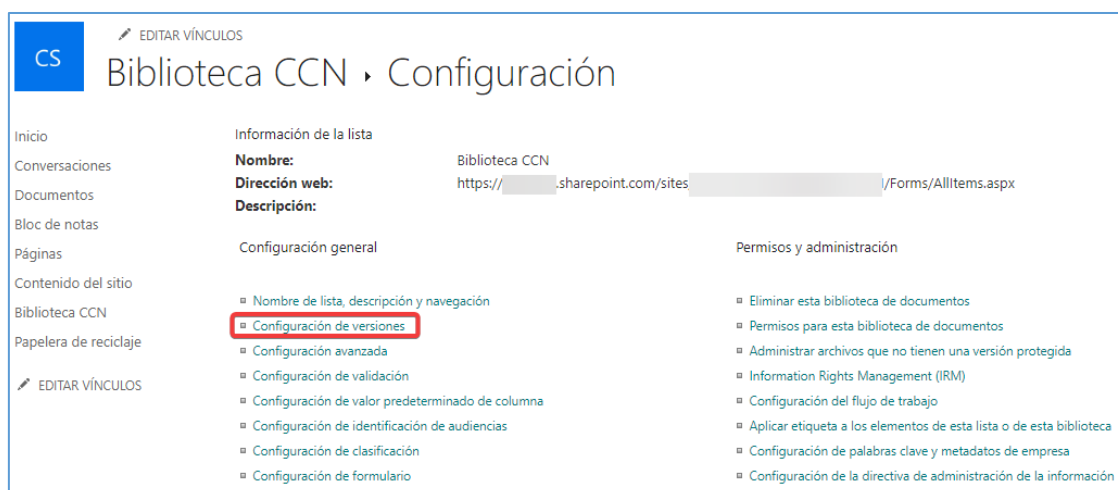
5.1 CONTROL DE VERSIONES

Cuando el control de versiones está habilitado en la lista o biblioteca de SharePoint, puede almacenar, hacer un seguimiento y restaurar elementos en una lista y archivos de una biblioteca cada vez que cambien.

El control de versiones es, sin duda, una de las herramientas más útiles en SharePoint: permite ver qué cambios se han producido en los documentos, mostrando el número de versión y tamaño de cada documento, quién y cuándo realizó el último cambio y ver y/o restaurar cualquier versión anterior.

Habilitar y configurar las versiones para una lista o biblioteca

1. Abrir la configuración de la biblioteca y pulsar enlace “Configuración de versiones”.

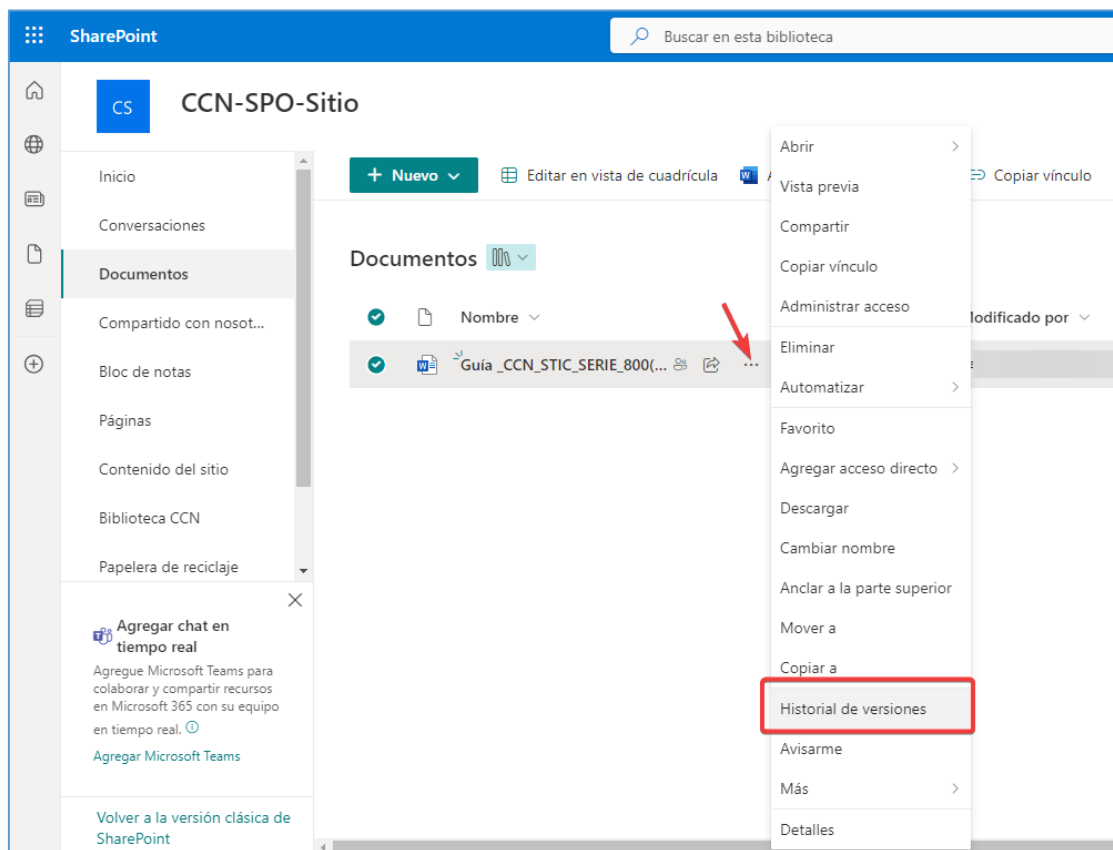


2. Configurar las opciones.



Consultar el historial de versiones

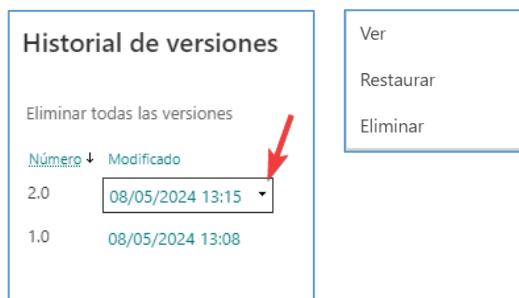
1. Se accede a través del [menú de acciones] que aparece en la propia línea del documento a consultar.



2. Se despliega a continuación todo el historial de versiones del documento:

Historial de versiones				
Eliminar todas las versiones				
Número	Modificado	Modificado por	Tamaño	Comentarios
2.0	08/05/2024 13:15		505,8 KB	
1.0	08/05/2024 13:08		502,1 KB	

- En cada *item* del historial, en el campo “modificado”, se muestra un desplegable con las acciones a realizar sobre esa versión concreta:

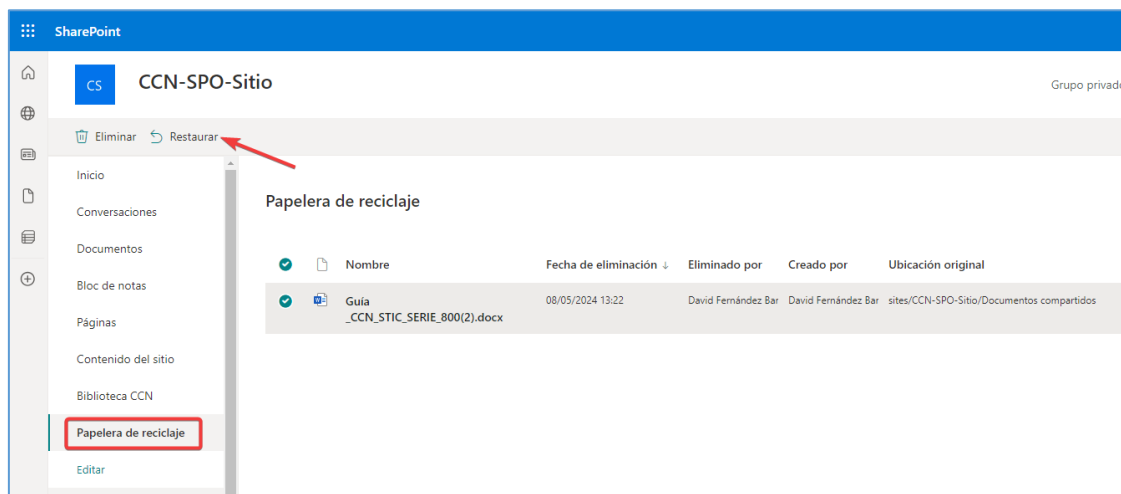


5.2 PAPELERA DE RECICLAJE

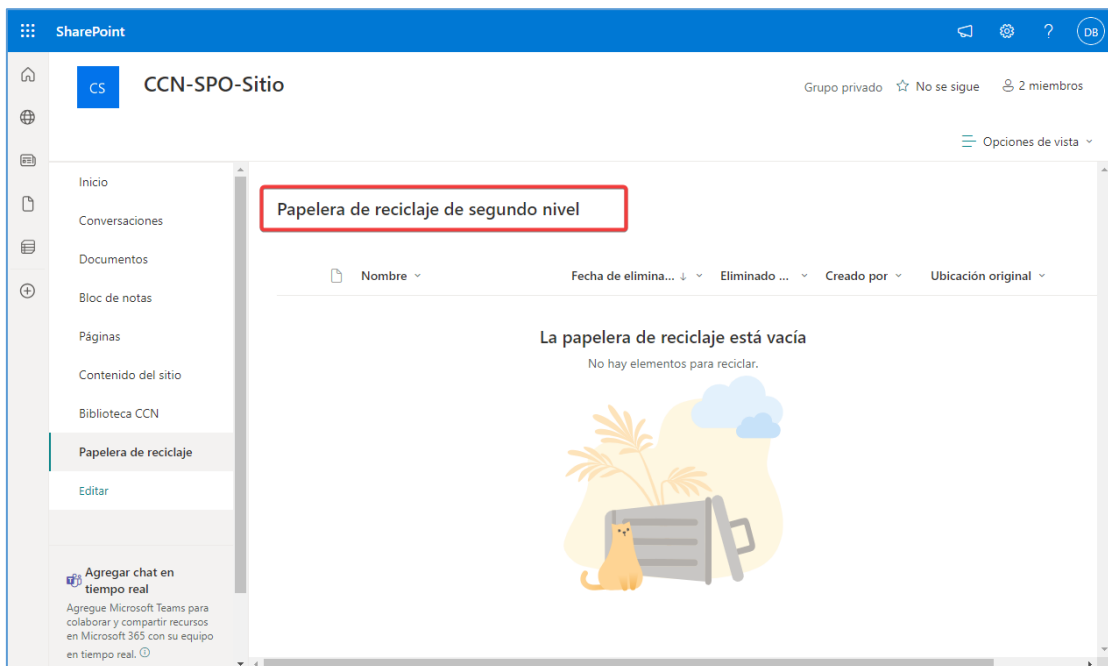
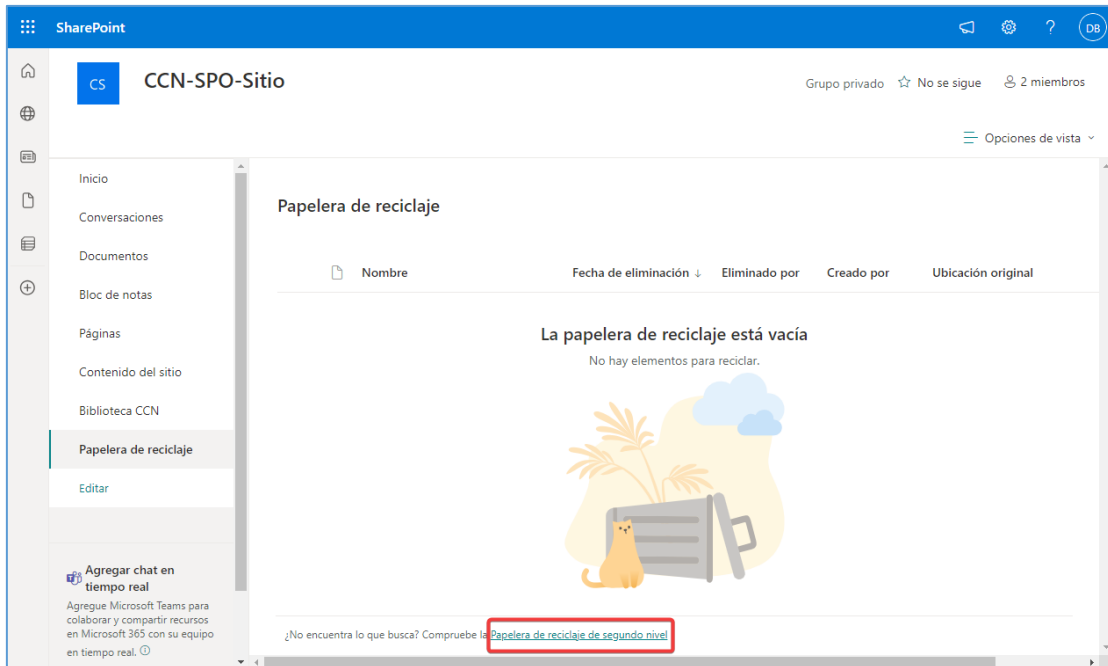
SharePoint Online establece dos niveles de papelera de reciclaje con dos áreas de almacenamiento independientes, cada una con un período de retención de la información. A diferencia de versiones anteriores no es configurable.

Nota: Para documentos sensibles que exijan un borrado inmediato, es responsabilidad del usuario su eliminación definitiva de todas las áreas de la papelera de reciclaje.

- Cuando se eliminan elementos (incluidos los de *OneDrive for Business*) de un sitio de SharePoint, se envían a la papelera de reciclaje del sitio, también denominada papelera de reciclaje de primer nivel, donde puede restaurarlos si es necesario.



- Cuando se eliminan elementos de una papelera de reciclaje de un sitio, se envían a la papelera de reciclaje de la colección de sitios, también denominada papelera de reciclaje de segundo nivel.



Un administrador de la colección de sitios de SharePoint puede ver y restaurar los elementos eliminados de la papelera de reciclaje de la colección de sitios a su ubicación original. Si se elimina un elemento de la papelera de reciclaje de la colección de sitios, o se supera el tiempo de retención, se eliminará de forma permanente.

¿Cuánto tiempo se conservan los elementos eliminados en la Papelera de reciclaje?

En SharePoint Online, los elementos se conservan por **93 días** desde el momento en que se eliminan de su ubicación original. Permanecen en la *papelera de reciclaje del sitio* todo el tiempo, a menos que alguien lo elimine o vacíe esa papelera de reciclaje.

En ese caso, los elementos van a la *papelera de reciclaje de la colección de sitios*, donde permanecen durante el resto de 93 días, a menos que:

- la papelera de reciclaje de la colección de sitios supera su cuota y comienza a purgar los elementos más antiguos.
- el administrador de la colección de sitios elimina manualmente los elementos de la papelera de reciclaje de la colección de sitios.

El almacenamiento de la *papelera de reciclaje del sitio* cuenta con la cuota de almacenamiento de la colección de sitios y el umbral de vista de lista. La cantidad de espacio asignado a la papelera de reciclaje de la colección de sitios es 200% de la cuota de la colección de sitios. Estos valores no se pueden configurar.

3. Tercer nivel de copia de seguridad.

SharePoint Online conserva las **copias de seguridad de todo el contenido durante 14 días adicionales** más allá de la eliminación real. Si el contenido no se puede restaurar a través de la papelera de reciclaje o de la restauración de archivos, un administrador puede ponerse en contacto con el soporte técnico de Microsoft para solicitar una restauración en cualquier momento dentro de la ventana de 14 días.

5.3 DIRECTIVAS DE USO COMPARTIDO

Los administradores globales y de SharePoint en Microsoft 365 pueden cambiar su configuración de uso compartido de nivel de organización para SharePoint y OneDrive.

Para ello acceder al *Centro de administración de SharePoint Online*:



Los niveles establecidos son los siguientes:

Todos	Los usuarios pueden compartir archivos y carpetas con vínculos que no requieren inicio de sesión.
--------------	---

Invitados nuevos y existentes	Los invitados deben iniciar sesión o proporcionar un código de verificación.
Invitados existentes	Solo los invitados que ya forman parte del directorio de su organización.
Solo los miembros de su organización	No se permite ningún tipo de uso compartido externo.

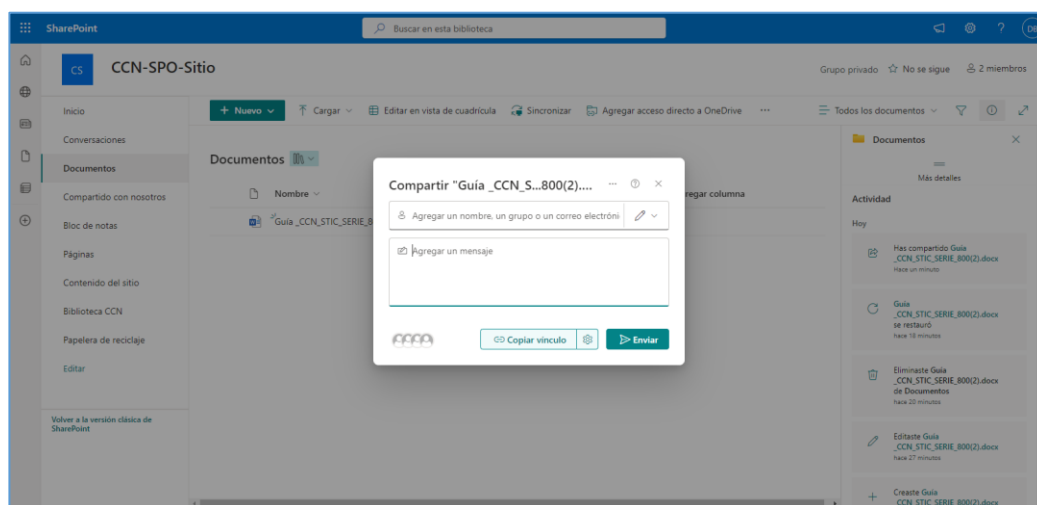
1. Seleccionar el nivel menos permisivo para no permitir el uso compartido externo, es decir, **sólo se permitirá la compartición de documentos entre miembros de la organización**.
2. A continuación, se elige la opción que les aparecerá a los usuarios de forma predeterminada.

Vínculos de archivos y carpetas

Elija el tipo de vínculo que se selecciona de forma predeterminada cuando los usuarios comparten archivos y carpetas en SharePoint y en OneDrive.

- ☐ Personas específicas (solo las personas que especifique el usuario)
☒ Solo los miembros de su organización
☐ Cualquiera con el vínculo

Así, por ejemplo, con esta opción a los usuarios les aparecerá al compartir un documento lo siguiente:



3. Elegir tipo de vínculo.

Elija el tipo de vínculo que se selecciona de forma predeterminada cuando los usuarios comparten archivos y carpetas en SharePoint y en OneDrive.

- ☐ Personas específicas (solo las personas que especifique el usuario)
☒ Solo los miembros de su organización
☐ Cualquiera con el vínculo

4. Seleccionar otras opciones de configuración.

Otras opciones de configuración

- ☒ Mostrar a los propietarios los nombres de las personas que han visualizado los archivos

5. Elegir “permiso de vínculo predeterminado”. Valor recomendado: Ver.

Elija el permiso seleccionado de forma predeterminada para compartir enlaces.

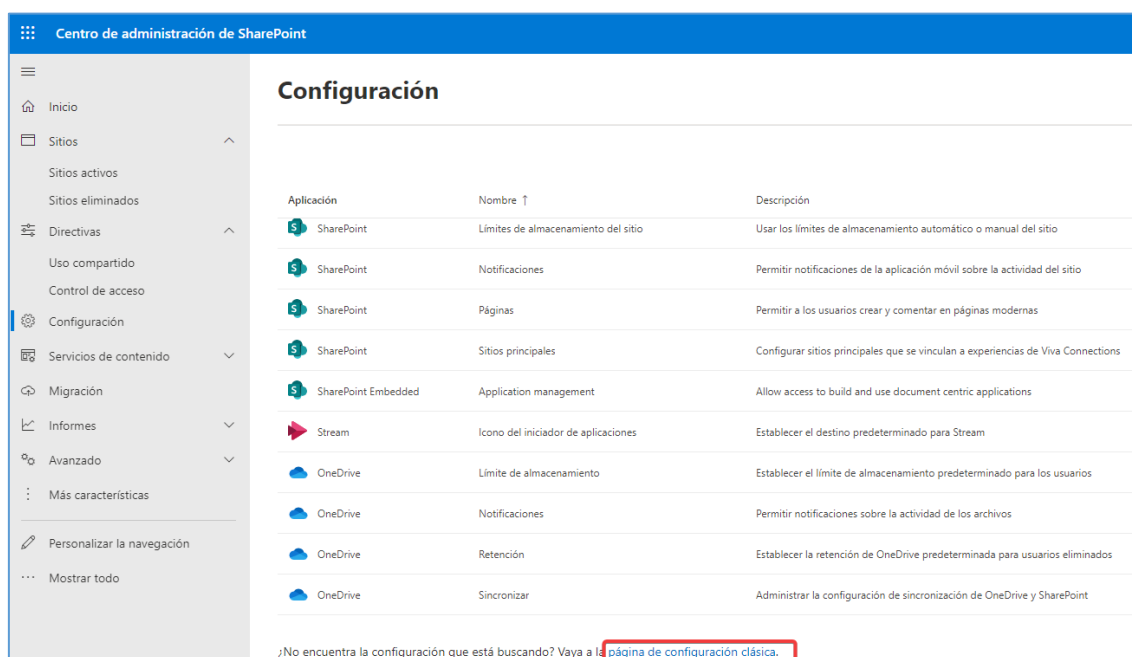
- ☒ Ver
- ☐ Editar

5.4 BLOQUEAR LA INTEGRACIÓN CON YAMMER

De forma predeterminada SharePoint Online habilita la integración con Yammer. Esto se puede restringir. Esta integración reemplaza a *Newsfeed* y cambia la navegación global de Microsoft 365. Además, Yammer no es un servicio disponible actualmente en el Centro de confianza de O365. Al habilitar la integración, Yammer podrá leer y copiar el acceso a la información de usuario y de grupo de la empresa.

Se puede activar o desactivar Yammer para conversaciones en SharePoint desde el *Centro de administración de SharePoint Online*.

1. Iniciar la página de *configuración clásica*.



Centro de administración de SharePoint

Configuración

Aplicación	Nombre ↑	Descripción
SharePoint	Límites de almacenamiento del sitio	Usar los límites de almacenamiento automático o manual del sitio
SharePoint	Notificaciones	Permitir notificaciones de la aplicación móvil sobre la actividad del sitio
SharePoint	Páginas	Permitir a los usuarios crear y comentar en páginas modernas
SharePoint	Sitios principales	Configurar sitios principales que se vinculan a experiencias de Viva Connections
SharePoint Embedded	Application management	Allow access to build and use document centric applications
Stream	Icono del iniciador de aplicaciones	Establecer el destino predeterminado para Stream
OneDrive	Límite de almacenamiento	Establecer el límite de almacenamiento predeterminado para los usuarios
OneDrive	Notificaciones	Permitir notificaciones sobre la actividad de los archivos
OneDrive	Retención	Establecer la retención de OneDrive predeterminada para usuarios eliminados
OneDrive	Sincronizar	Administrar la configuración de sincronización de OneDrive y SharePoint

¿No encuentra la configuración que está buscando? Vaya a la [página de configuración clásica](#).

2. En colaboración social empresarial, seleccionar “Utilizar SharePoint Newsfeed”.

Colaboración social para empresas

El servicio Yammer.com se ha retirado y esta configuración se quitará.

- ☐ Usar el servicio Yammer.com (ya no disponible)
- ☒ Utilizar SharePoint Newsfeed (valor predeterminado)

6. GLOSARIO Y ABREVIATURAS

A continuación se describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía:

Término	Definición
IRM	<i>Information Rights Management.</i>
SPO	<i>SharePoint Online</i>
Sitio de SPO	es un sitio web que ofrece un espacio central de colaboración y almacenamiento de documentos, información e ideas.
Sitio de comunicación	para difundir información, compartir noticias, informes, estados, etc. a una audiencia amplia en un formato visualmente atractivo. Sólo genera contenido un pequeño conjunto de miembros y es un público mucho mayor quien lo consulta.
Sitio de grupo	proporciona una ubicación concreta en la que un grupo de personas pueden trabajar en un proyecto concreto y compartir información desde cualquier lugar con cualquier dispositivo. Son grupos cerrados, la información se limita sólo a los miembros del grupo o participantes específicos.
Sitio de grupo público	sitio de SPO accesible por cualquier persona de la organización.
Sitio de grupo privado	sitio de SPO sólo accesible por miembros del grupo.

7. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio, donde la organización podrá valorar qué medidas de las propuestas se cumplen.

Control ENS	Configuracion		Estado
op	Marco Operacional		
op.acc	Control de Acceso		
op.acc.1	Identificación		
	Se ha configurado el uso de cuentas y la asignación de licencias a usuarios. Siguiendo las recomendaciones de Office 365 basada en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.2	Requisitos de Acceso		

Control ENS	Configuracion	Estado	
	Se han comprobado los <u>niveles de permisos</u> para los recursos de la organización: propietarios, miembros y visitantes.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.3	Segregación de funciones y tareas		
	Se ha asignado adecuadamente el rol de Admin a un usuario administrador de SharePoint (en caso de que se haya establecido una delegación para este servicio).	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:

Control ENS	Configuracion	Estado	
Op.acc.4	Proceso de gestión de derechos de acceso		
	Se han creado “niveles de permisos” específicos para la organización.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.5	Mecanismo de autenticación (usuarios externos)		
	Se ha informado a los usuarios que mantengan deshabilitadas las <u>cookies</u> <u>persistentes</u> en el inicio de sesión.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: Si No	Observaciones:

Control ENS	Configuracion	Estado	
		☐	☐
Op.acc.5	Mecanismo de autenticación (usuarios externos)		
	Se ha configurado la advertencia y cierre de las sesiones de los usuarios después de un período de inactividad.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.5	Mecanismo de autenticación (usuarios externos)		
	Se ha bloqueado el acceso a aplicaciones que no usan la autenticación moderna.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas:	Observaciones:

Control ENS	Configuracion	Estado	
		☐ Si ☐ No	
Op.acc.5	Mecanismo de autenticación (usuarios externos)		
	Se encuentra habilitado el “doble factor de autenticación” y se dispone de una adecuada política de gestión de credenciales.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.5	Mecanismo de autenticación (usuarios externos)		
	Se han configurado directivas de acceso condicional o reglas en AD FS, como se describe en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

Control ENS	Configuracion	Estado	
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.5	Mecanismo de autenticación (usuarios externos)		
	Se ha activado la <i>Ubicación de red</i> para permitir el acceso solo desde determinadas direcciones IP. Y la limitación de acceso a los administradores.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
Op.acc.5	Mecanismo de autenticación (usuarios externos)		
	Se han configurado directivas de acceso condicional para el acceso remoto, como se describe en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

Control ENS	Configuracion	Estado	
		Evidencias Recogidas:	Observaciones:
		☐ Si ☐ No	
Op.acc.6	Mecanismo de autenticación (usuarios de la organización)		
	Ídem controles aplicados a Op.acc.5	Aplica:	Cumple:
		☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas:	Observaciones:
		☐ Si ☐ No	
op.exp	Explotacion		
op.exp.6	Protección frente a código dañino		
	Se ha bloqueado que los usuarios puedan ejecutar scripts personalizados en	Aplica:	Cumple:

Control ENS	Configuracion	Estado	
	sitios personales y en sitios creados por ellos mismos.	☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.exp.6	Protección frente a código dañino		
	Se recomienda la detección de amenazas en tiempo real, accesible desde el <i>Centro de Seguridad y cumplimiento de Office 365</i> . <i>*Para dichas tareas la organización debe dispone de Microsoft Defender para Office 365.</i>	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.exp.8	Registro de la actividad		

Control ENS	Configuracion	Estado	
	Se ha activado el registro de auditoría.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
op.mon	Monitorización del sistema		
	Se han configurado alertas en el <i>Centro de Seguridad y cumplimiento</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:

Control ENS		Configuracion		Estado	
mp	Medidas de Protección				
mp.info	Protección de la información				
mp.info.2	Calificación de la información				
	Se han aplicado políticas de retención.	Aplica:		Cumple:	
		☐ Si ☐ No	☐ Si ☐ No		
		Evidencias Recogidas:		Observaciones:	
		☐ Si ☐ No			
mp.info.2	Calificación de la información				
	Se han aplicado políticas de DLPs cómo se describe en el apartado Calificación de la información de la guía [CCN-STIC-884A - Guía de configuración segura para Azure].	Aplica:		Cumple:	
		☐ Si ☐ No	☐ Si ☐ No		

Control ENS	Configuracion	Estado	
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.2	Calificación de la información		
	Se han aplicado <i>sensitivity labels</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.2	Calificación de la información		
	Se ha aplicado un cifrado especial mediante etiquetas de sensibilidad a sitios de SharePoint que precisan una protección especial.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

Control ENS	Configuracion	Estado	
	* Microsoft cifra automáticamente los datos en reposo y de manera transparente para el usuario. Para un cifrado adicional se pueden usar las <i>sensitivity labels</i> .	Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.5	Limpieza de documentos		
	Se ha eliminado información personal y en general cualquier metadato que pudiera estar asociado a los documentos. *Mediante la herramienta Inspector de documentos (característica que se accede desde las propias aplicaciones de Word, Excel, PowerPoint o Visio) o aplicaciones de terceros. Como se describe en el apartado Limpieza de documentos de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.6	Copias de seguridad		
	Se han aplicado políticas de retención para gestionar el tiempo de almacenamiento de los documentos y correos.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

Control ENS	Configuracion	Estado	
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info.6	Copias de seguridad		
	Se ha comunicado a los usuarios cómo gestionar el “control de versiones” de los documentos y la papelera de reciclaje.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info	Evitar indización de bibliotecas con contenido sensible		
	Se ha configurado que las bibliotecas con contenido sensible no aparezcan en el buscador.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No

Control ENS	Configuracion	Estado	
		☐ ☐	☐ ☐
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.info	Evitar indización de bibliotecas con contenido sensible		
	Se ha configurado que las bibliotecas con contenido sensible no aparezcan en el buscador. Incluyendo de igual modo la descarga de elementos cuando no existe conexión.	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:
mp.s	Protección de los servicios		
mp.s.4	Protección frente a la denegación de servicio		

Control ENS	Configuracion	Estado	
	Se ha tenido en cuenta la información detallada en la guía [CCN-STIC-884A - Guía de configuración segura para Azure] sobre el <i>sistema de defensa DDoS de Azure</i> .	Aplica: ☐ Si ☐ No	Cumple: ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	Observaciones:

OTRAS CONSIDERACIONES DE SEGURIDAD			
Uso compartido externo			
Se ha restringido el uso compartido externo.	Aplica:	Cumple:	
	☐ Si ☐ No	☐ Si ☐ No	
	Evidencias Recogidas:	Observaciones:	
	☐ Si ☐ No		
Integración con Yammer			
Se ha bloqueado la integración con Yammer	Aplica:	Cumple:	
	☐ Si ☐ No	☐ Si ☐ No	
	Evidencias Recogidas:	Observaciones:	
	☐ Si ☐ No		

