Guía de Seguridad de las TIC
CCN-STIC 885D

Guía de configuración segura para Microsoft Teams

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
2020.02.26 13:25:22 +01'00'

NIPO: 083-19-263-7
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. MICROSOFT TEAMS

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 *Microsoft Teams* 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

Microsoft Teams es un espacio de trabajo basado en chat de Office 365 diseñado para mejorar la comunicación y colaboración de los equipos de trabajo de las empresas, reforzando las funciones colaborativas de la plataforma en la nube, 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*.

Microsoft Teams ofrece la posibilidad de utilizar las aplicaciones de Office 365, personalizando el entorno según las necesidades de tu equipo. Con Teams los usuarios de un equipo pueden:

- Realizar chats de grupo o privados para mantener conversaciones de grupo con pocos miembros.
- Ver el contenido y el historial de chat en cualquier momento.
- Iniciar reuniones de vídeo o voz gracias a la integración de *Skype empresarial*.
- Obtener acceso instantáneo a todo el contenido, las herramientas de colaboración, los usuarios y las conversaciones a través de pestañas.
- Agregar acceso rápido a los documentos, a los sitios web y a las aplicaciones que se usen con frecuencia.
- Acceso a notas y documentos gracias a la integración con *OneNote* y *SharePoint*.
- Trabajar con documentos de Office Online directamente desde Teams.
- Planificar tareas gracias a la integración con *Planner*.
- Agregar informes de *Power BI*.

- Disfrutar de un espacio común de trabajo con interfaz web y para dispositivos móviles.
- Al estar basado en grupos permite al usuario moverse de una plataforma de colaboración a otra fácilmente.
- Agregar conectores que permiten integrar aplicaciones como Yammer y servicios de terceros, como por ejemplo: RSS, Canal de noticias de Bing o Twitter.
- Crear una integración personalizada con interfaces de programación de aplicaciones y otras herramientas de desarrollo.

1.3 Prerrequisitos para el despliegue mediante PowerShell

PowerShell de Office 365 permite gestionar y configurar *Microsoft Teams* 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].

Los comandos para administrar Teams se encuentran en dos módulos diferentes:

- **Módulo PowerShell de Microsoft Teams**: contiene los cmdlets necesarios para crear y manejar equipos.

  Para instalarlo, abrir una versión de PS en modo administrador:

```
#   Install-Module -Name MicrosoftTeams

#   Install-Module -name MicrosoftTeams -AllowClobber
```

- **Módulo PowerShell de Skype for Business**: contiene los cmdlets para manejar políticas, configuraciones y otras herramientas de Teams.
  1. Localizar el módulo en el “Centro de Descargas” de Microsoft:

     https://www.microsoft.com/en-us/download/details.aspx?id=39366

  2. Descargar el archivo “SkypeOnlinePowerShell.exe” y ejecutar.

Para conectarse al módulo de Microsoft Teams:

```
#   Connect-MicrosoftTeams
```

Para consultar los *teams* (equipos) creados:

```
#   get-team
```

2. DESPLIEGUE DE MICROSOFT TEAMS

Microsoft Teams 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].

Microsoft Teams, 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 *Microsoft Teams* a través del portal de administración de Office 365 (portal.office365.com).

Al pulsar en el icono de Teams se accede al *Centro de administración de Microsoft Teams*.

En el menú [Configuración de toda la organización] se controla la configuración de usuario de toda la organización. A continuación se describen las más relevantes desde el punto de vista de la seguridad.

Acceso externo

Acceso externo permite que los usuarios de *Teams* y *Skype Empresarial* se comuniquen con usuarios de fuera de la organización o dominio. Menú [Configuración de toda la organización\Acceso externo].

El acceso externo se utiliza cuando:

- Existen usuarios en diferentes dominios de la organización.
- Se necesita que personas de la organización usen Teams para ponerse en contacto con personas de empresas específicas de fuera de la organización.

1. En la pantalla anterior, pulsar "+ Agregar un dominio" para agregar dominios permitidos o bloqueados.

   De forma predeterminada, la organización puede comunicarse con todos los dominios externos. Si se agregan dominios bloqueados, se permitirán todos los demás dominios. No obstante, si se agregan dominios permitidos, se bloquearán todos los demás dominios.

2. Añadir dominios a la lista de bloqueados o permitidos.

2.1. Escribir el nombre del dominio.
2.2. Seleccionar la acción.
2.3. Pulsar “Listo”.

Así se van añadiendo los dominios individualmente.

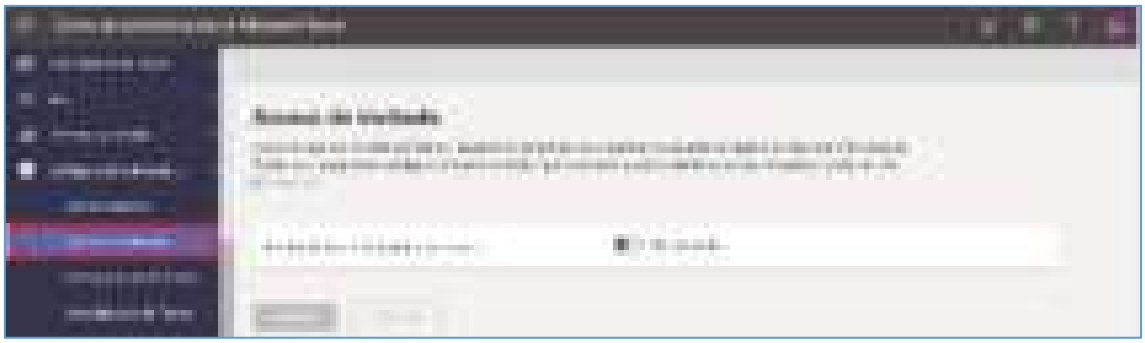
Es importante restringir los dominios externos, desde el punto de vista de la seguridad, para evitar que usuarios de otras organizaciones puedan ponerse en contacto con miembros de nuestra organización.

Con esta configuración, también se controlará el acceso de los usuarios a otras organizaciones. La capacidad de comunicarse con usuarios de otras organizaciones es un elemento fundamental en Teams, por lo tanto, se recomienda mantener una lista de dominios autorizados o bloqueados, y mantener adecuadamente dicha lista a lo largo del tiempo.

Acceso de invitado

Con el acceso de invitados se permite que personas que no pertenecen a la organización se les conceda acceso a *equipos* y *canales* en uno o más espacios empresariales. Todo contacto que tenga una cuenta de correo electrónico (como Outlook o Gmail u otros) puede participar como invitado en Teams con acceso total a los chats, las reuniones y los archivos del equipo.

Se accede a través del menú [Configuración de toda la organización\Acceso de invitado].



El acceso de invitado **se encuentra desactivado de forma predeterminada**, y se recomienda no activarlo salvo que sea necesario.

Todos los *invitados* de Teams están protegidos con el mismo cumplimiento de normativas y auditorías que el resto de Office 365, y se pueden administrar de forma segura dentro de Azure AD.

Diferencias entre el acceso de invitado y acceso externo

- Acceso de invitado concede permiso de acceso a una persona. Acceso externo concede permiso de acceso a un dominio completo.
- El acceso de invitados, una vez otorgado por el propietario de un equipo, permite que un invitado tenga acceso a recursos, como archivos y debates de canales, para un equipo específico y conversar con otros usuarios del equipo al que han sido invitados.
- Con el acceso externo (chat federado), los participantes del chat externo no tienen acceso a los equipos de la organización o a los recursos del equipo. Solo pueden participar en un chat federado (one-on-one).
- Los administradores del tenant pueden elegir entre las dos opciones de comunicación dependiendo del nivel de colaboración que sea deseable con la parte externa. Los administradores pueden elegir entre dos enfoques o ambos, según las necesidades de la organización.

En la siguiente tabla se muestra una comparativa de las características de ambos:

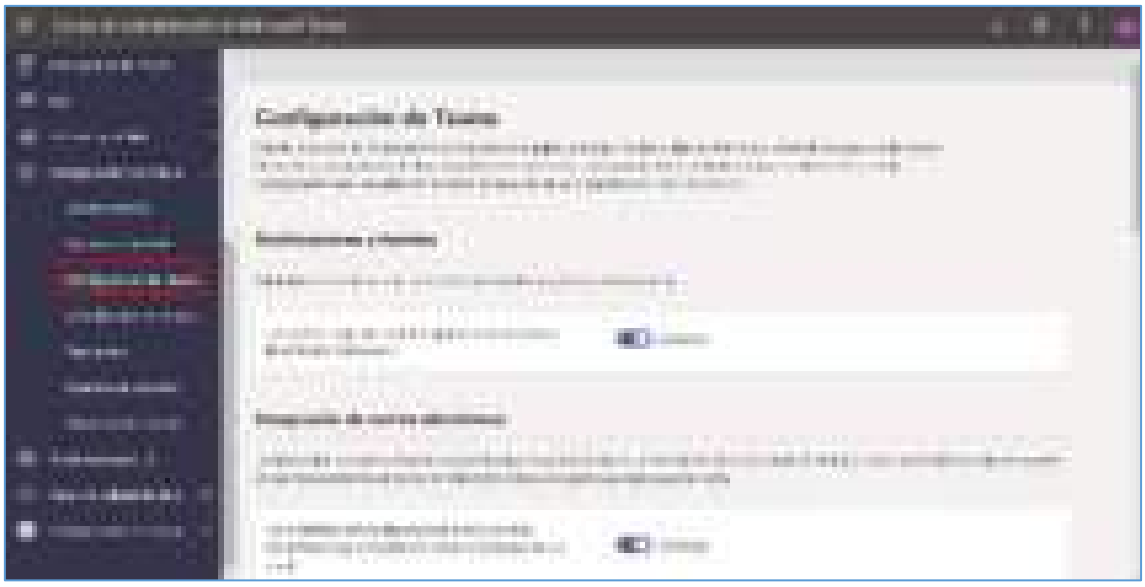
Característica	**Usuarios de acceso externo**	**Usuarios de acceso de invitado**
El usuario puede chatear con alguien de otra empresa	Sí	Sí
El usuario puede llamar a alguien de otra empresa	Sí	Sí
El usuario puede ver si alguien de otra empresa está disponible para realizar llamadas o chats	Sí	Sí[1]

El usuario puede buscar usuarios en *tenants* externos	Sí[2]	No
El usuario puede compartir archivos	No	Sí
El usuario puede acceder a los recursos de Teams	No	Sí
Se puede Agregar un usuario a un chat grupal	No	Sí
Se puede Agregar un usuario a una reunión	Sí	Sí
Se pueden agregar usuarios adicionales a un chat con un usuario externo	No[3]	N/D
Se muestra la presencia	Sí	Sí
Se muestra un mensaje de fuera de la oficina	No	Sí
Usuario individual puede bloquearse	No	No
@mentions son soportadas	No	Sí
Hacer llamadas privadas	Sí	Sí
Permitir video IP	Sí	Sí
Modo de uso compartido de pantalla	No	Sí
Permitir “reunirse ahora	No	Sí
Editar mensajes enviados	No	Sí
Puede eliminar mensajes enviados	No	Sí

[1] siempre que el usuario se haya agregado como invitado y haya iniciado sesión como invitado para el inquilino invitado.
[2] solo por correo electrónico o dirección de protocolo de inicio de sesión (SIP).
[3] el chat externo (federado) solo es 1:1.

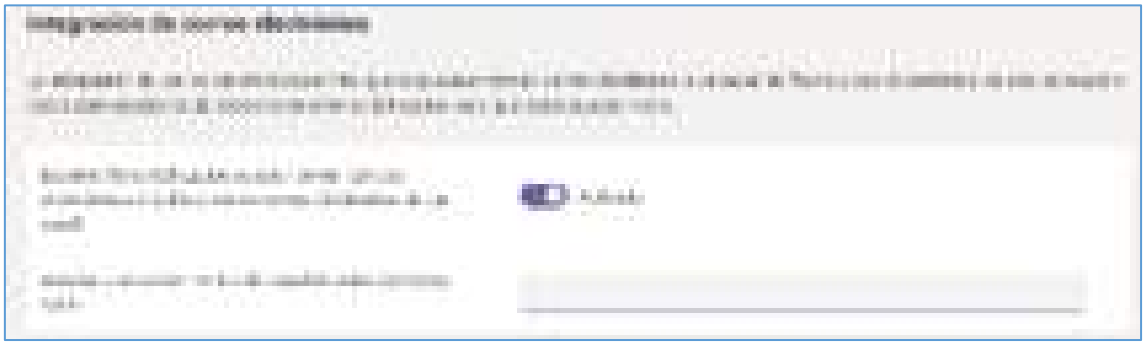
Configuración de toda la organización

En el menú [Configuración de toda la organización\Configuración de Microsoft Teams] se puede controlar qué características están disponibles para los usuarios de la organización, incluyendo notificaciones y fuentes, integración de email, opciones de almacenamiento en la nube, y dispositivos.



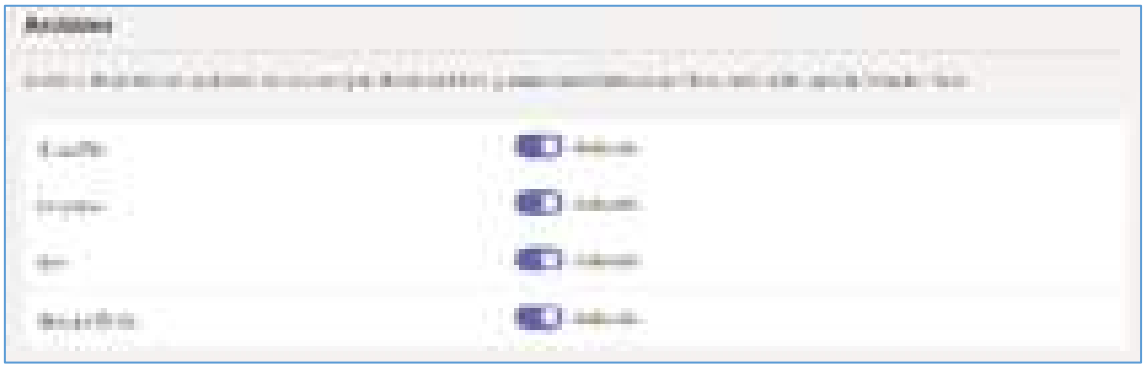
Integración de correo electrónico

Activar esta característica para que los usuarios puedan enviar un correo electrónico a un canal en Microsoft Teams mediante la dirección de correo electrónico del canal.



Archivos

Aquí se pueden activar o desactivar las opciones de uso compartido de archivos y de almacenamiento de archivos en la nube.



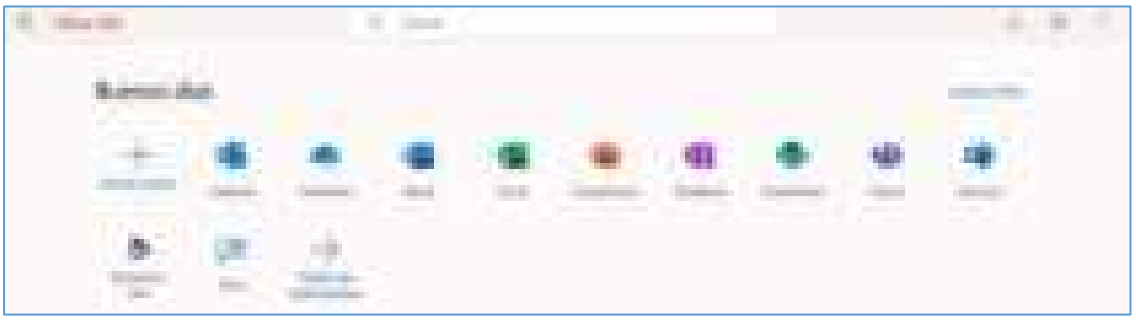
Los usuarios pueden cargar y compartir archivos de los servicios de almacenamiento en nube en los canales y chats de Teams. Las opciones de almacenamiento en nube en Microsoft Teams actualmente incluyen ShareFile, Dropbox, Box y Google Drive. Activar

el conmutador de los proveedores de almacenamiento en la nube que quiera usar la organización.

Nota: Como recomendación conviene habilitar únicamente aquellos servicios de almacenamiento en nube que hayan sido aprobados y estén controlados por la organización. De lo contrario, existe el riesgo de almacenar información sensible en proveedores externos no controlados por las directivas de la organización.

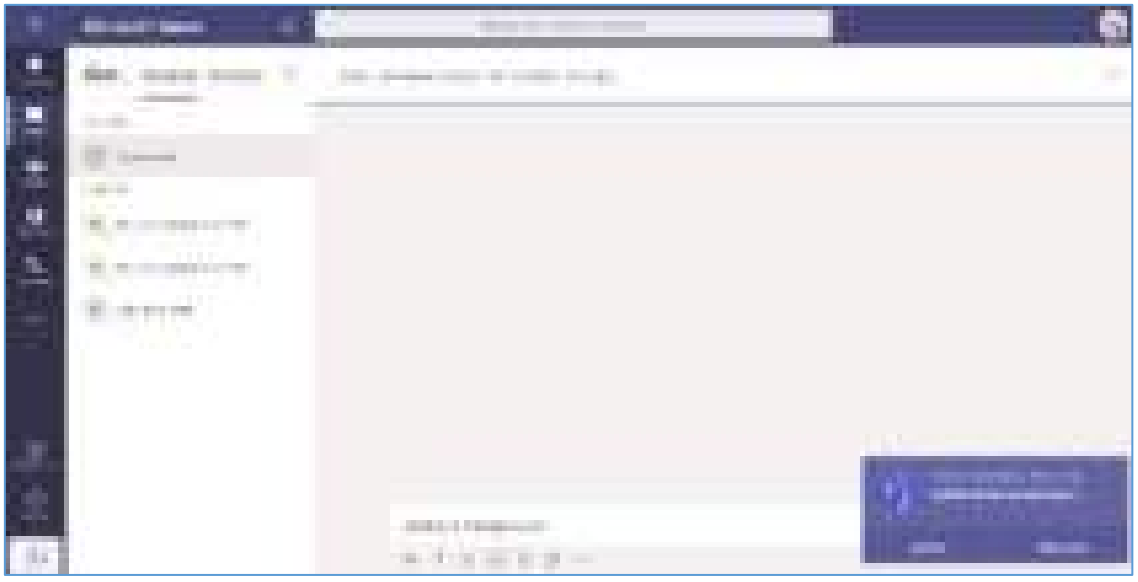
2.2 *Usuario final - primeros pasos*

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 Teams para acceder al portal de *Microsoft Teams* (https://teams.microsoft.com).



Las distintas opciones que se presentan en el menú de usuario son:

Actividad: comentarios y repuestas que ha hecho cada miembro del equipo sobre algún tema. Para mostrar solamente las del propio usuario se debe seleccionar la opción “Mi actividad”.

Chat: para establecer nuevas conversaciones con cualquier miembro de la organización o bien reanudar conversaciones.

Equipos: lista de canales, que son secciones que pueden crearse dentro de un *equipo*. Se pueden organizar los canales por temas, departamentos o proyectos.

Calendario: todas las reuniones y compromisos planificadas del usuario. Al dar clic podrán ver su agenda completa.

Llamadas: muestra opciones de marcación rápida, lista de contactos e historial de llamadas y correo de voz.

Archivos: vistas de los archivos accedidos por el usuario o alguno de los miembros de los equipos con los que trabaja.

Aplicaciones: acceso a las distintas aplicaciones integradas en Teams.

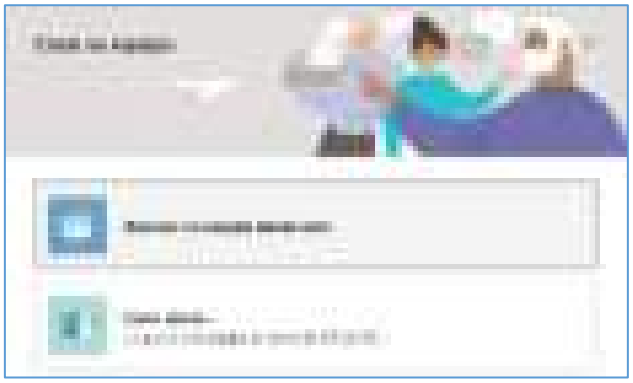
Creación de un equipo

Los equipos son recopilaciones de personas, contenido y herramientas alrededor de varios proyectos y tareas dentro de una organización.

- Los equipos pueden crearse para ser privados, solo para los usuarios invitados.
- Los equipos también se pueden crear como públicos y abiertos, de modo que todos los integrantes de la organización se pueden unir (hasta 5 000 miembros).

Además puede crearse un equipo desde cero, o partiendo de un grupo existente en Office 365.

Pulsar el botón de "Crear equipo", y elegir si se crea el equipo *desde cero*, o *desde un grupo existente* en Office 365.

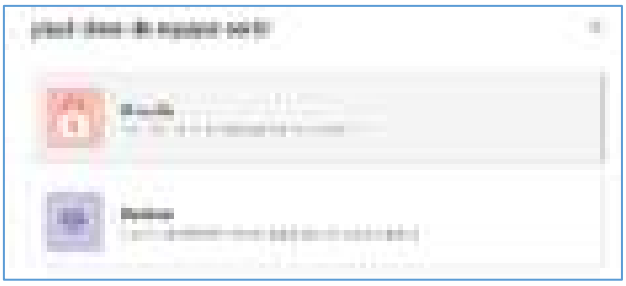


Crear un equipo desde cero

Cuando se crea un equipo, esto es lo que se crea:

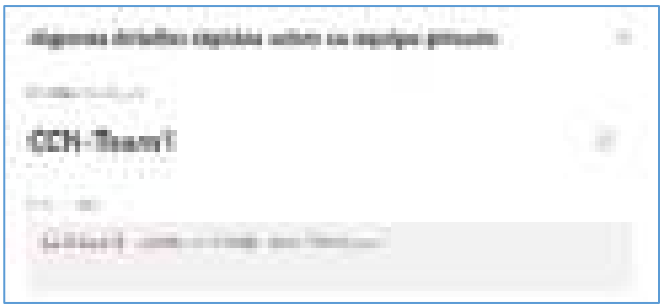
- Un nuevo grupo de Office 365.
- Un sitio de SharePoint Online y la biblioteca de documentos para almacenar los archivos del equipo.
- Un buzón y un calendario compartidos de Exchange Online.
- Un bloc de notas de OneNote.
- Relaciones con otras aplicaciones de O365, como Planner y Power BI.

1. Pulsar el botón "Generar un equipo desde cero".
2. Elegir si es Público o Privado.



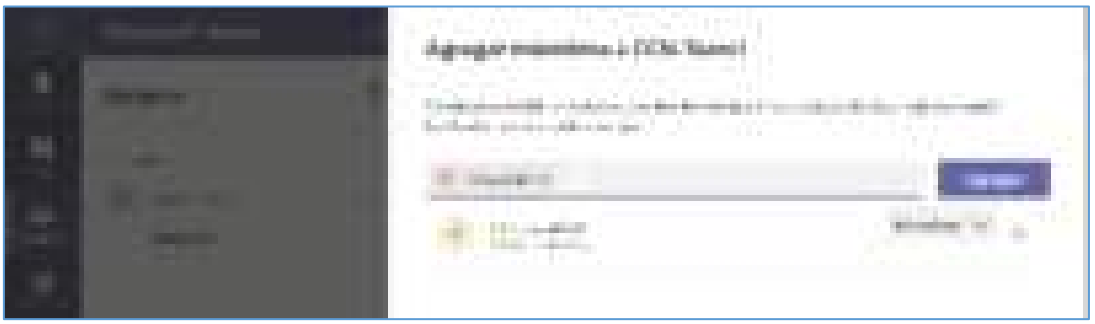
A continuación se describen las acciones para la creación de un *equipo privado*, es decir, las personas del equipo necesitarán un código para unirse.

3. Asignar un *nombre* al equipo, y pulsar el botón "Crear".



Al pulsar el botón "Crear", se creará el equipo en Teams y se pasará al siguiente paso.

4. Agregar *miembros* al equipo.



5. Revisar configuración del equipo y realizar más operaciones si procede.

En el ejemplo, se ha creado el *equipo* "CCN-Team1"

y un *canal* asociado "General" (por defecto).

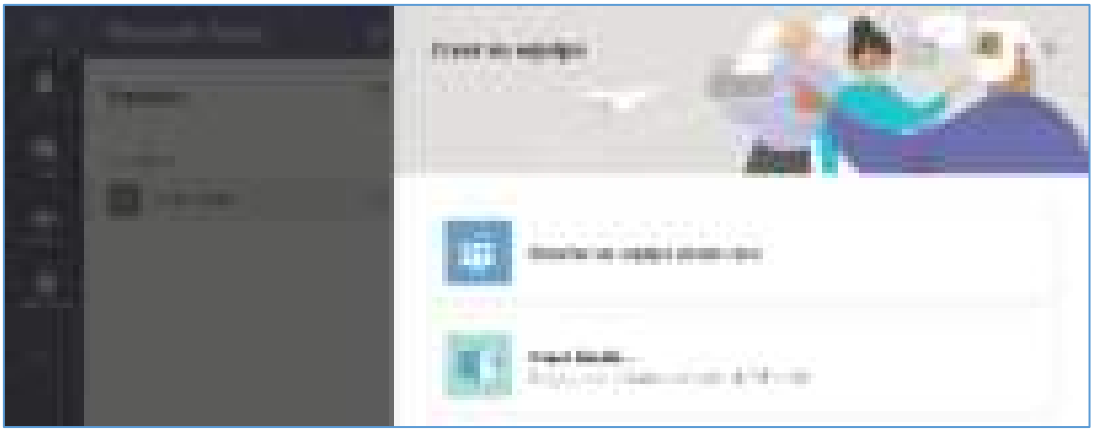
Pulsando en el menú "Mas opciones" del equipo se desplieguen múltiples opciones:

Más adelante se describe la opción "Administrar equipo" que es la opción más interesante desde el punto de vista de la seguridad.

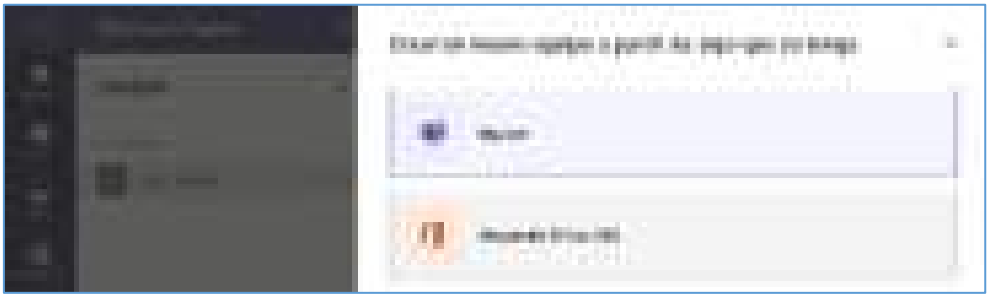
Crear un equipo desde un grupo existente en Office 365

Cuando se crea un equipo desde un grupo existente, la pertenencia del grupo, el sitio, el buzón y el bloc de notas se muestran en Teams.

1. Desde el menú lateral izquierdo de Teams, "Equipos", botón "Crear equipo".
2. Pulsar el botón "Crear desde…".

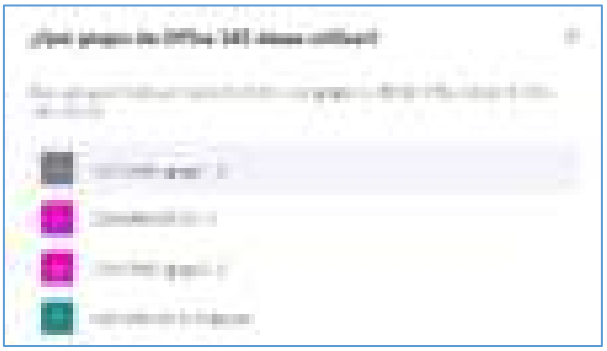


3. Elegir el elemento previo para crear el equipo: equipo de teams o grupo de Office 365.



En este ejemplo elegir “Grupo de Office 365”.

4. Elegir el grupo de Office 365 a utilizar.



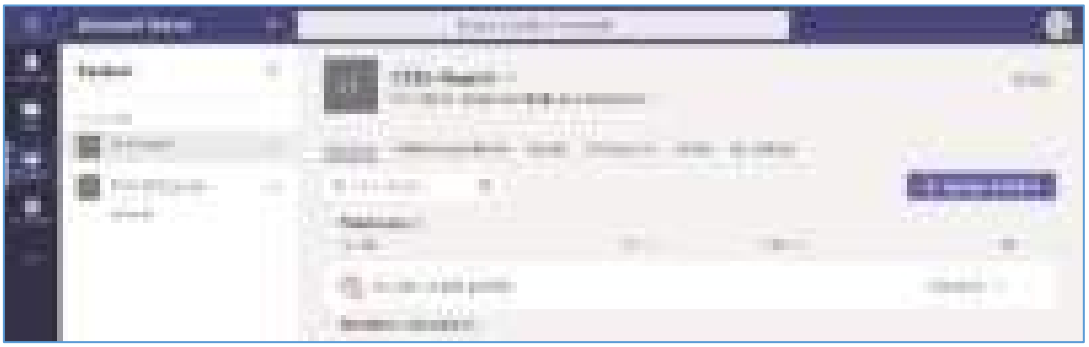
En este ejemplo elegir el grupo creado desde Sharepoint “CCN-O365-grupo1”. Consultar información sobre la creación de grupos de Sharepoint en la guía [CCN-STIC-885B - Guía de configuración segura para Sharepoint Online].

5. Revisar configuración del equipo y realizar más operaciones si procede.

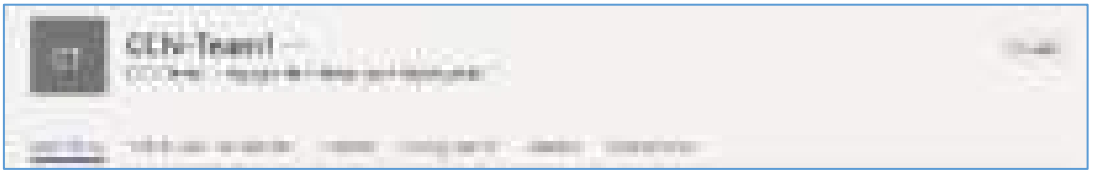
Administrar equipo de Teams

1. Seleccionar el equipo en el desplegable de equipos y pulsar el botón “Más opciones”.

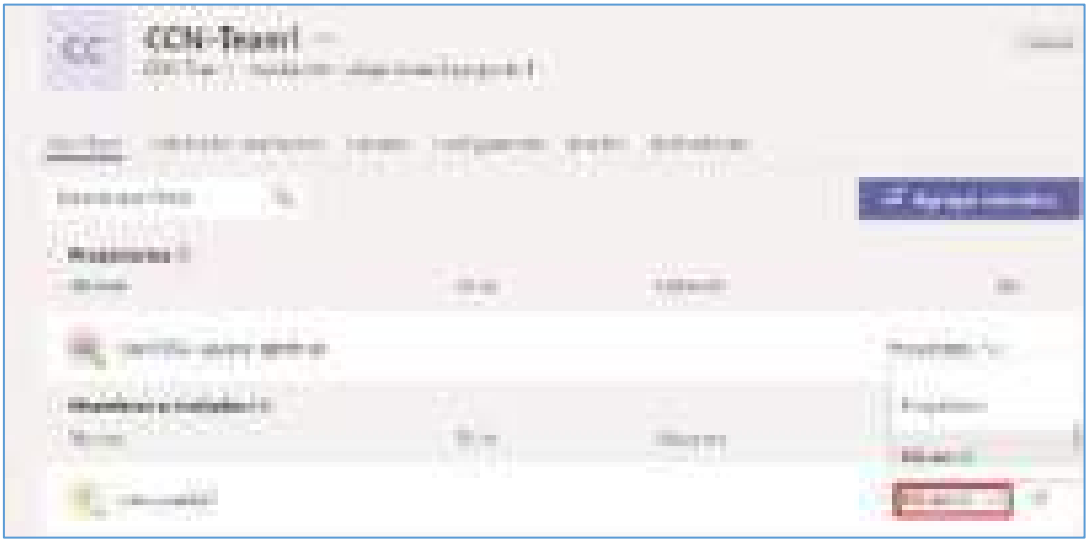
2. Seleccionar el item “Administrar equipo”.



Se muestra una pantalla con varias pestañas:



En la pestaña [Miembros] aparecen todos los miembros del equipo y su rol correspondiente. El propietario del equipo puede cambiar el **rol** de cada miembro desde el desplegable de la columna *rol*.



En la pestaña [Configuración] aparecen distintas opciones, las más destacadas desde el punto de vista de la seguridad son:

- *Permisos de miembros*: permitir la creación de canales, agregar aplicaciones y más.
- *Permisos de invitados*: permitir a invitados acciones sobre canales.
- *Código de equipo*: código para compartir y que sea posible unirse al equipo directamente (no se recibir solicitud para unirse).

Los permisos sobre miembros e invitados son:

Para ver como se administran permisos sobre el equipo y canales asociados consultar el apartado [3.1.1.2 Requisitos de acceso].

3. CONFIGURACIÓN DE MICROSOFT TEAMS

A continuación, se abordará la configuración del servicio *Microsoft Teams* 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 *Microsoft Teams* 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

En este apartado se abordan los niveles de permisos existentes sobre un equipo y un canal, y cómo se conceden los derechos de acceso a los distintos miembros.

Propietarios y miembros

En Microsoft Teams hay dos *niveles de permisos de usuario*: **propietario** y **miembro**. De forma predeterminada, a un usuario que crea un equipo nuevo se le concede el estado de propietario. Además, los propietarios y miembros pueden tener capacidades de moderador para un canal (siempre que se haya configurado la moderación). Si se crea un equipo a partir de un grupo existente de Office 365, se heredan los permisos.

En la tabla siguiente se muestra la diferencia entre un propietario y un miembro:

	Propietario de equipo	**Integrante de grupo**
Crear un equipo	Sí[1]	No
Abandonar equipo	Sí	Sí
Editar nombre o descripción del equipo	No	No
Eliminar equipo	No	No
Agregar canal	Sí	Sí[2]
Editar nombre o descripción del canal	Sí	Sí[2]
Eliminar canal	Sí	Sí[2]
Agregar miembros	Sí[3]	No[4]
Solicitud para agregar miembros	N/D	Sí[5]
Agregar fichas	Sí	Sí[2]
Agregar conectores	Sí	Sí[2]

Agregar bots	Sí	Sí[2]

[1] Los propietarios del equipo pueden crear equipos a no ser que se les haya quitado el permiso para hacerlo.

[2] Un propietario puede desactivar estos elementos en el nivel del equipo, en cuyo caso los miembros no tendrían acceso a ellos.

[3] Tras agregar un miembro a un equipo, un propietario también puede promover un miembro al estado de propietario. El propietario también puede degradar su propio estado a miembro.
[4] Los miembros del equipo pueden agregar otros miembros a un equipo público.
[5] Aunque un miembro del equipo no puede agregar directamente miembros a un equipo privado, puede solicitar que se añada a una persona a un equipo del que ya es miembro. Cuando un miembro solicita que se añada a una persona a un equipo, los propietarios del equipo reciben una alerta de que tienen una solicitud pendiente que pueden aceptar o denegar.

Los propietarios pueden convertir en propietarios a otros miembros del equipo, como se describió en el apartado [2.2. Usuario final – primeros pasos]. Un equipo puede tener hasta 100 propietarios. Se recomienda tener al menos dos propietarios para evitar tener grupos huérfanos si un propietario abandona el equipo.

3.1.1.3 Segregación de funciones y tareas

Microsoft Teams dispone de varios **roles de administración** enfocados a administrar distintas partes y elementos del servicio:

- *Administrador de servicios de Teams*, se encarga de administrar el servicio de Microsoft Teams, así como administrar y crear Grupos de Office 365.
- *Administrador de comunicaciones de Teams*, se encarga de administrar las características relativas a llamadas y reuniones dentro del servicio de Microsoft Teams.

- *Ingeniero de soporte en comunicaciones de Teams*, se encarga de hacer el *troubleshooting* de problemas de comunicaciones en Teams haciendo uso de herramientas avanzadas.
- *Especialista de soporte técnico de comunicaciones de Teams*, se encarga de hacer el *troubleshooting* de problemas de comunicaciones en Teams haciendo uso de herramientas básicas.

El rol genérico de *Administrador de Teams* puede asignarse desde el *Centro de administración de Microsoft 365*. Para asignar los roles específicos descritos anteriormente se debe utilizar Azure AD. Consultar la guía [CCN-STIC-884A - Guía de configuración segura para Azure].

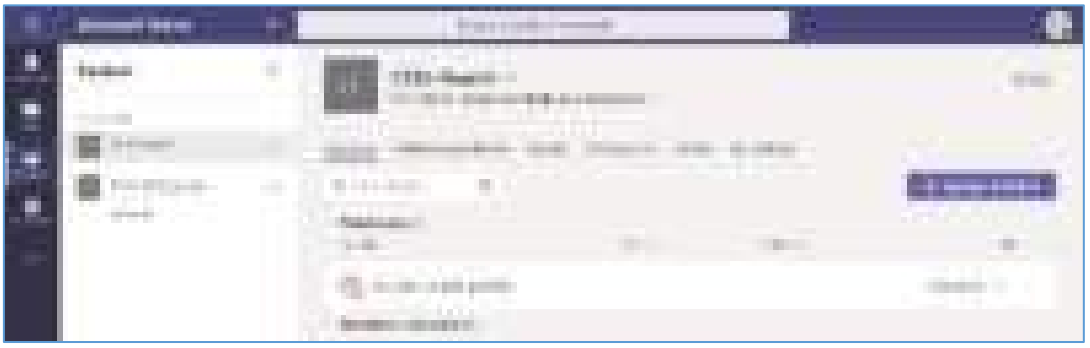
3.1.1.4 Proceso de gestión de derechos de acceso

En este apartado se describe cómo un propietario puede asignar permisos al resto de miembros sobre el propio equipo o los canales asociados.

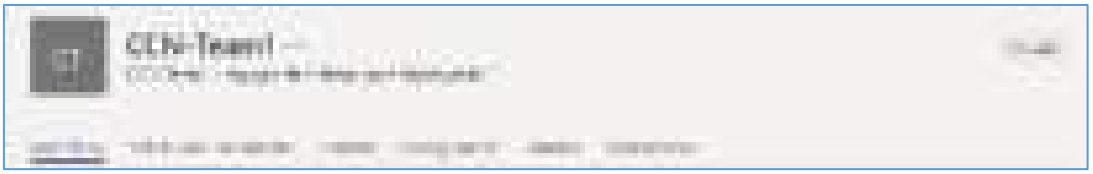
Administrar equipo de Teams por un propietario

1. Seleccionar el equipo en el desplegable de equipos y pulsar el botón “Más opciones”.

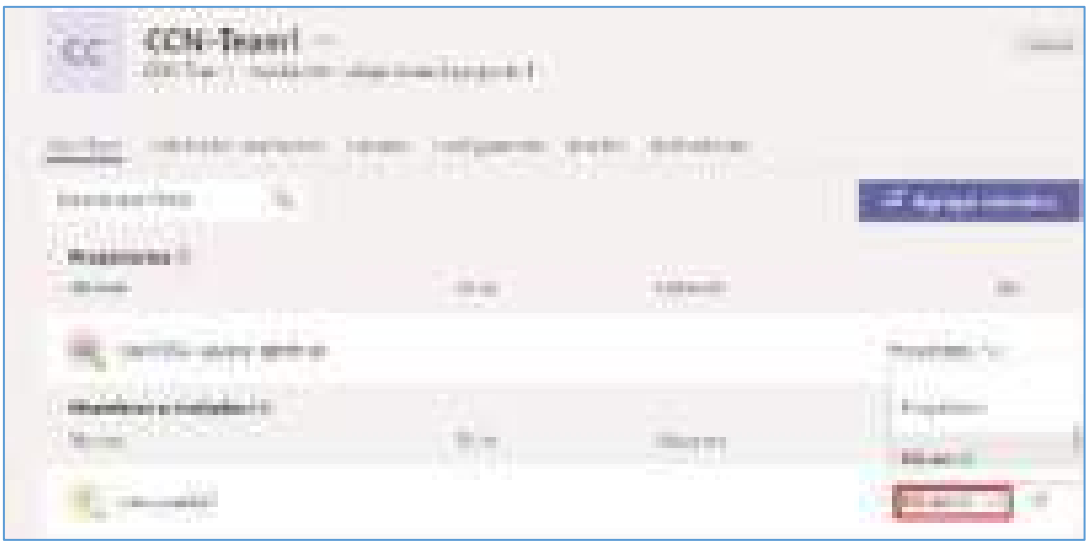
2. Seleccionar el item “Administrar equipo”.



Se muestra una pantalla con varias pestañas:



En la pestaña [Miembros] aparecen todos los miembros del equipo y su rol correspondiente. El propietario del equipo puede cambiar el **rol** de cada miembro desde el desplegable de la columna *rol*.



En la pestaña [Configuración] aparecen distintas opciones, las más destacadas desde el punto de vista de la seguridad son:

- *Permisos de miembros*: permitir la creación de canales, agregar aplicaciones y más.
- *Permisos de invitados*: permitir a invitados acciones sobre canales.
- *Código de equipo*: código para compartir y que sea posible unirse al equipo directamente (no se recibir solicitud para unirse).

Los permisos sobre miembros e invitados son:

Asignar permisos en la configuración de un canal por un propietario

Además de otras funciones, los propietarios y miembros de los equipos pueden tener capacidades de **moderador para un canal** (siempre que la moderación esté activada para un equipo). Los moderadores pueden iniciar publicaciones nuevas en un canal y controlar si los miembros del equipo pueden responder a los mensajes de canal existentes. También pueden controlar si los bots y los conectores pueden enviar mensajes de canal.

Para administrar la moderación de canales (por un propietario de un equipo):

1. En Teams, seleccionar canal de un equipo y pulsar el icono de “Más opciones”.
2. En el desplegable pulsar “Administrar canal”.
3. Gestionar los permisos.

3.1.1.5 Mecanismos de autenticación

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

Microsoft Teams usa la autenticación moderna para que la experiencia de inicio de sesión sea sencilla y segura. La autenticación moderna es un proceso que permite a los equipos saber que los usuarios ya han escrito sus credenciales (como el correo electrónico y la contraseña del trabajo) en otro lugar y no es necesario que las vuelvan a escribir para iniciar la aplicación.

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].

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 *portal de Azure AD.* Ver guía [CCN-STIC-884A - Guía de configuración segura para Azure].

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

Microsoft Teams **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, cumpliendo con el *Esquema Nacional de Seguridad* en su categoría Alta.

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].

Destacar que cuando un archivo en *SharePoint Online*, *OneDrive For Business* o *Microsoft Teams* se identifica como malintencionado, ATP bloquea el archivo.

La imagen siguiente muestra un ejemplo de un archivo malintencionado detectado en una biblioteca. Puede verse que el archivo está allí, pero está bloqueado y muestra un icono de advertencia junto a él.

La opción más segura es **eliminar el archivo**.

3.1.2.2 Registro de actividad

Para configurar el registro de actividad del servicio de Teams, 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].

Mencionar además que existen muchas actividades relacionadas con Teams en el registro de auditoría, accesibles desde el *Centro de Seguridad y cumplimiento de Office 365* menú [Buscar/Búsqueda de registros de auditoría]:

Como ejemplo de tales consultas:

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

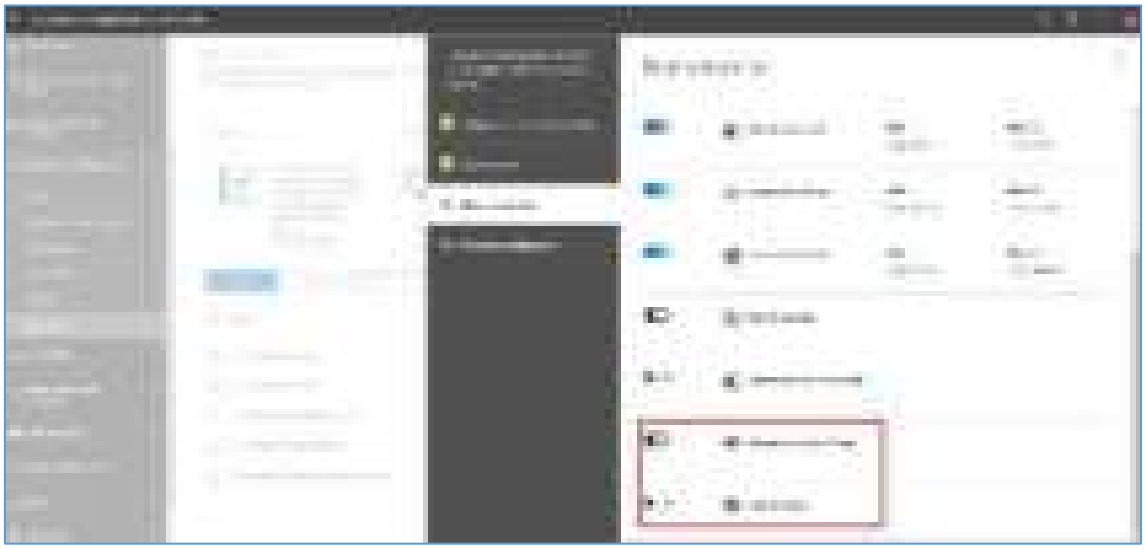
Consultar la guía [CCN-STIC-885A - Guía de configuración segura para Office 365] para ver los distintos mecanismos de monitorización del servicio, y el apartado [3.1.2.2 Registro de actividad] de la presente guía.

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].

Respecto a las etiquetas de retención para Teams, desde el *Centro de Seguridad y cumplimiento de Office 365* es posible establecer como ubicaciones en políticas de retención, tanto los "Mensajes de canal de Teams" como los "Chats de Teams". Es decir, que se puede actuar proactivamente en decidir si conservar y/o eliminar contenido en función de la duración del tiempo, tanto en las conversaciones, chats como en los mensajes de canal.



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**.

Los archivos de Teams se almacenan en SharePoint y están respaldados por el cifrado de SharePoint. Consultar la guía [CCN-STIC-8xx ANEXO X - Guía de configuración segura para Sharepoint Online].

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 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.

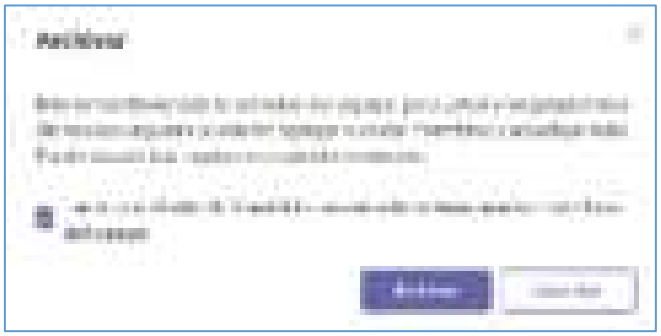
Una opción interesante relacionada con los mecanismos de respaldo es el "**Archivado**". Con el tiempo, es posible que un equipo creado en Microsoft Teams se quede fuera de uso o que se desee archivar o eliminar un equipo al final de un proyecto.

Archivar un *equipo* en Microsoft Teams

Cuando archiva un *equipo*, se detiene toda la actividad de ese equipo. El archivado de un equipo también archiva los canales privados y sus colecciones de sitios asociadas. Sin embargo, aún se puede agregar o quitar miembros y actualizar roles, y aún se puede ver toda la actividad del equipo en los canales, los archivos y los chats estándar y privados.

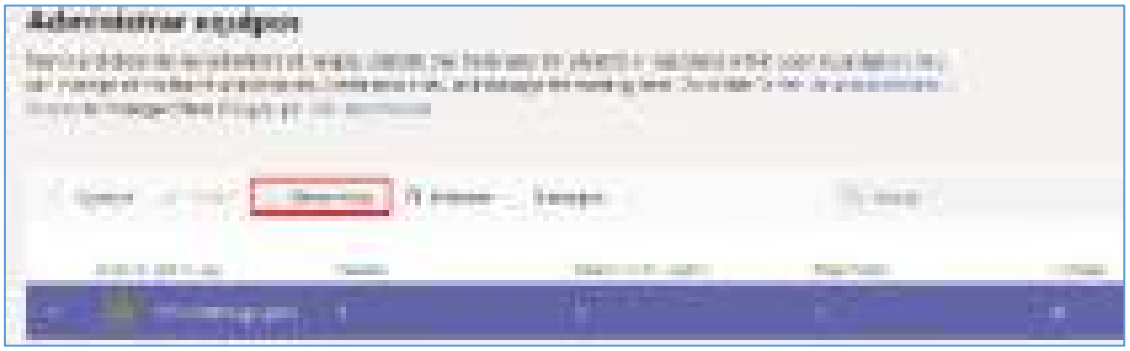
1. En el centro de administración de Microsoft Teams, seleccionar [Equipos\Administrar equipos].
2. Seleccionar un equipo haciendo clic en el nombre del equipo.
3. Seleccione ***Archivar***.

Y aparecerá el siguiente mensaje:



Al pulsar “Archivar” el estado asociado al equipo pasará de “Activo” a “Archivado”.

En cualquier momento se puede deshacer la operación con la opción “Desarchivar”:



Eliminar un *equipo* en Microsoft Teams

Si el equipo no se va a necesitar en el futuro, puede eliminarse en lugar de archivarlo.

1. En el centro de administración de Microsoft Teams, seleccionar [Equipos\Administrar equipos].
2. Seleccionar un *equipo* haciendo clic en el nombre del equipo.
3. Seleccione “Eliminar”. Aparecerá un mensaje de confirmación.

La operación de **restauración** de un equipo se realiza restaurando el grupo de Office 365 asociado con el equipo. Al restaurar el grupo de Office 365 de un equipo, se restaura el contenido del equipo, incluidas las pestañas, los canales estándar, los canales privados y sus colecciones de sitios asociadas.

De forma predeterminada, un grupo de Office 365 eliminado se conserva durante 30 días.

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. OTRAS CONSIDERACIONES DE SEGURIDAD

Desde el *Centro de administración de Microsoft Teams* pueden configurarse directivas de equipos, mensajería, reuniones, aplicaciones y voz y controlar a qué usuarios de la organización deben aplicarse. A continuación se muestran aquellas características que tienen cierta relevancia en la seguridad.

4.1 Directiva de equipos

Las directivas de equipos y canales se usan para controlar la configuración o características que están disponibles para los usuarios cuando usan los equipos y canales. Se puede usar la directiva global (predeterminada para toda la organización) y personalizarla, o bien se puede crear una o varias directivas personalizadas para los miembros de un equipo o canal de la organización.

- Descubrir equipos privados: Activar esta opción para permitir que los usuarios detecten equipos privados en los resultados de búsqueda y en la galería de equipos.
- Crear canales privados: Activar esta opción para permitir a los usuarios crear canales.

4.2 Directivas de mensajería

Las directivas de mensajería se usan para controlar qué características de mensajería por chat y canales están disponibles para los usuarios de Teams. Se puede usar la directiva global (predeterminada para toda la organización), o bien se puede crear una o varias directivas de mensajería personalizadas para los contactos de la organización.

De forma predeterminada, se crea una directiva denominada **global** (opción predeterminada para toda la organización). A todos los usuarios de la organización se les asignará esta directiva de mensajería de forma predeterminada. Se pueden realizar cambios en esta Directiva o crear una o más directivas personalizadas y asignarles usuarios.

Por ejemplo, supongamos que se desea asegurarse de que los mensajes enviados no se eliminen ni modifiquen por parte de los usuario. Se debería crear una nueva directiva personalizada denominada "retener mensajes enviados" y con la configuración siguiente:

- Los propietarios pueden eliminar los mensajes enviados.
- Los usuarios NO pueden eliminar mensajes enviados
- Los usuarios NO pueden editar mensajes enviados

1. Acceder al *Centro de administración de Microsoft Teams.* Menú [Directivas de mensajería].
2. Pulsar el botón “Agregar”.

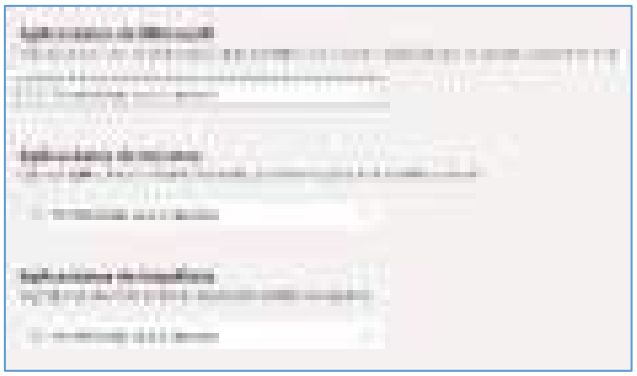
3. Configurar la opciones y “Guardar”.

4.3 Directivas de permisos de aplicaciones

Las directivas de permisos de aplicaciones controlan qué aplicaciones estarán disponibles para los usuarios de Teams en la organización. Se puede usar la directiva global (predeterminada para toda la organización) y personalizarla, o bien se puede crear una o varias directivas para satisfacer las necesidades de su organización.

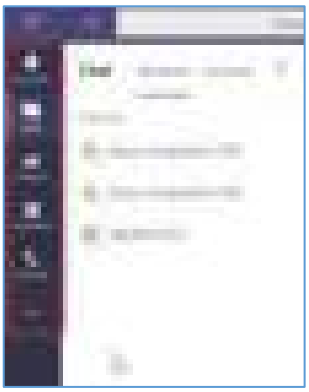
Se accede desde el *Centro de administración de Microsoft Teams*. Menú [Aplicaciones de Teams\Directivas de permisos].

Permite configurar qué aplicaciones de Microsoft, de terceros y de *Tenant* pueden instalar los usuarios. Se recomienda habilitar únicamente aquellas aplicaciones que hayan sido probadas y autorizadas por la organización, y mantener un control sobre las aplicaciones que se publican en la tienda.



4.4 Directivas de configuración de la aplicación

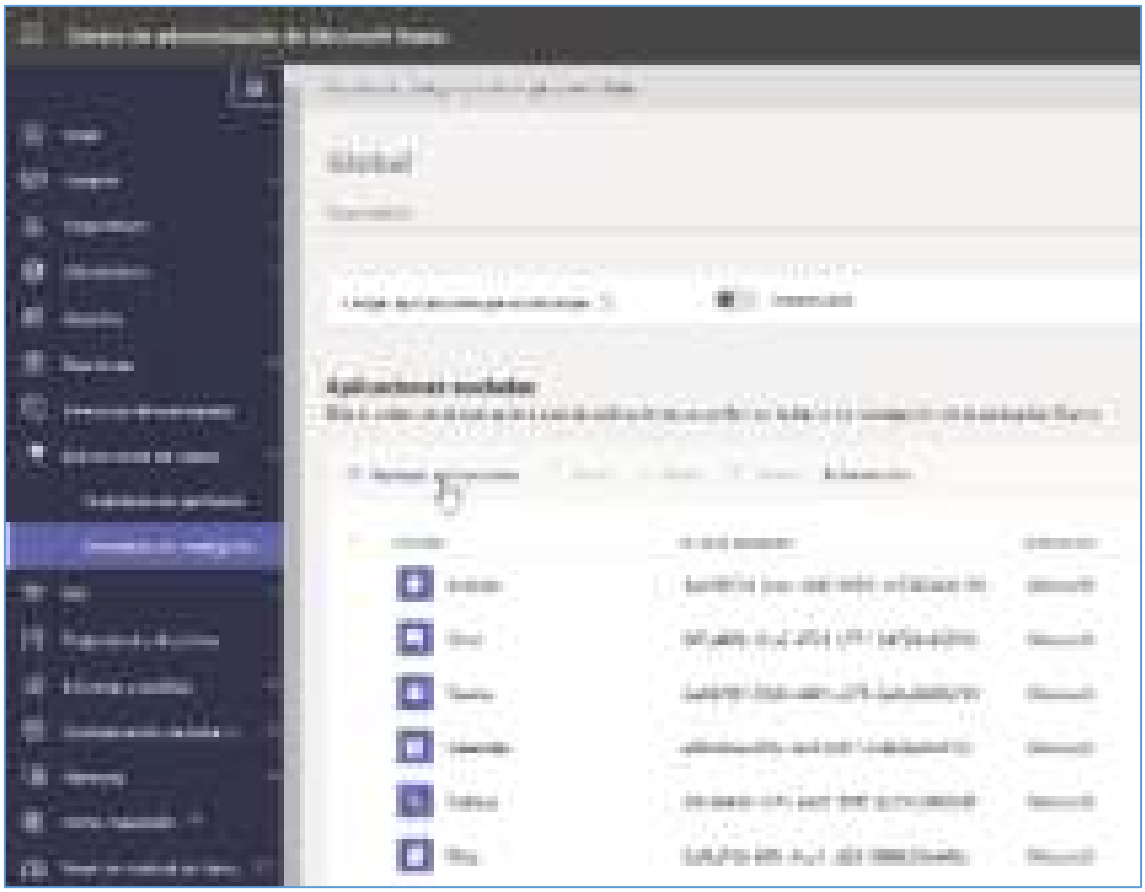
Las directivas de configuración de aplicaciones controlan la forma en que las aplicaciones están disponibles para el usuario con la aplicación de Teams.



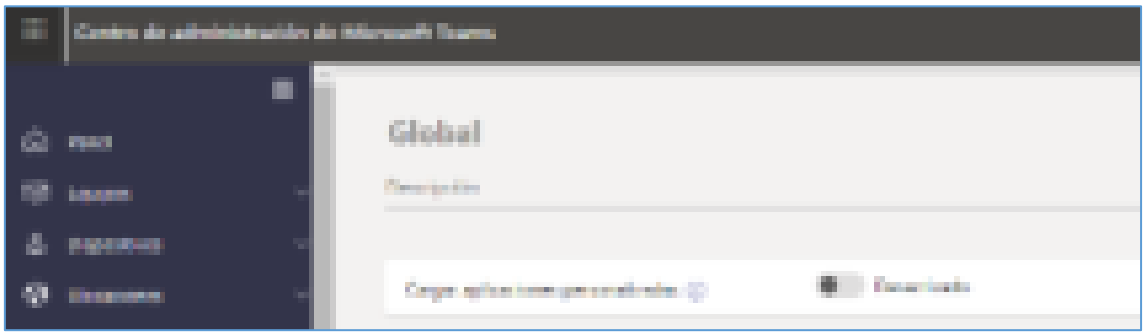
Las aplicaciones se anclan a la barra de la aplicación. Esta es la barra en el lateral del cliente de escritorio de Teams y en la parte inferior de los clientes móviles de Teams (iOS y Android).

Puede usarse la directiva global (predeterminada para toda la organización) y personalizarla, o bien pueden crearse directivas personalizadas y asignarlas a un conjunto de usuarios.

Se accede desde el *Centro de administración de Microsoft Teams*. Menú [Aplicaciones de Teams\Directivas de configuración].



Se recomienda NO permitir la “carga de aplicaciones personalizadas”.



4.5 Directivas de voz

En Microsoft Teams, las directivas de llamadas controlan qué características de llamadas y desvío de llamadas están disponibles para los usuarios. Las políticas de llamadas determinan si un usuario puede hacer llamadas privadas, usar el desvío de llamadas o llamar de forma simultánea a otros usuarios o números de teléfono externos, enrutar llamadas al buzón de voz, enviar llamadas a grupos de llamadas, usar la delegación para llamadas entrantes y salientes, etc.

Nota: Microsoft Teams permite conectar el servicio Online con una centralita telefónica local o de nube, a través del enrutamiento directo. Se requiere un controlador de borde de sesión

(SBC) compatible. Desde el punto de vista de la seguridad, si su organización tiene previsto integrar este servicio, se deberá garantizar que la comunicación SIP esté cifrada con TLS 1.2.

4.6 Directivas de reunión

Las *directivas de reunión* se usan para controlar qué características están disponibles para los usuarios cuando se unen a reuniones de Microsoft Teams.

Se accede desde el *Centro de administración de Microsoft Teams.* Menú [Reuniones\ Directivas de reunión].

Puede usarse la directiva global (predeterminada para toda la organización) y personalizarla, o bien pueden crearse una o varias directivas de reunión personalizadas para las personas que organicen reuniones en la organización.

Con estas directivas puede establecerse, por ejemplo, el bloqueo para usuarios anónimos, permitir o bloquear grabación, permitir el uso compartido, etc.

4.7 Directivas de dispositivos

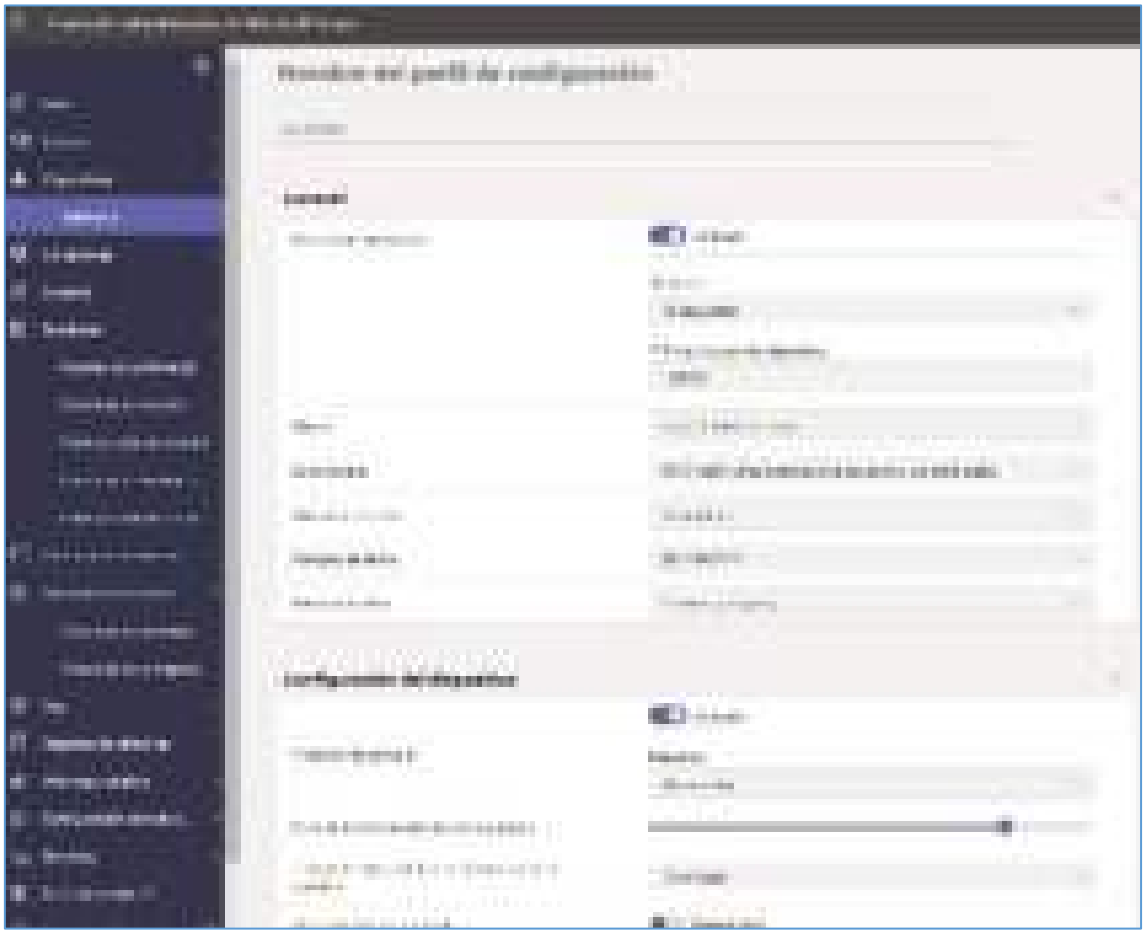
Teams permite conectar dispositivos (teléfonos IP) directamente con el servicio. Cada vez es más habitual ver dispositivos de conferencia y teléfonos utilizándose con Teams.

Se pueden controlar los teléfonos IP y dispositivos periféricos, como auriculares y cámaras web que se han certificado para su uso con Teams. Pueden crearse y cargar perfiles de configuración para cada tipo de dispositivo que disponga la organización, de forma que puedan realizarse cambios en su configuración.

Se accede desde el Centro de administración de Microsoft Teams. Menú [Dispositivos\ Teléfonos].

Perfiles de configuración

Desde la pestaña "Perfiles de configuración" es posible controlar opciones de seguridad del dispositivo (teléfono IP) como bloqueo, PIN, protector de pantalla, logs, etc.



5. 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 colspan="2">Configuracion</th><th>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 colspan="2" 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* de los recursos: propietarios y miembro.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.acc.3	**Segregación de funciones y tareas**		
	Se ha asignado adecuadamente los roles de administrador (en caso de que se haya establecido una delegación para este servicio). Siguiendo las recomendaciones del apartado 3.1.1.3 Segregación de funciones y tareas 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.4	**Proceso de gestión de derechos de acceso**		
	Se han revisado los permisos específicos en cada uno de los usuario de los equipos creados.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.acc.5	**Mecanismo de autenticación**		
	Se ha habilitado *Multi-Factor Authentication* (MFA) para los usuarios de la organización. *Siguiendo las recomendaciones del 3.1.1.5 Mecanismos de autenticación 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 encuentra habilitado el “doble factor de autenticación” y/o directivas de acceso condicional, 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 dispone de un registro de intentos de accesos con éxito y fallidos al sistema.	**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 comprueba periódicamente la detección de amenazas en tiempo real, accesible desde el *Centro de Seguridad y cumplimiento de Office 365*, y se genera el informe pertinente. * Si la organización 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. *Siguiendo las recomendaciones del apartado 3.1.2.4 Protección de los registros de actividad 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.mon	**Monitorización del sistema**		
	Se han configurado alertas en el *Centro de Seguridad y cumplimiento de Office 365.* *Siguiendo las recomendaciones del apartado 3.2.2 Monitorización del sistema en la guía [CCN-STIC-885A - Guía de configuración segura para 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. *Siguiendo las recomendaciones del apartado 3.2.3.1.2 DLPs (Data Loss Prevention) en 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.2	**Calificación de la información**		
	Se han aplicado *sensitivity labels.* *Siguiendo las recomendaciones del apartado 3.2.3.1 Calificación de la información en la guía [CCN-STIC-885A - Guía de configuración segura para Office 365]*	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No	
mp.info.9	**Copias de seguridad**		
	Se ha comprobado el archivado/eliminación de *equipos* en Microsoft Teams.	**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		
	Directivas de equipos		
	Se han revisado las directivas de equipos	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
	Directivas de mensajería		
	Se han revisado las directivas de mensajería.	**Aplica:** Si No	**Cumple:** Si No

		☐ ☐	☐ ☐
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
	Directivas de permisos de aplicaciones		
	Se han revisado las directivas de configuracion y permisos de aplicaciones.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
	Directivas de reunión		
	Se han revisado las directivas de reunión.	**Aplica:**	**Cumple:**

		☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
	Directivas de dispositivos		
	Se han revisado las directivas de dispositivos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**