Guía de Seguridad de las TIC
CCN-STIC 885B

Guía de configuración segura para Sharepoint Online

ENERO 2020

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.01.14 15:33:47 +01'00'

© Centro Criptológico Nacional, 2020

NIPO: 083-19-262-1

Fecha de Edición: enero de 2020

Plain Concepts ha participado en la realización y modificación del presente documento y sus anexos. Sidertia Solutions S.L. ha participado en la revisión de esta guía.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán

Secretario de Estado

Director del Centro Criptológico Nacional

ÍNDICE

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 Office 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-2010-1330.

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 *Office 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 Office 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:

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

1.3 Prerequisitos para el despliegue mediante PowerShell

PowerShell de Office 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

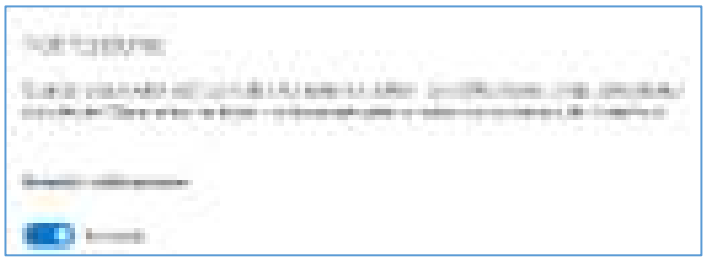
Sharepoint Online no necesita instalación previa en el entorno *on-premise* del cliente, ya que es un servicio *on-line* accesible desde internet y alojado en el *tenant* de Office 365 de la organización. Utiliza la infraestructura de "Nube pública" referida en la guía [823-Cloud Computing].

Sharepoint Online, así como el conjunto de Office 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 Office 365 (portal.office365.com).

En el menú [Configuración] se puede controlar qué características están disponibles para los usuarios de la organización.



Notificaciones

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

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

Límites de almacenamiento del sitio

Automático para compartir el almacenamiento entre todos los sitios.

Manual: establecer límites específicos para cada sitio.

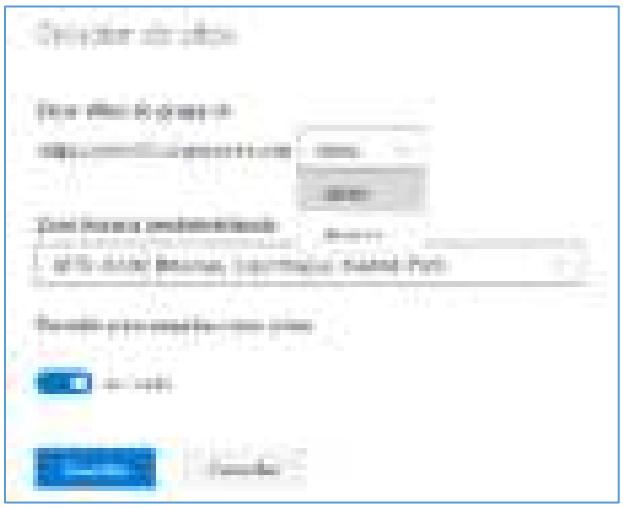
*Recomendación: dejar valor por defecto. No afecta a la seguridad.

Experiencia de administración predeterminada

Para activar o desactivar el nuevo *Centro de administración de Sharepoint* de forma predeterminada.

Se recomienda dejar activada esta opción, para una experiencia de usuario administrador más moderna, de lo contrario se activa el *Centro de administración clásico*.

Creación de sitios



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

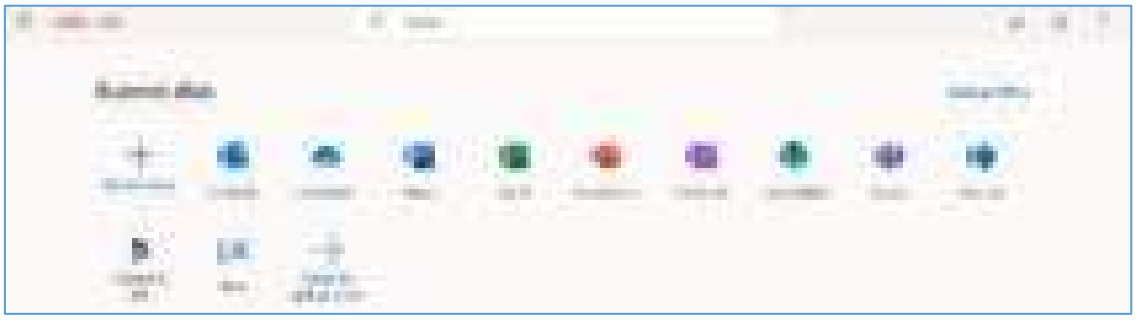
Configurar la zona horaria.

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

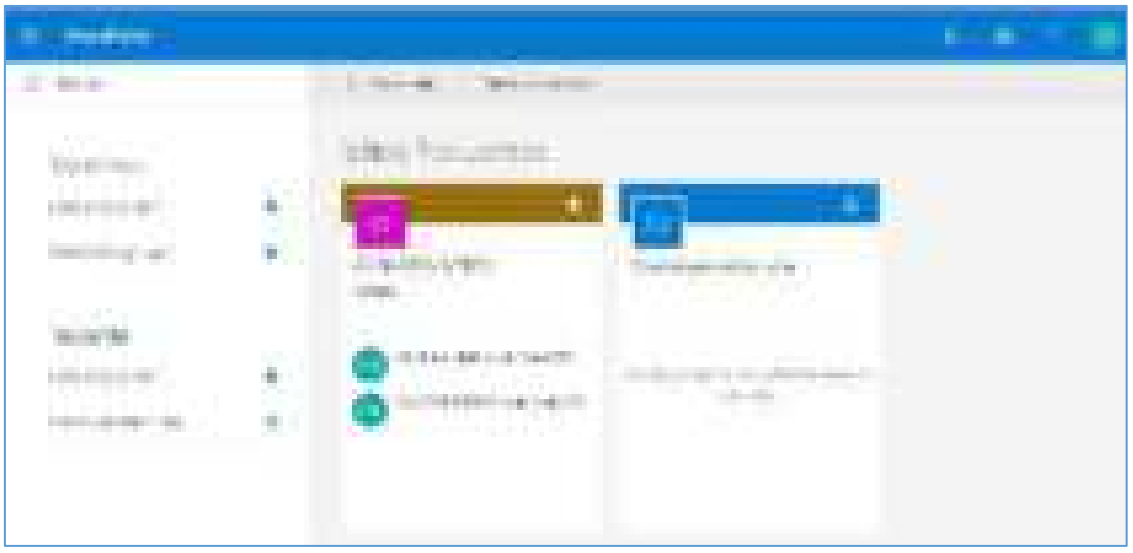
*Recomendación: elegir la zona horaria adecuada y dejar resto de valores por defecto.

2.2 Usuario final - primeros pasos

El *usuario final* podrá acceder al portal Office 365 a través de la *url*: *portal.office365.com* o *www.office.com*. Tras introducir las credenciales se muestra un panel con todas las aplicaciones a las que tiene acceso.

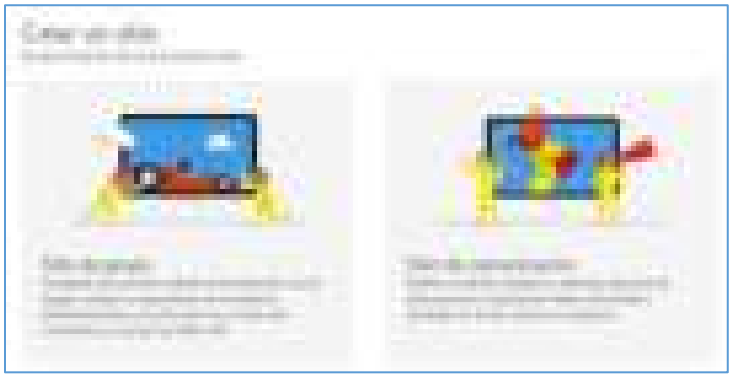


Pulsar en el icono de Sharepoint para acceder al portal de Sharepoint.



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.



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: crear un sitio de grupo sin un grupo de Office 365, o bien un centro de documentos, una wiki empresarial, un portal de publicación o un sitio de Project Web App.

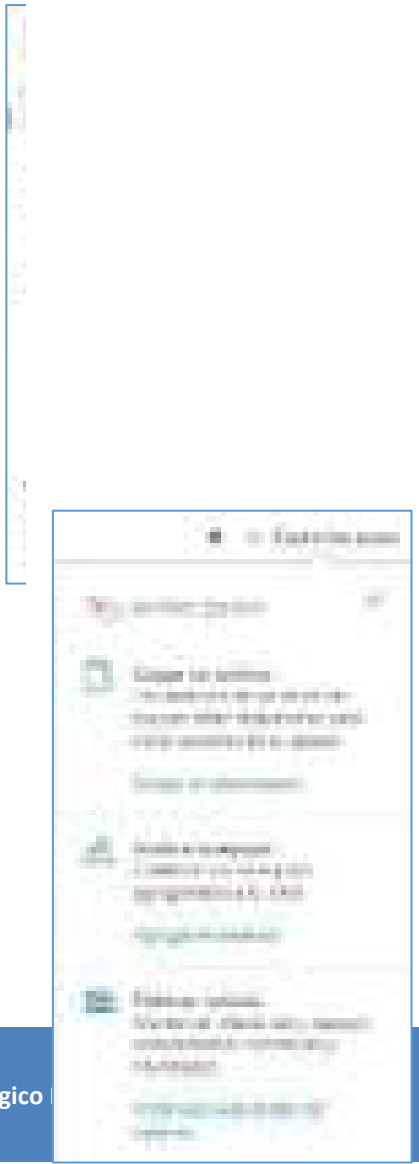
Crear un sitio de grupo

1. Añadir una descripción.

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).

2. Agregar propietarios y miembros.

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



4. Los siguientes pasos para el usuario podrían ser:

- Cargar archivos en el sitio.
- Invitar a miembros al equipo.
- Publicar noticias.

Crear un sitio de comunicación

1. Añadir una descripción.

2. Al pulsar “Finalizar” se crea el *sitio de comunicación* y se navega a la página del sitio recién creado.

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 que aplican exclusivamente a este servicio.

3.1 Marco Operacional

3.1.1 Control de acceso

3.1.1.1 Identificación

La gestión de identidades de Sharepoint Online es común a todas las aplicaciones de la solución Office 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 tres grupos siguientes de forma predeterminada, con un nivel de permisos asociado:
  - **propietarios** (tareas de administrador)
  - **miembros** (tareas de colaborador)
  - **visitantes** (lector)

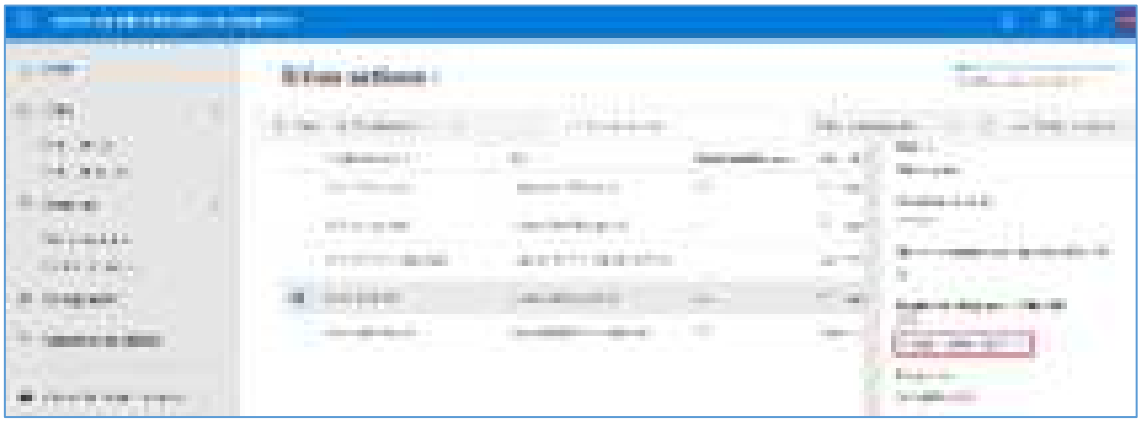
  Estos grupos son independientes de los grupos de Office 365 y Azure Active Directory (AD) y constituyen la base para asignar permisos a los recursos del sitio.

  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.



2. Pulsar el enlace “Agregar o quitar propietarios”.

- Para agregar un nuevo propietario basta con escribir el nombre.
- Para eliminar un propietario pulsar el “aspa” a la derecha del nombre.

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 Office 365, Exchange Online, Teams, etc.

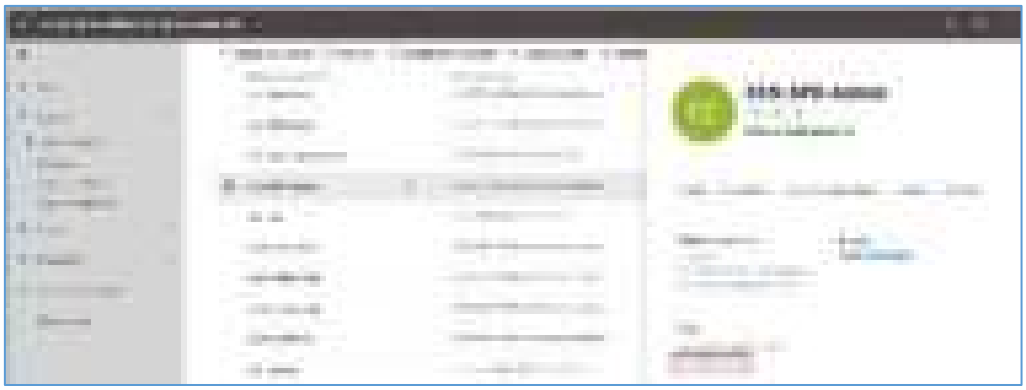
Para **proporcionar o restringir el acceso** de los usuarios a un sitio Sharepoint consultar el apartado [3.1.1.4 Proceso de gestión de derechos de acceso].

3.1.1.3 Segregación de funciones y tareas

Rol de administrador

Los administradores globales de Office 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 Office 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 seleccionar usuario.



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

Puede ser interesante asociar, junto con el rol de administrador de SharePoint, la función de **administrador de servicios**. De esta forma, puede ver información relacionada con el servicio en el *Centro de administración de Microsoft 365*: el estado del servicio de SharePoint Online, cambiar y publicar notificaciones, etc.

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 y mucho más.

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

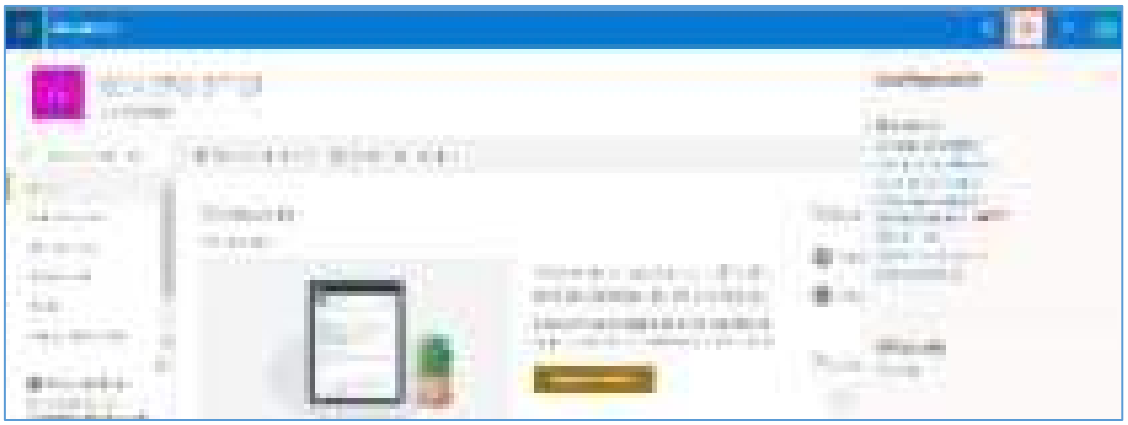
3.1.1.4 Proceso de gestión de derechos de acceso

Configurar permisos del sitio por un propietario

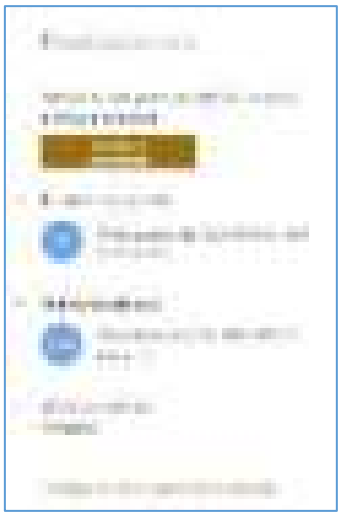
Después de crear un sitio de SharePoint, **se debe proporcionar o restringir el acceso** de los usuarios al sitio o a su contenido. Por ejemplo, puede proporcionarse acceso solo a los miembros de un equipo, o bien a todos los usuarios, pero restringir la edición

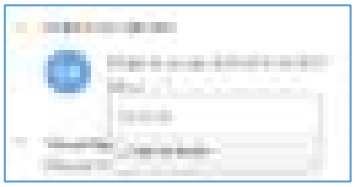
para algunos. La manera más sencilla de trabajar con permisos es usar los niveles de permisos y grupos predeterminados ofrecidos, que abarcan los escenarios más comunes.

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]:

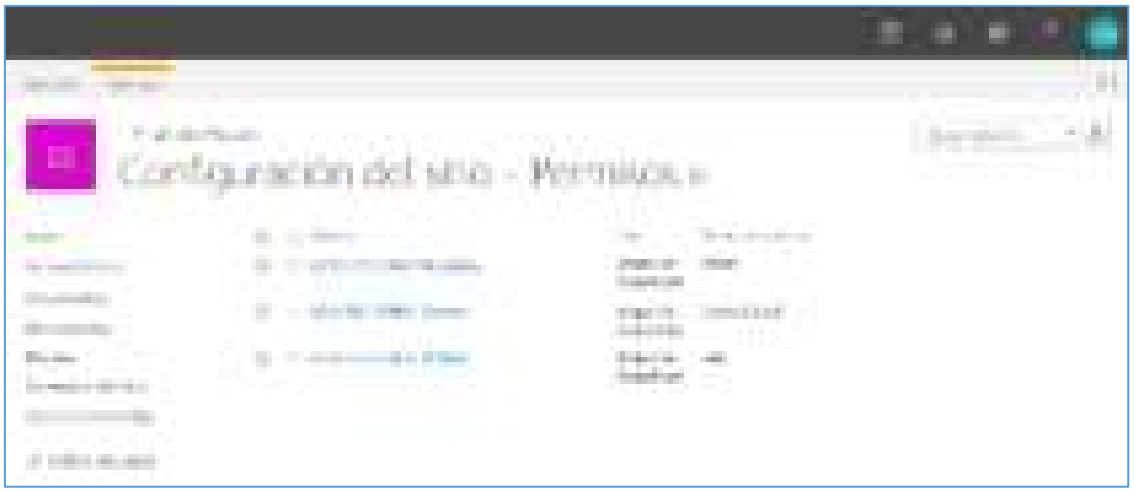


2. Desde aquí, un propietario puede invitar a nuevas personas y gestionar su nivel de permisos: propietario (control total), miembro (editor), visitante (lector).

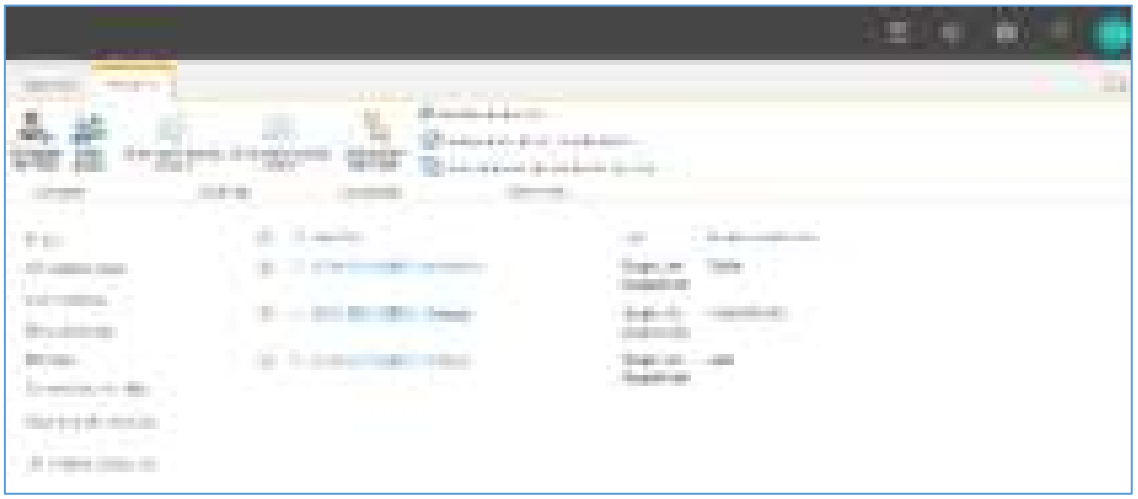




3. Clicar sobre el enlace "Configuración de permisos avanzada", para un control más exhaustivo de los permisos a aplicar.

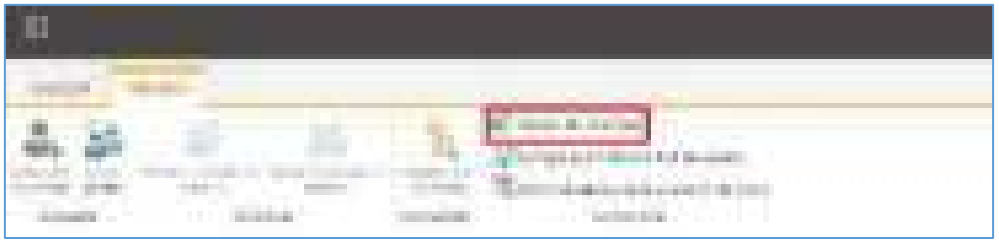


4. Pulsar en la pestaña de “PERMISOS” para acceder al menú de permisos.



5. 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.

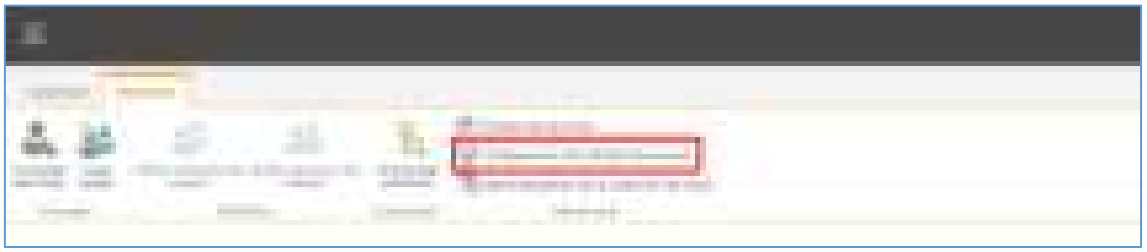
1. Pulsar el enalce “Agregar un nivel de permisos”.

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 "uso compartido externo", 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 elije quién puede solicitar acceso o invitar a otros a este sitio.

3.1.1.5 Mecanismos de autenticación

Los mecanismos de autenticación de Sharepoint Online son comunes a todas las aplicaciones de la solución Office 365 y 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:**

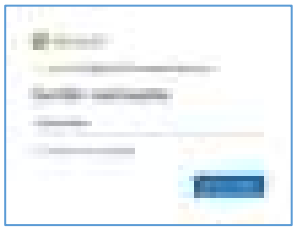
Se explica cómo funciona el escenario con el IdP (*Identity Provider*) predeterminado de Azure Active Directory (Azure AD).

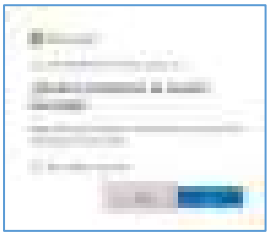
La cookie de *autenticación de Federación* (FedAuth) es para cada sitio de alto nivel de SharePoint Online, como el sitio raíz, *mySite* y el sitio de administración. La cookie de *autenticación de Federación raíz* (rtFA) se usa en todos los SharePoint Online. Cuando un usuario visita un nuevo sitio 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.

Azure AD muestra en 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.





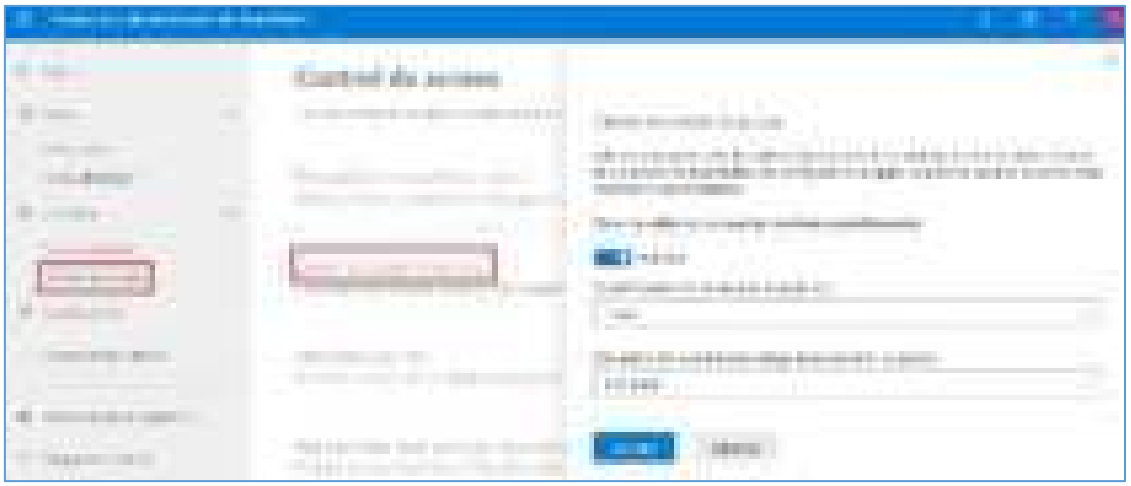
Ante la pregunta: ¿Quiere mantener la sesión iniciada? Responder: No.

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.

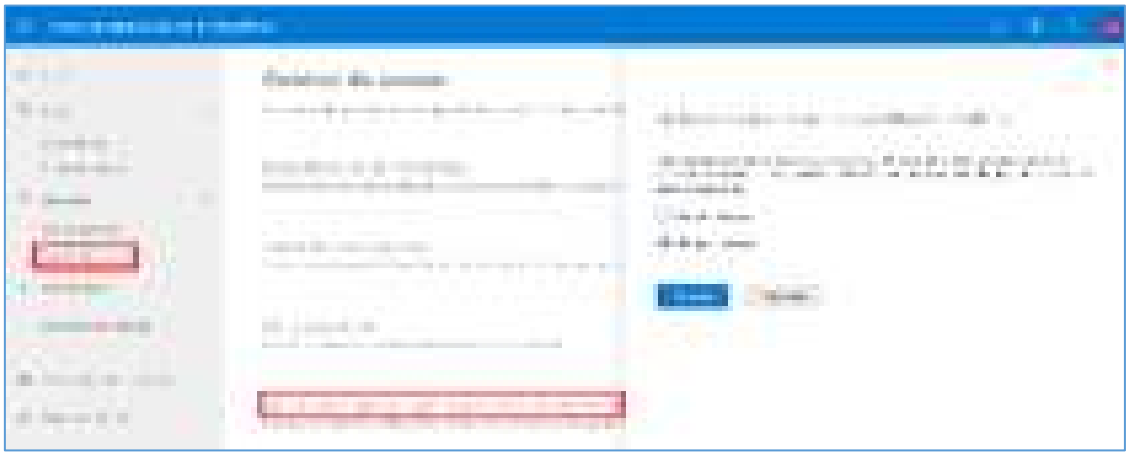
Se accede desde el *Centro de administración de Sharepoint*, menú [Control de acceso\Cierre de sesión inactiva].



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 [Control de acceso\Aplicaciones que no usan la autenticación moderna].



3.1.1.6 Acceso local

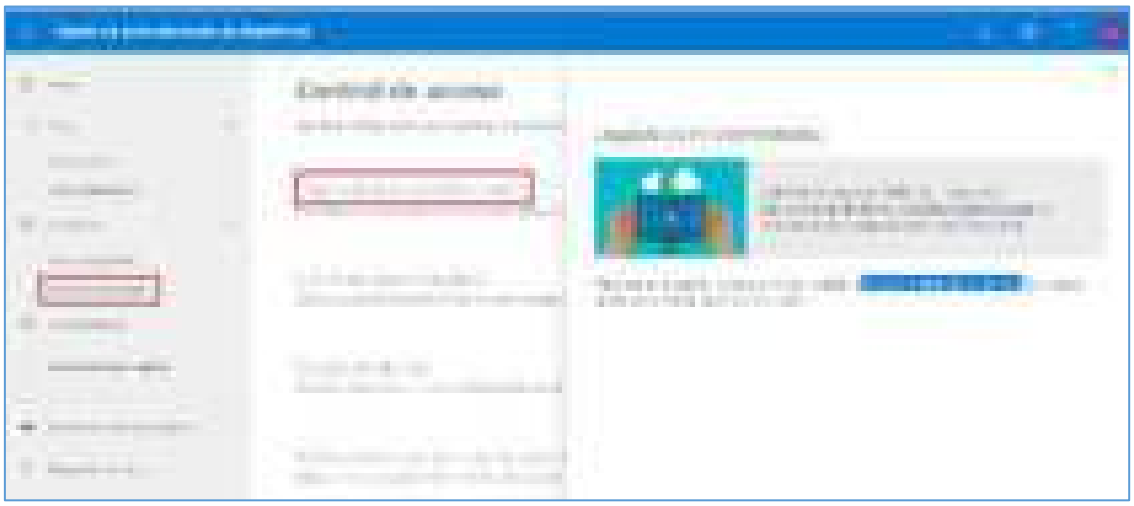
Se entiende como *acceso local* al acceso desde la red corporativa o sedes autorizadas.

Se requiere establecer un "doble factor de autenticación" (MFA) y tener una política adecuada de gestión de credenciales, que se describen en el apartado [3.1.1.5 Mecanismos de autenticación]. Así mismo, se requiere un registro de intentos de accesos con éxito y fallidos al sistema, descritos en el apartado [3.1.2.2 Registro de actividad]. Adicionalmente se puede controlar el acceso a Office 365 mediante directivas de acceso condicional o reglas en ADFS, como se describe en la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

Se puede controlar el acceso a SharePoint Online mediante directivas de acceso condicional por ubicación de red en *Centro de administración de SharePoint*, menú [Control de acceso\Ubicación de red].

También se puede limitar el acceso a dispositivos no administrados. Centro de administración de SharePoint, menú [Control de acceso\Dispositivos no administrados]. Se requiere una suscripción a *Enterprise Mobility + Security*.

Se pueden relajar las medidas de seguridad cuando el equipo está en alguna de las subredes corporativas.



3.1.1.7 Acceso remoto

El acceso remoto se entiende como acceso desde Internet (cualquier IP). Se recomienda reforzar la seguridad cuando se accede desde Internet (*solo equipos administrados*, *MFA*, *conformidad de dispositivos*, etc.).

Todo administrable desde el *Centro de administración de SharePoint*, menú [Control de acceso\Ubicación de red] y [Control de acceso\Dispositivos no administrados], como ya se ha comentado en secciones anteriores.

A destacar en este punto que Office 365 es una solución *cloud* accesible por el usuario final a través de internet. Se aplicará el cifrado de datos tal y como se describe en el

apartado [3.2.3.2 Cifrado] de la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

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 *Office 365 Advanced Threat Protection* (Office 365 ATP) 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.

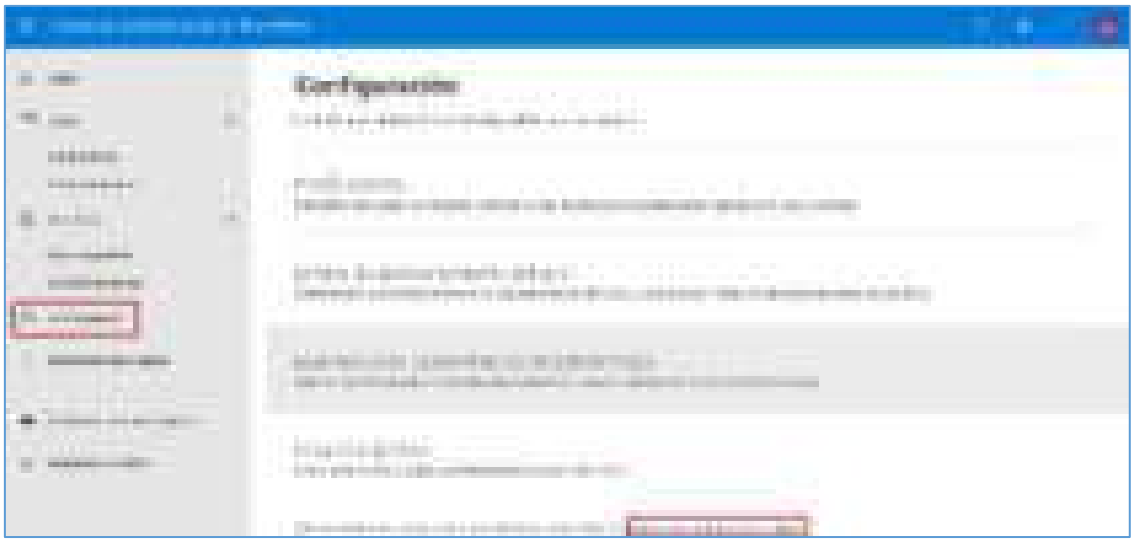
Una vez que permita el scripting, no se podrá identificar:

- 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”.



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

3.1.2.2 Registro de actividad

Para configurar el registro de actividad del servicio de Sharepoint, será necesario hacer uso de la funcionalidad de Auditoría disponible a través del *Centro de Seguridad y cumplimiento de Office 365*. Más información en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

3.1.2.3 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”.

3.2 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 Office 365 de manera automática. 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 Office 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 eliminará soporte de TLS 1.0 y 1.1. Esto tiene implicaciones directas en los clientes (https://docs.microsoft.com/en-us/office365/troubleshoot/security/prepare-tls-1.2-in-office-365).

3.2.2 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. Reseñamos algunas de ellas:

- Actividad de archivo de usuario externo inusual . Genera una alerta cuando un número inusualmente grande de actividades se realizan en archivos de SharePoint o en OneDrive por usuarios externos a la organización. Esto incluye actividades como obtener acceso a archivos, descargar archivos y eliminar archivos. Esta directiva tiene una configuración de gravedad alta.
- 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.
- Volumen inusual de eliminación de archivo. Genera una alerta cuando se elimina un número inusualmente grande de archivos en SharePoint o OneDrive en un breve período de tiempo. Esta directiva tiene una configuración de gravedad media.
- Campaña de *malware* detectada en SharePoint. Genera una alerta cuando se detecta un volumen inusualmente alto de *malware* o virus en los archivos ubicados en los sitios de SharePoint o en las cuentas de OneDrive de la organización. Esta directiva tiene una configuración de gravedad alta.

3.2.3 Protección de la información

3.2.3.1 Calificación de la información

Office 365 cuenta con diversos mecanismos para calificar la información, como se explican en el apartado [3.2.3.1 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.

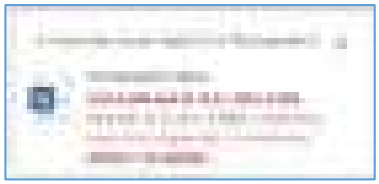
3.2.3.1.1 Etiquetas de retención

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.



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.

3.2.3.1.2 *O365 Sensitivity labels*

Esta característica está disponible, a fecha de edición de esta guía, en las **aplicaciones de escritorio** de Windows: Word, Excel, PowerPoint y Outlook, así como en aplicaciones de otras plataformas. Está prevista la disponibilidad en las aplicaciones web (Word, Excel, PowerPoint) a partir del cuarto trimestre de 2019.

¿Cómo se usan las sensitivity labels desde un documento?

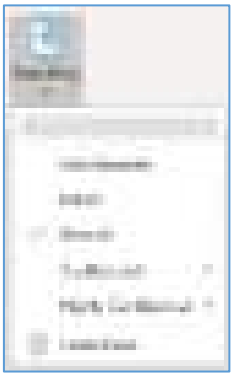
Para usar esta característica debe instalarse el cliente *Azure Information Protection* ***unified labeling***, tal y como se describen en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365].

Tras su instalación, aparecerá en las aplicaciones de escritorio el nuevo icono:

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

Importante: La *sensibilidad* no está visible si la cuenta de Office no es una cuenta profesional con una licencia de Office 365 E3 o E5 asignada, si el administrador no ha configurado *etiquetas de sensibilidad* y ha habilitado la característica, o si el otro cliente de *Azure Information Protection* se está ejecutando en Office.

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



Nota: Si la organización ha configurado un sitio web para obtener más información sobre sus *etiquetas de sensibilidad*, también se verá la opción más información...

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.*

¿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 *Information Rights Management* se puede aplicar al correo electrónico o documento.
- Puede aparecer un encabezado o pie de página en el documento o correo electrónico.
- Puede aparecer una marca de agua en el documento

3.2.3.2 Cifrado

Consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365] para ver el mecanismo de cifrado genérico de Office 365, específicamente el cifrado de **datos en reposo** y **en tránsito**.

En cuanto al cifrado en reposo

El cifrado en reposo incluye dos componentes: cifrado de nivel de disco de BitLocker y cifrado por archivo del contenido del cliente. Este cifrado es transparente para el usuario y es implementado **automáticamente** por Microsoft.

BitLocker se implementa para *OneDrive For Business* y *SharePoint Online* en todo el servicio. El cifrado por archivo también se encuentra en *OneDrive For Business* y SharePoint Online en Office 365 *multitenant* y en entornos dedicados nuevos que se basan en tecnología multiempresa.

Mientras que BitLocker cifra todos los datos en un disco, el cifrado por archivo va más allá al incluir una clave de cifrado única para cada archivo. Además, la actualización de cada archivo se cifra mediante su propia clave de cifrado. Antes de almacenarse, las claves del contenido cifrado se almacenan en una ubicación físicamente independiente del contenido. Cada paso de este cifrado usa el Estándar de cifrado avanzado (AES) con claves de 256 bits y cumple el Estándar federal de procesamiento de información (FIPS) 140-2. El contenido cifrado se distribuye entre varios contenedores en el centro de datos y cada contenedor tiene credenciales exclusivas. Estas credenciales se almacenan en una ubicación física independiente del contenido o de las claves de contenido.

Aplicar *etiquetas de sensibilidad* de Office365

Aplicar *Etiquetas de sensibilidad de Office 365* para proteger y cifrar los archivos en un sitio de grupo de SharePoint Online altamente sensible. Para más información, ver el apartado [3.2.3.1 Calificación de la información] de la presente guía.

*Alternativamente puede usarse Azure Information Protection (AIP) aunque recomendamos la opción anterior.

Aplicar Information Rights Management (IRM) en bibliotecas

Además de poder aplicar etiquetas individualmente a documentos en donde es el usuario el responsable de aplicarlas o no, se puede configurar IRM directamente en las bibliotecas documentales. De esta forma, cuando se sube un documento, se cifra y se protege automáticamente, aunque el usuario no haya aplicado ninguna etiqueta. Consideramos importante esta funcionalidad para la seguridad de documentos.

*Para *SharePoint Online*, los usuarios pueden experimentar tiempos de espera al descargar los archivos más grandes protegidos por IRM. Si es así, es mejor aplicar la protección IRM mediante el uso de los programas de Office y almacenar archivos de mayor tamaño en una biblioteca de SharePoint que no utilice IRM.

* Para activar el servicio Azure Rights Management, debe disponer de un plan Premium de Azure Information Protection o de un plan de Office 365 que incluya

Rights Management. Por ejemplo, su organización tiene un plan de Office 365 E3 u Office 365 E5.

Para activar *Rights Management* desde el *Centro de administración de Microsoft 365*, acceder a la página de configuración clásica:

A continuación, activar el servicio de IRM:

Una vez activado el servicio a nivel de *tenant*, ya es posible aplicarlo a nivel de biblioteca.

1. En la pantalla de configuración de la biblioteca aparecerá ahora la opción "Information Rights Management (IRM)".

2. Definir las características de IRM:

3.2.3.3 Limpieza de documentos

Al compartir una copia electrónica de determinados documentos de Office365 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.

3.2.3.4 Copias de Seguridad

No existe una solución global de respaldo de Office 365. 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.

Aunque un mecanismo basado en "políticas de retención" en ciertos casos puede resultar suficiente para garantizar el respaldo de la información. Consultar el apartado [3.2.3.1 Calificación de la información] para ver cómo se aplican a un documento y cómo puede servir para protegerlo de ser eliminado.

3.2.3.5 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:

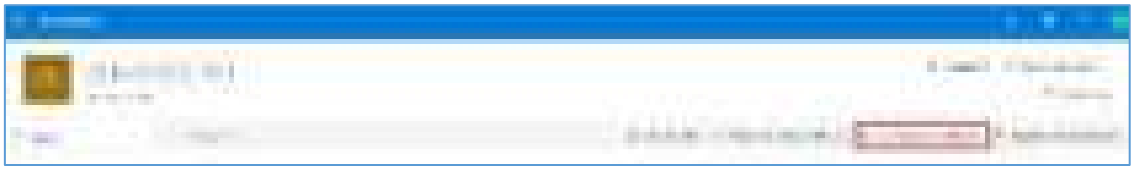
- Crear una *directiva de administración de información* para usar en varios tipos de contenido dentro de una colección de sitios.
- Crear una *directiva de administración de información* para un tipo de contenido de sitio.
- Crear una *directiva de administración de información* para una lista o biblioteca.

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:

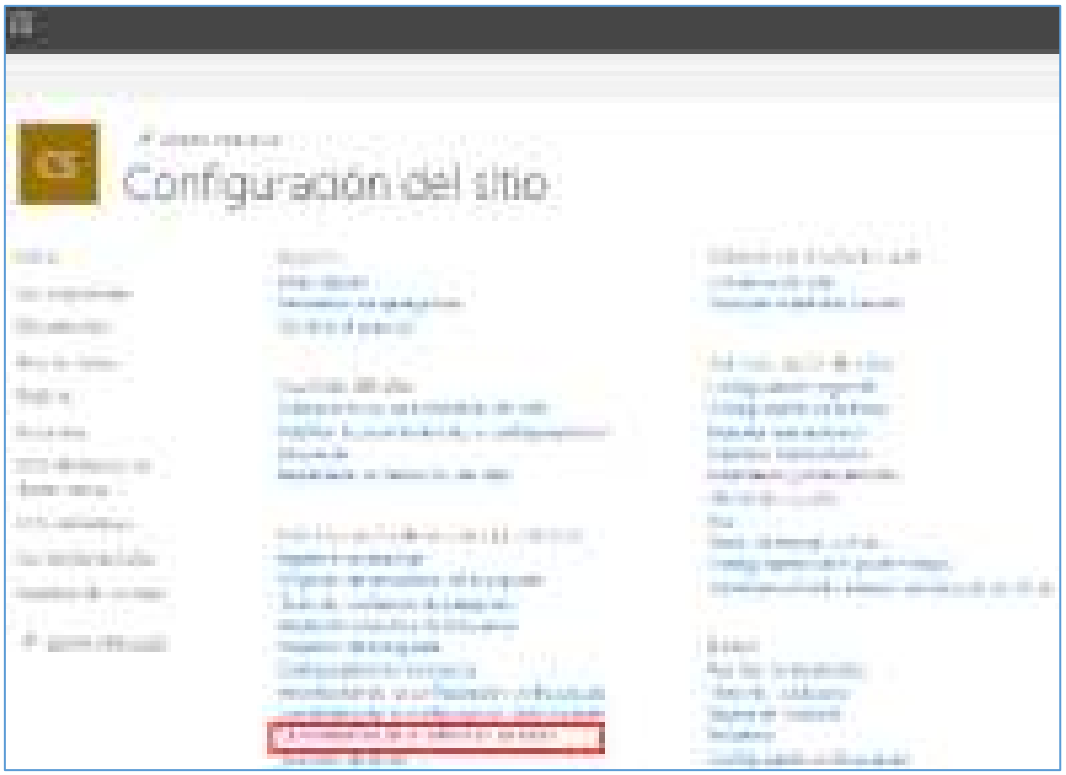
https://support.office.com/es-es/article/crear-y-aplicar-directivas-de-administraci%C3%B3n-de-informaci%C3%B3n-eb501fe9-2ef6-4150-945a-65a6451ee9e9

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

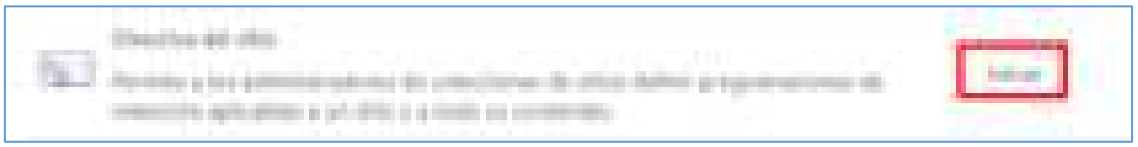
1. Acceder a la página principal del sitio y pulsar el icono "Configuración del sitio".



2. En "Administración de la colección de sitios", seleccionar "Características de colección de sitios".

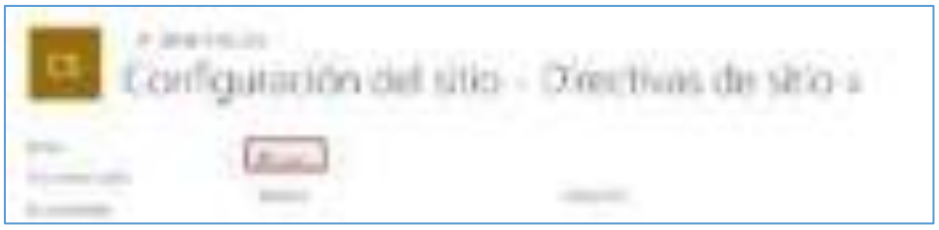


3. En la pantalla de características del sitio, navegar hasta “Directiva del sitio”, y activarlo.



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

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

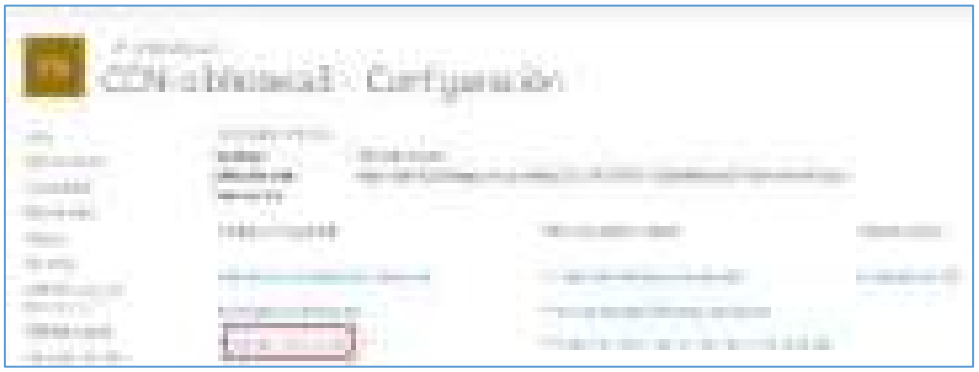


5. Establecer la política de retención adecuada.

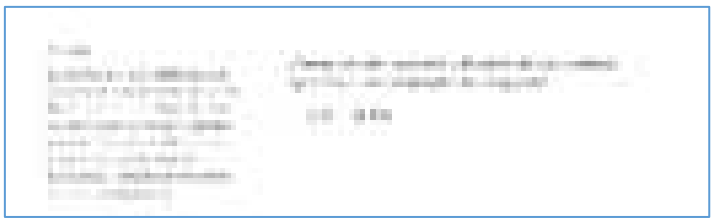
3.2.3.6 Evitar que una biblioteca se muestre en los resultados de búsqueda

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].



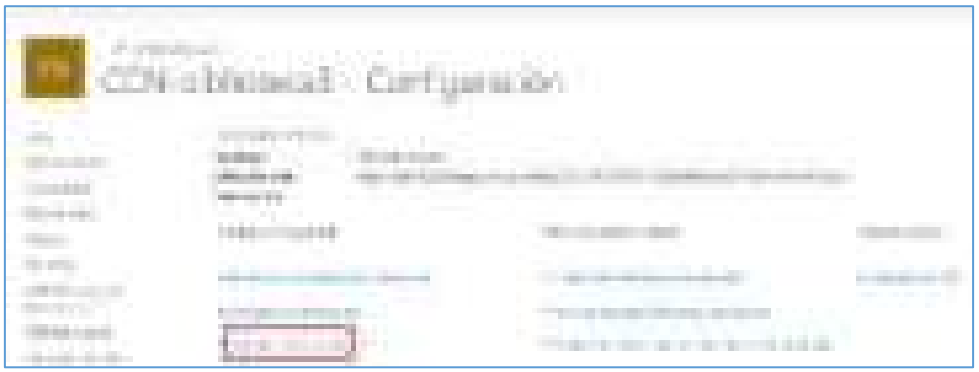
2. Desactivar la búsqueda.



3.2.3.7 Evitar que se 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.

3.2.4 Protección de los servicios

3.2.4.1 Protección frente a la denegación de servicio

Office 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 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="<the full email address of a SharePoint administrator account, example:
    jdoe@contosotoycompany.onmicrosoft.com>"

#   $orgName="<name of your Office 365 organization, example: 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="<name of your Office 365 organization, example: 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.

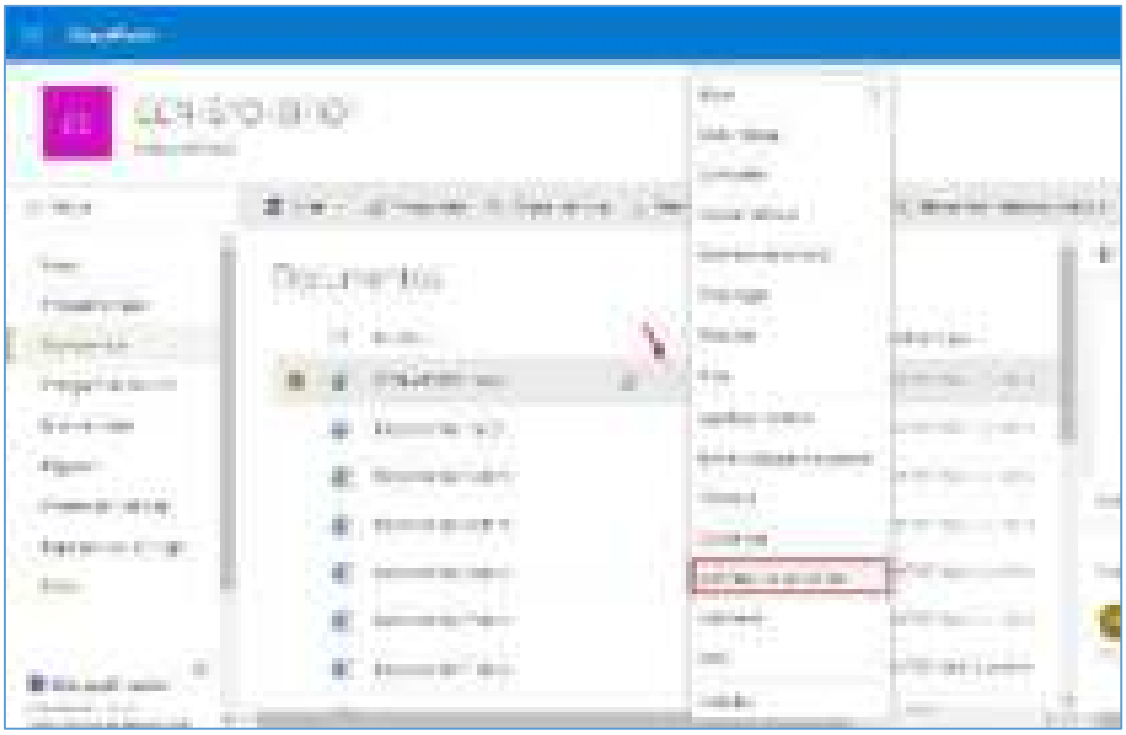
Habilitar y configurar las versiones para una lista o biblioteca

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

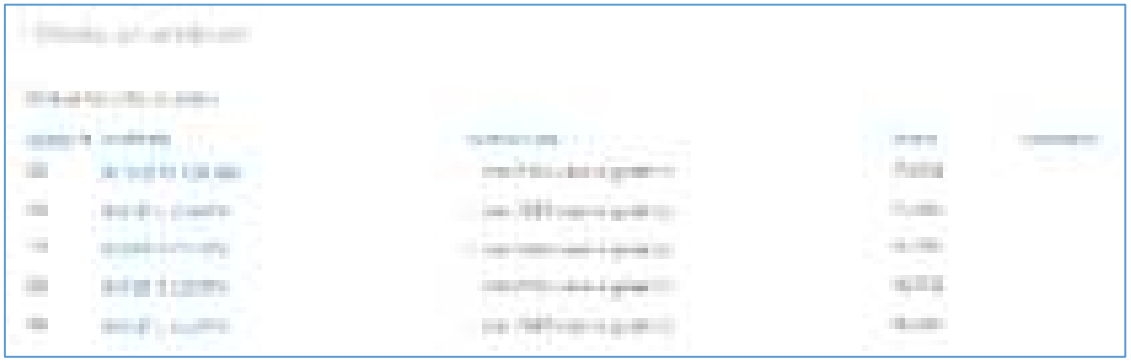
2. Configurar las opciones.

Consultar el historial de versiones

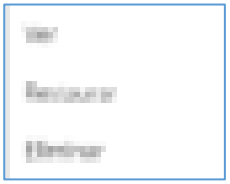
1. Se accede a través del [menú de acciones] que aparece en la propia línea del documento a consultar.



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



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

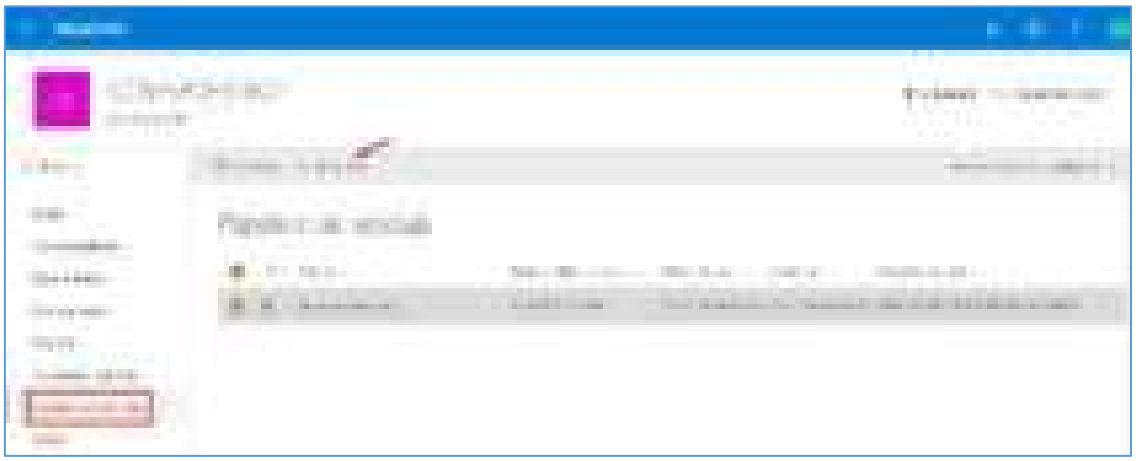


5.2 Papelera de reciclaje

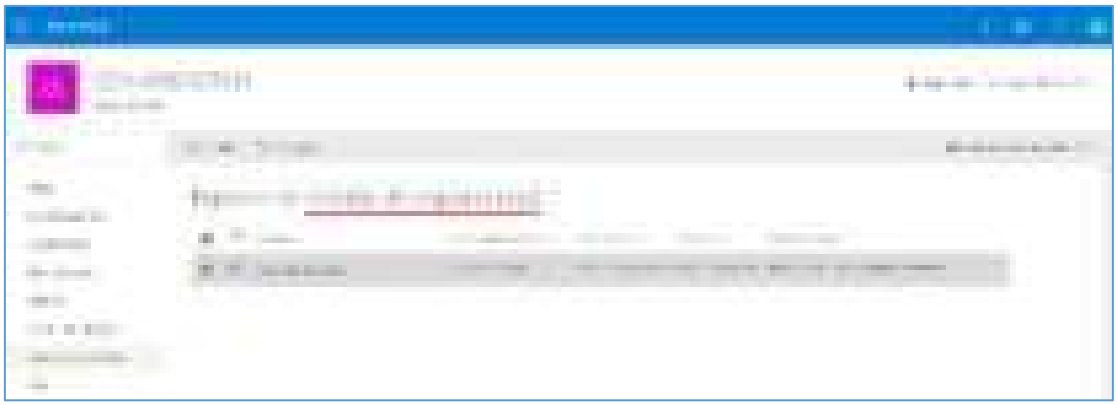
Sharepoint Online establece dos niveles de papelera de reciclaje con dos áreas de almacenamiento independientes, cada una con un período de retención de la información. A diferencia de versiones anteriores no es configurable.

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

1. 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.



2. 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.

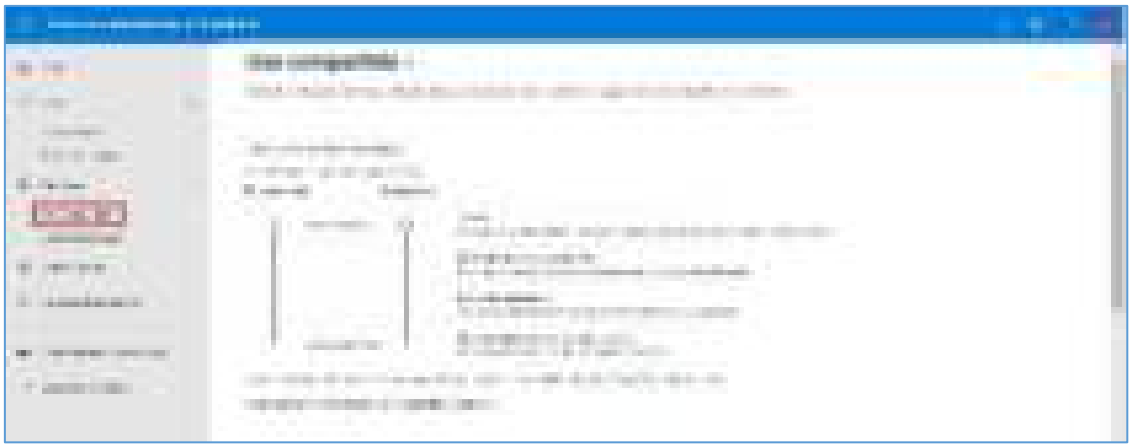
3. Tercer nivel de copia de seguridad.

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 Office 365 pueden cambiar su configuración de uso compartido de nivel de organización para SharePoint y OneDrive.

Para ello acceder al C*entro de administración de Sharepoint Online:*

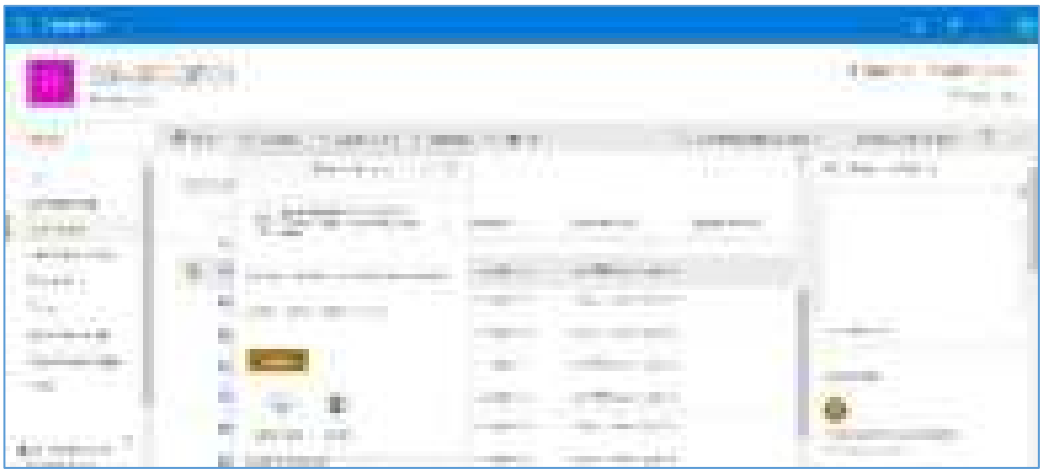


Los niveles establecidos son:

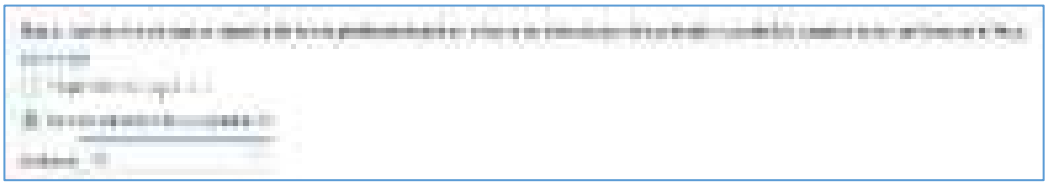
Todos	Los usuarios pueden compartir archivos y carpetas con vínculos que no requieren inicio de sesión.
Invitados nuevos y existentes	Los invitados deben iniciar sesión o proporcionar un código de verificación.
Invitados existentes	Solo los invitados que ya forman parte del directorio de su organización.
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.

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



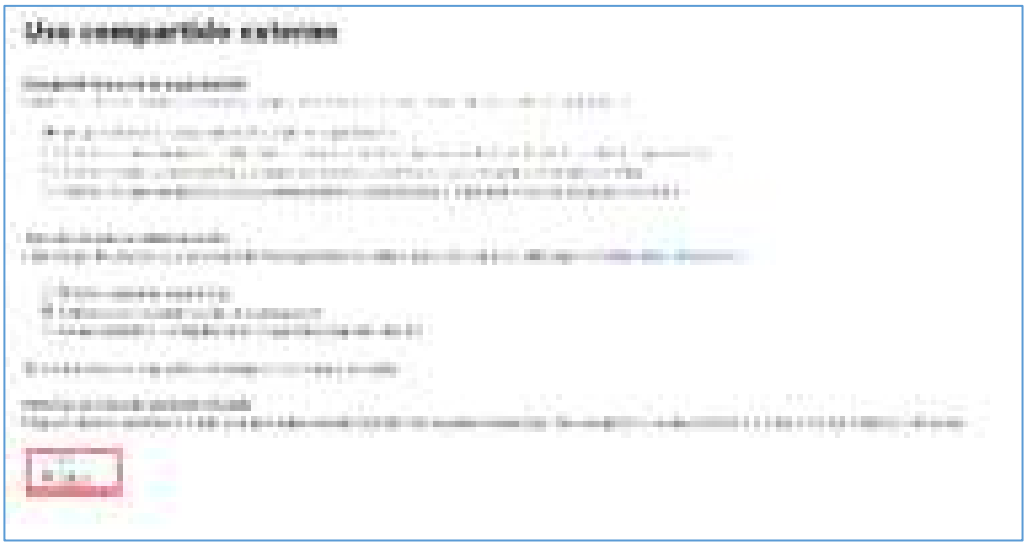
3. Elegir tipo de vínculo.



4. Seleccionar otras opciones de configuración.

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

Cualquiera de esos vínculos redirige a una página para poder seleccionar esa opción, así como otros parámetros ya seleccionados anteriormente.

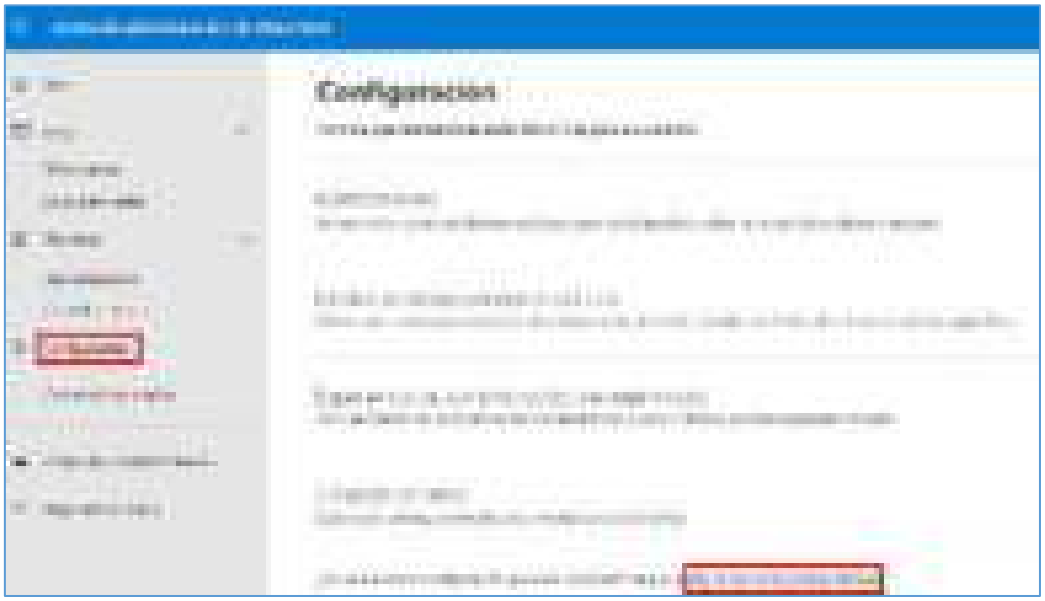


5.4 Bloquear la integración con Yammer

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 Office 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*.



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

6. GLOSARIO Y ABREVIATURAS

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

Término	Definición
IRM	*Information Rights Management.*
SPO	*Sharepoint Online*
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.

<table>
<tr><th>Control ENS</th><th>Configuracion</th><th colspan="2">Estado</th></tr>
<tr><td>op</td><td colspan="3">Marco Operacional</td></tr>
<tr><td>op.acc</td><td colspan="3">Control de Acceso</td></tr>
<tr><td rowspan="3">op.acc.1</td><td colspan="3">Identificación</td></tr>
<tr><td rowspan="2">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]</td><td>Aplica:
☐ Si ☐ No</td><td>Cumple:
☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Si ☐ No</td><td>Observaciones:</td></tr>
<tr><td>Op.acc.2</td><td colspan="3">Requisitos de Acceso</td></tr>
</table>

	Se han comprobado los *niveles de permisos* 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:**

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**		
	Se ha informado a los usuarios que mantengan deshabilitadas las *cookies* persistentes en el inicio de sesión.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

Op.acc.5	**Mecanismo de autenticación**		
	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**		
	Se ha bloqueado el acceso a aplicaciones que no usan la autenticación moderna.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

Op.acc.6	**Acceso local**		
	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.6	**Acceso local**		
	Se han configurado directivas de acceso condicional o reglas en ADFS, como se describe 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.6	**Acceso local**		
	Se ha activado la *Ubicación de red* 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.7	**Acceso remoto**		
	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
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.exp	**Explotacion**		
op.exp.6	**Protección frente a código dañino**		
	Se ha bloqueado que los usuarios puedan ejecutar scripts personalizados en sitios personales y en sitios creados por ellos mismos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ 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 *Centro de Seguridad y cumplimiento de Office 365*. *Para dichas tareas la organización debe dispone de *Office 365 Advanced Threat Protection* (Office 365 ATP).	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.exp.8	**Registro de la actividad de los usuarios**		
	Se ha activado el registro de auditoría.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.10	**Protección de los registros de actividad**		
	Se ha securizado la consulta del registro de actividad mediante el establecimiento de los roles adecuados.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

op.mon	**Monitorización del sistema**		
	Se han configurado alertas en el *Centro de Seguridad y cumplimiento de Office 365.*	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp	**Medidas de Protección**		
mp.info	**Protección de la información**		
mp.info.2	**Calificación de la información**		
	Se han aplicado políticas de retención.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ 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 3.2.3.1 Calificación de la información de la guía [CCN-STIC-884A - Guía de configuración segura para Azure].	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.info.2	**Calificación de la información**		
	Se han aplicado *sensitivity labels.*	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No	
mp.info.3	**Cifrado**		
	Se ha aplicado un cifrado especial mediante etiquetas de sensibilidad a sitios de Sharepoint que precisan una protección especial. * Microsoft cifra automáticamente los datos en reposo y de manera transparente para el usuario. Para un cifrado adicional se pueden usar las *sensitivity labels*.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
mp.info.3	**Cifrado**		
	Se ha aplicado IRM en bibliotecas documentales que precisen una protección adicional.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No	
mp.info.6	**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. Cómo se describe en el apartado 3.2.3.3 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.9	**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
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No	
mp.info.9	**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
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No	
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.8	**Protección frente a la denegación de servicio**		
	Se ha tenido en cuenta la información detallada en la guía [CCN-STIC-884A - Guía de configuración segura para Azure] sobre el *sistema de defensa DDoS de Azure*.	**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:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
	Integración con Yammer		
	Se ha bloqueado la integración con Yammer	**Aplica:** Si No	**Cumple:** Si No

		☐ ☐	☐ ☐
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**