centro criptológico nacional

ICT Security Guide
CCN-STIC 885D

Secure Configuration Guide for Microsoft Teams

JANUARY 2020

MINISTERIO DE DEFENSA

Edit:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.09.23 16:02:25 +02'00'

NIPO: 083-20-197-6
Date of Edition: january 2020

Plain Concepts has participated in the creation and modification of this document and its annexes.
Sidertia Solutions S.L. has participated in the revision of this guide.

LIMITATION OF RESPONSIBILITY

This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are indicated even when warning is provided concerning this damage.

LEGAL NOTICE

FOREWORD

The current national and international scenario is dominated by developments in Information and Communication Technologies (ICT) and by risks emerging from their use. The Administration is fully aware of this scenario and it is necessary for this body to develop, acquire, conserve and secure use of ICTs to guarantee that its services run effectively for the citizen's and the country's best interests.

Working from the Centre's knowledge and experience on threats and vulnerabilities in terms of emerging risks, Law 11/2002, dated 6th May, regulating the National Intelligence Centre, entrusts the National Intelligence Centre the functions related to information technology security, according to the Article 4.e), and to the protection of classified information, according to the Article 4.f). It also gives, through the Article 9.2.f), its Secretary of State-Director the responsibility of managing the National Cryptologic Centre.

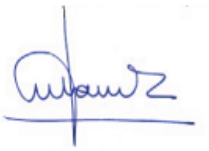
One of the most outstanding functions that it assigns to it, in Royal Decree 421/2004, dated 12th March, regulating the National Cryptologic Centre is to draw up and disseminate standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technologies.

Royal Decree 3/2010, dated 8th January, develops the National Security Framework (hereinafter called ENS) in the field of Electronic Administration which is also referred in the second section of Article 156 of Law 40/2015, dated 1st October, of the Public Sector Legal System. The National Security Framework establishes the security policy, in matters of use of electronic means, which ensures the protection of information.

Indeed, Royal Decree 3/2010, dated 8th January, updated by Royal Decree 951/2015, dated 23rd October, sets the basic principles and minimum requirements as well as any protection measures to be introduced in Administration systems. In article 29, it authorises the CCN to develop CIS guidelines to ease the fulfilment of these minimum requirements.

The CCN-STIC documents series was drawn up to comply with this function and the ENS, aware of the importance of establishing a frame of reference on this matter that can be used as support so that Administration staff can carry out their difficult and occasionally thankless task of providing security for ICT systems within their responsibility.

July 2019



Felix Sanz Roldan
Secretary of State
Director of the National Cryptologic Centre

INDEX

1. MICROSOFT TEAMS

1.1 Description of the use of this guide

The purpose of this guide is to indicate the steps to be followed for the configuration of the *Microsoft Teams* service in compliance with the necessary requirements of the *National Security Framework* in its HIGH category.

This guide should be used in conjunction with [CCN-STIC-885A - Secure Configuration Guide for Office 365], which describes generalities of Office 365 and features common to all services, as well as a *glossary* of security terms and abbreviations used in these guides.

The following sources have been consulted for the preparation of this guide:

- Official Microsoft documentation.
- CCN-STIC-823 Cloud Services.
- CCN-STIC-884A - Secure Configuration Guide for Azure.
- CCN-STIC-885A - Secure Configuration Guide for Office 365.
- ENS Royal Decree BOE-A-2010-1330.

1.2 Service definition

Microsoft Teams is an Office 365 chat-based workspace designed to improve the communication and collaboration among business teams by enhancing the collaborative capabilities of the Office 365 cloud platform (a set of cloud-based applications and services hosted on servers owned by Microsoft and available from Internet-connected devices). It should also be noted that Office 365 executes on *Microsoft Azure*.

Microsoft Teams offers the possibility of using Office 365 applications, customizing the environment according to the needs of your computer. With Teams, users can:

- Conduct group or private chats to have group conversations with a few members.
- View content and chat history at any time.
- Start video or voice meetings by integrating *Skype* into your *business*.
- Get instant access to all the content, the collaboration tools, the users and the conversations through tabs.
- Add quick access to frequently used documents, websites, and applications
- Access to notes and documents thanks to the integration with *OneNote* and SharePoint.
- Work with Office Online documents directly from Teams.
- Planning tasks thanks to the integration with Planner.
- Adding *Power BI* reports.
- Enjoy a common workspace with a web and mobile devices interface.

- Being group-based allows the user to move easily from one collaboration platform to another.
- Add connectors that allow to integrate applications such as Yammer and third-party services, such as RSS, Bing News Channel or Twitter.
- Create custom integration with application programming interfaces and other development tools.

1.3 Prerequisites for deployment using PowerShell

Office 365 PowerShell allows to manage and configure *Microsoft Teams* from the command line, with one user having management rights. See the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

The commands for managing Teams are in two different modules:

- **Microsoft Teams PowerShell module** - contains the necessary cmdlets to create and manage teams.

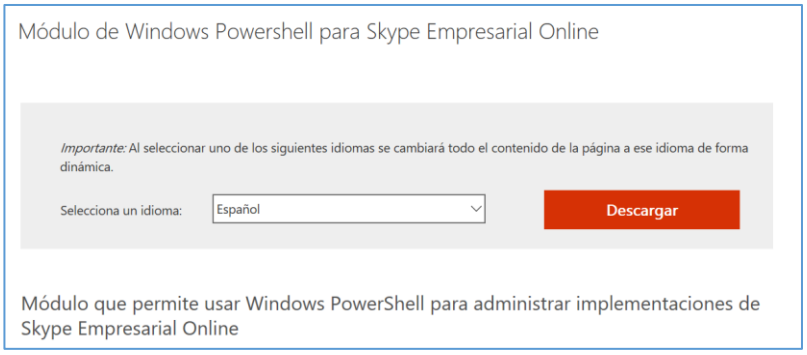
  To install it, open a version of PS in administrator mode:

```
#   Install-Module -Name MicrosoftTeams

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

- **Skype for Business PowerShell Module** - contains the cmdlets to manage policies, settings and other Teams tools.
  1. Locate the module in Microsoft's "Download Center":

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



  2. Download the file "SkypeOnlinePowerShell.exe" and execute.

To connect to the Microsoft Teams module:

```
#   Connect-MicrosoftTeams
```

To consult the *teams* created:

```
#    get-team
```

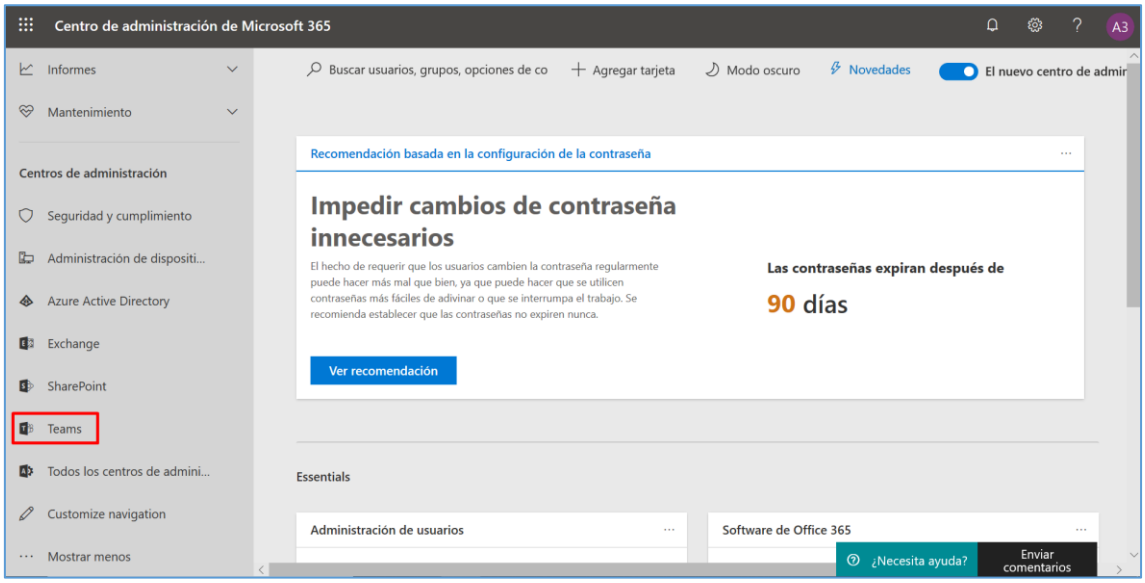
2. MICROSOFT TEAMS DEPLOYMENT

Microsoft Teams does not require prior installation in the client's *on-premise* environment, as it is an *online* service accessible from the Internet and hosted in the organization's Office 365 *tenant.* It uses the "Public Cloud" infrastructure referred to in the [823-Cloud Computing] guide.

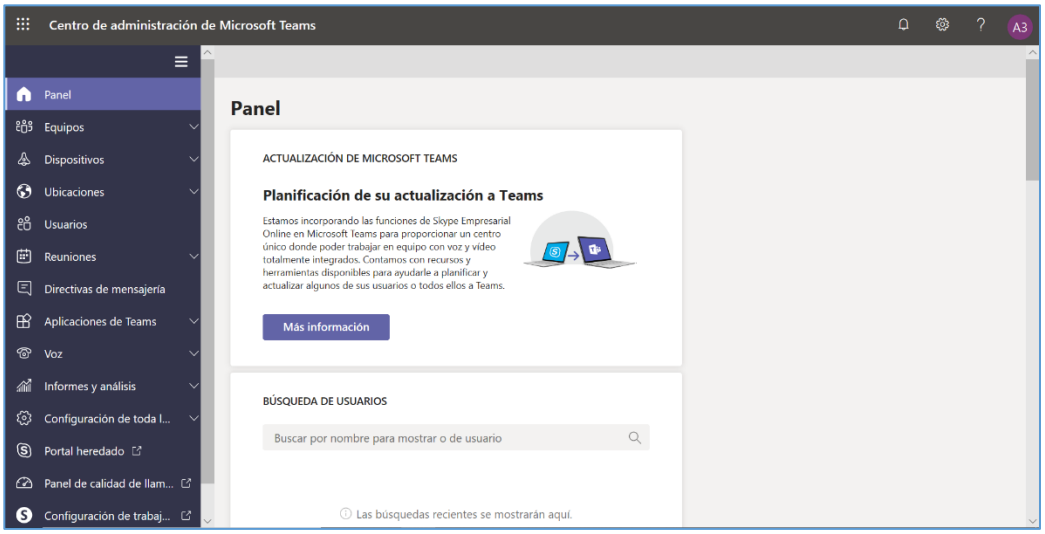
Microsoft Teams, as well as the Office 365 suite, is included in the ***SaaS*** (Software as a Service) category. The *CSP* (Microsoft) is in charge of offering the client the software as a service.

2.1 *Administrator - initial configuration*

The *administrator* user can access the *Microsoft Teams a*dministration *portal* through the Office 365 administration portal (portal.office365.com).



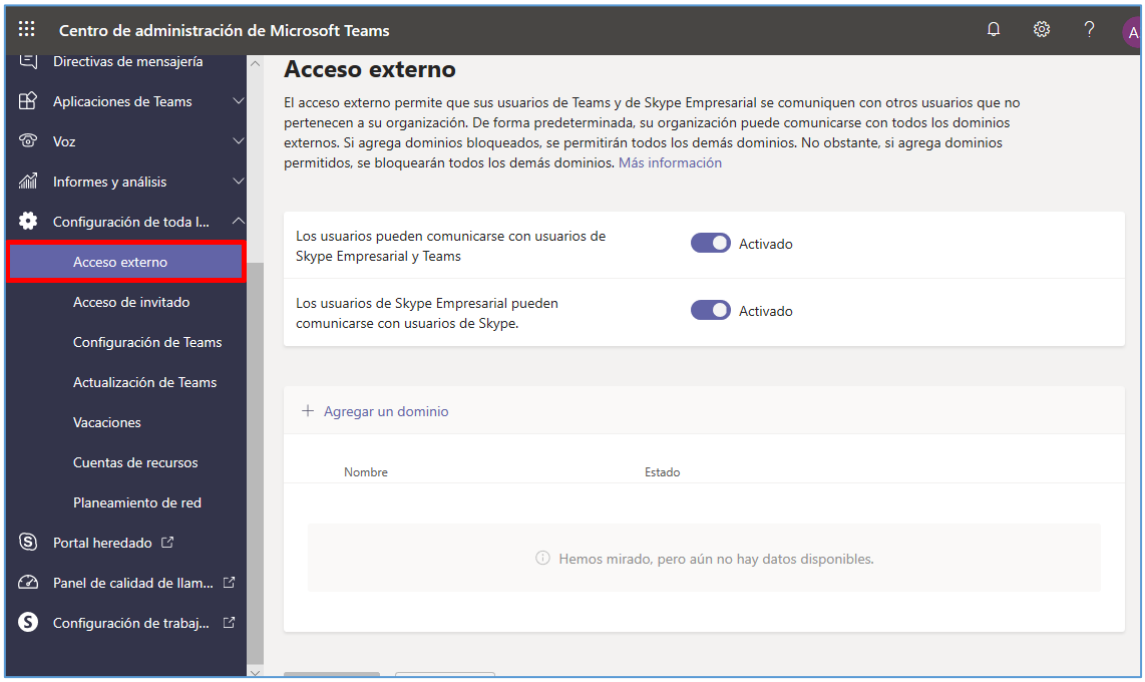
Clicking on the Teams icon takes you to the *Microsoft Teams Administration Center*.



The [Organization-wide Settings] menu controls the user settings for the entire organization. The most relevant ones from the security point of view are described below.

External access

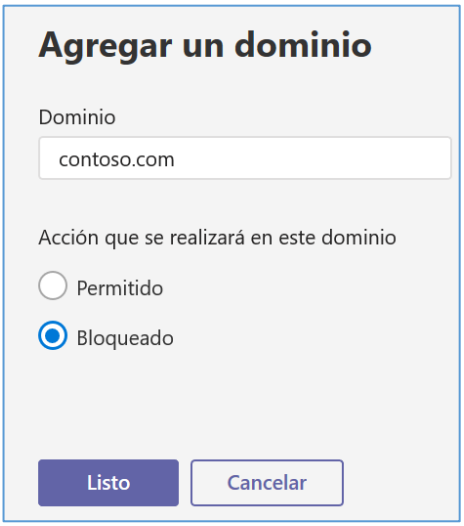
External access allows *Teams* and *Skype Business* users to communicate with users outside the organization or domain. The [Organization-Wide Settings] menu



External access is used when:

- There are users in different domains of the organization.
- People in the organization are required to use Teams to contact people of specific companies outside the organization.

1. In the previous screen, click on "+ Add a domain" to add allowed or blocked domains.



By default, the organization can communicate with all the external domains. If blocked domains are added, all other domains are allowed. However, if you add allowed domains, all other domains will be blocked.

2. Add domains to the list of blocked or allowed.

2.1. Write down the domain name.
2.2. Select the action.

2.3. Press "Ready".

This is how the domains are added individually.

It is important to restrict external domains, from a security point of view, to prevent users from other organizations from contacting members of our organization.

With this configuration, the user access to other organizations will also be controlled. The ability to communicate with users from other organizations is a key element in Teams, therefore, it is recommended to maintain a list of authorized or blocked domains, and to properly maintain this list over time.

Guest access

Guest access allows people outside the organization to be granted access to *teams* and *channels* in one or more business spaces. Any contact who has an email account (such as Outlook or Gmail or others) can participate as a guest in Teams with full access to chats, meetings and team files.

You can access it through the menu [Organization-wide settings\Guest access].

Guest access **is disabled by default,** and it is recommended to not activate it unless necessary.

All Teams' *guests* are protected with the same regulatory compliance and auditing as the rest of Office 365, and can be managed securely within Azure AD.

Differences between guest access and external access

- Guest access grants access permission to one person. External access grants access permission to a whole domain.
- Guest access, once granted by a team owner, allows a guest to access resources, such as files and channel discussions, for a specific computer and to chat with other users of the team to which they have been invited.
- With external access (federated chat), external chat participants do not have access to the organization's teams or team resources. They can only participate in a federated chat (one-on-one).

- Tenant managers can choose between the two communication options depending on the level of collaboration that is desirable with the external part. Administrators can choose between two approaches or both, depending on the needs of the organization.

The following table shows a comparison of the characteristics of both:

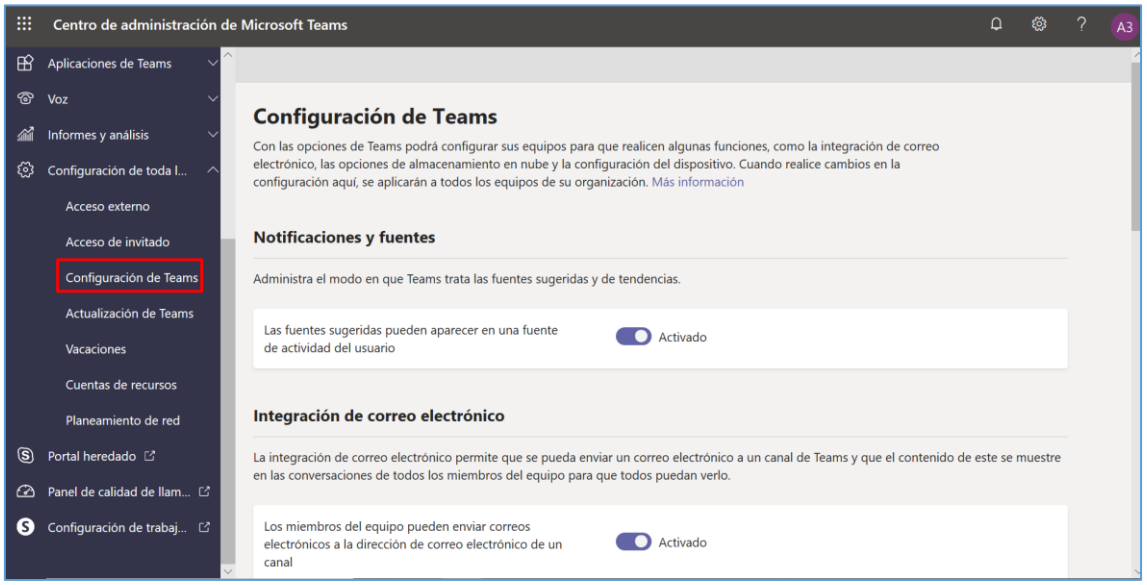
Feature	**Users of external access**	**Users of guest acces**
User	Yes	Yes
User	Yes	Yes
The user	Yes	Yes[1]
User *tenants*	Yes2Yes2	NoNo
User filesUser	NoNo	YesYes
The user TeamsUser	NoNo	YesYes
You can Add a user to a group chatUser	NoNo	YesYes
A user	YesYes	YesYes
Se pueden agregar usuarios adicionales a un chat con un usuario externo	No3No3	N/DN/A
Presence	YesYes	YesYes
An out of	NoNo	YesYes
Individual	NoNo	NoNo
@mentions	NoNo	YesYes
Making private callsMake	YesYes	YesYes
Allow IPAllow	YesYes	YesYes
Screen	NoNo	YesYes
Allow " nowAllow	NoNo	YesYes
Edit messagesEdit	NoNo	YesYes
You can messagesCan	NoNo	YesYes

[1] provided that the user has been added as a guest and has logged in as a guest for the guest tenant

[2] only by email or login protocol address (SIP).
[3] external (federated) chat is 1:1 only.

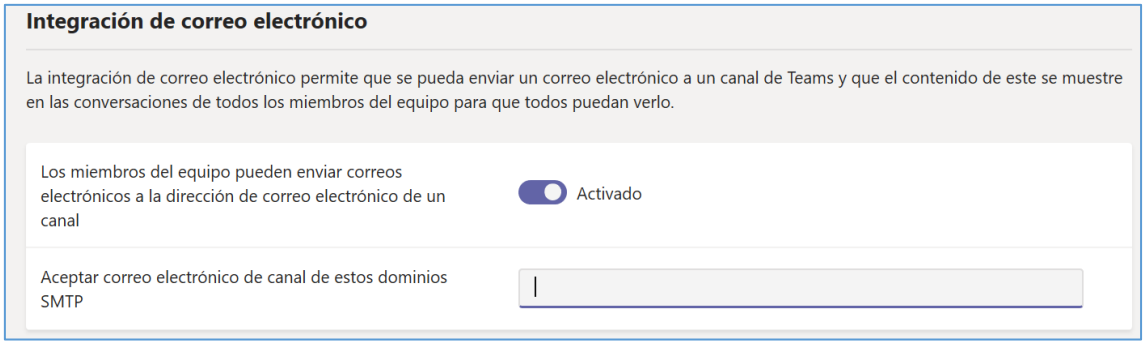
Organization-wide Settings

From the [Organization-Wide Settings\Microsoft Teams Settings] menu, you can control what features are available to users in your organization, including notifications and sources, e-mail integration, cloud storage options, and devices.



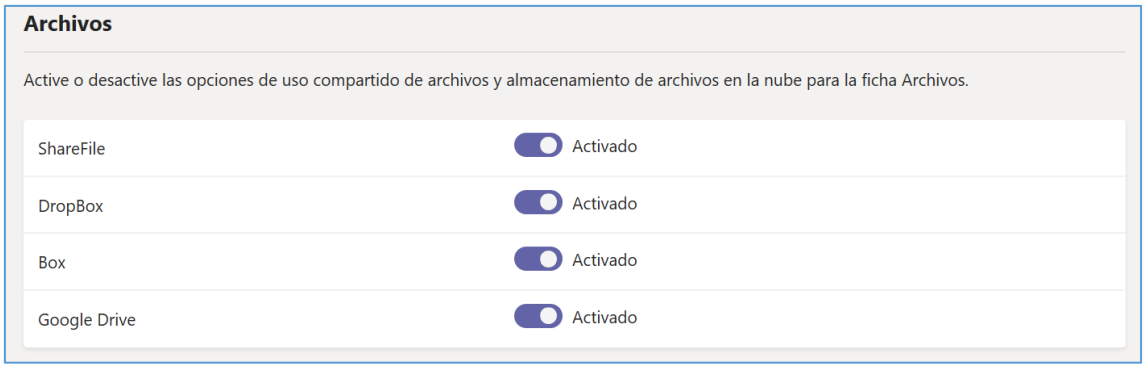
E-mail Integration

Enable this feature so that users can send an email to a channel on Microsoft Teams using the channel's email address.



Archives

Here you can enable or disable file sharing and cloud storage options.

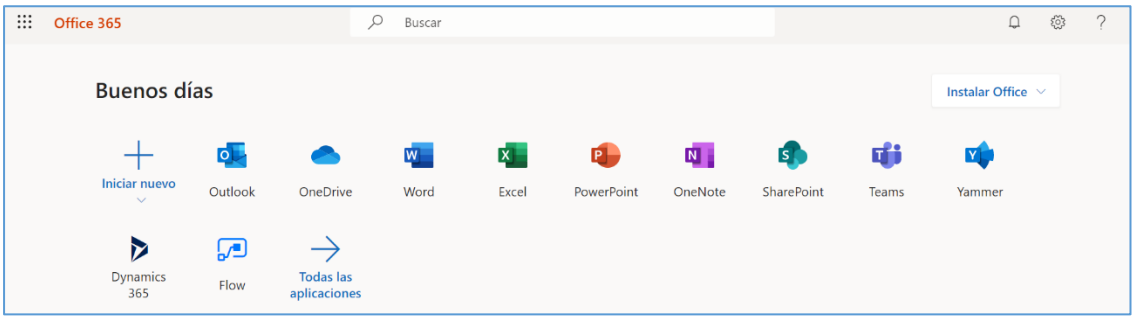


Users can upload and share files from cloud storage services on Teams' channels and chats. Cloud storage options on Microsoft Teams currently include ShareFile, Dropbox, Box and Google Drive. Enable the switch of cloud storage providers that the organization wants to use.

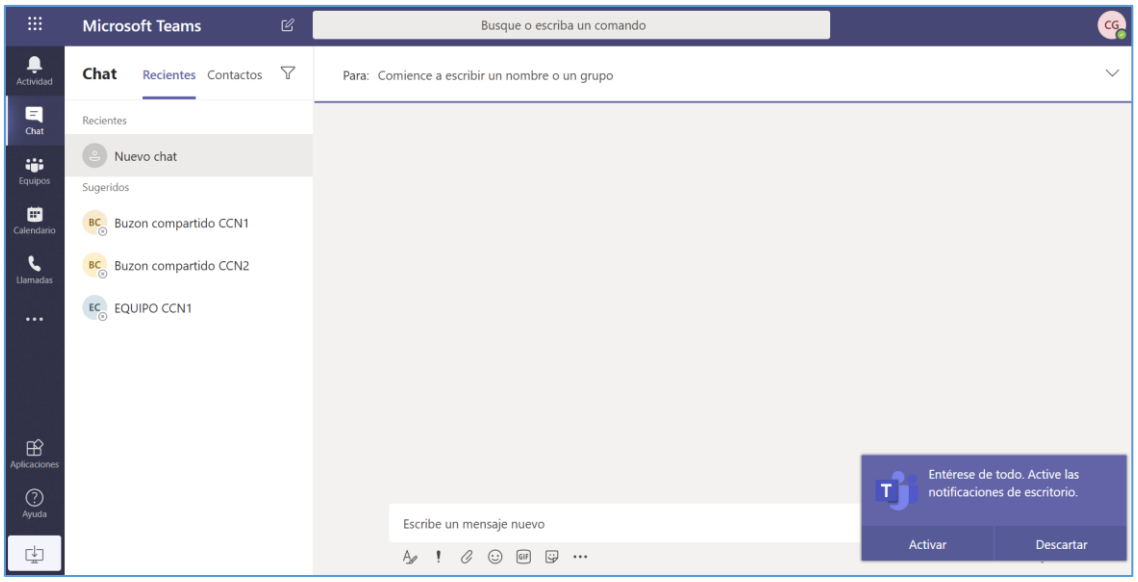
Note: It is recommended to enable only those cloud storage services that have been approved and controlled by the organization. Otherwise, there is a risk of storing sensitive information with external providers not controlled by the organization's policies.

2.2 *End user - first steps*

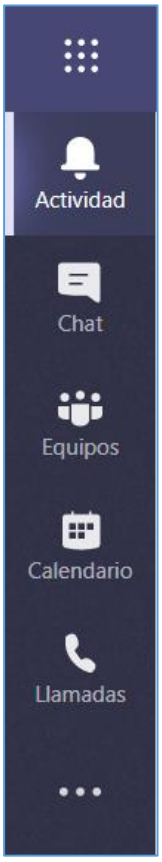
The *end user* can access the Office 365 portal through the *url*: *portal.office365.com* or www.office.com. After entering the credentials, a panel with all the applications to which you have access is displayed.



Click on the Teams icon to access the *Microsoft Teams'* portal (https://teams.microsoft.com).



The different options presented in the user menu are:



Activity: comments and responses made by each team member on a topic. To show only the user's own replies, select the option "My activity".

Chat: to establish new conversations with any member of the organization or to resume conversations.

Teams: channel list, which are sections that can be created within a *team*. Channels can be organized by topic, department or project.

Calendar: all the user's planned meetings and commitments By clicking on it you will be able to see your complete agenda.

Calls - displays speed dialing, contact list and call/voicemail history options.

Files: views of the files accessed by the user or any of the team members you work with.

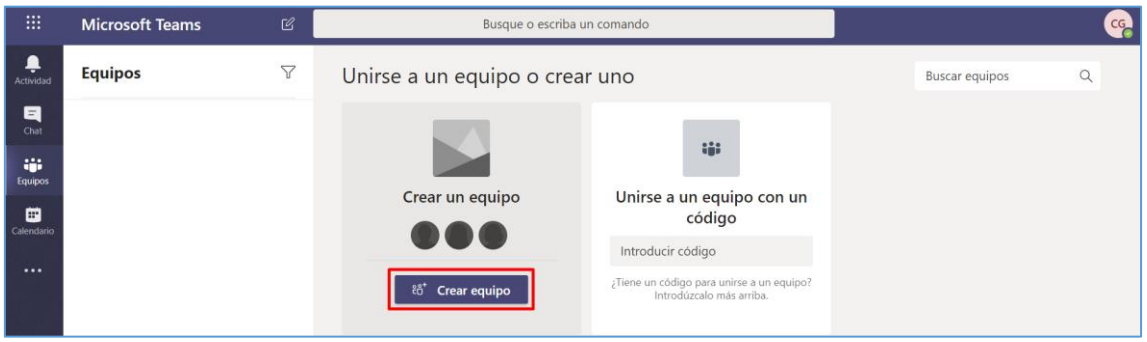
Applications: access to the different applications integrated in Teams.

Creating a team

Teams are collections of people, content and tools around various projects and tasks within an organization.

- Teams can be created to be private, for guest users only.
- Teams can also be created as public and open, so that all members of the organization can join (up to 5,000 members).

A Team can also be created from scratch, or from an existing group in Office 365.



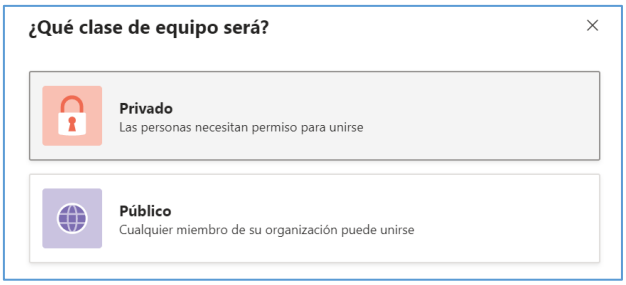
Click on the "Create Team" button, and choose whether to create the team from *scratch,* or *from an existing group* in Office 365.

Creating a team from scratch

When you create a team, this is what you create:

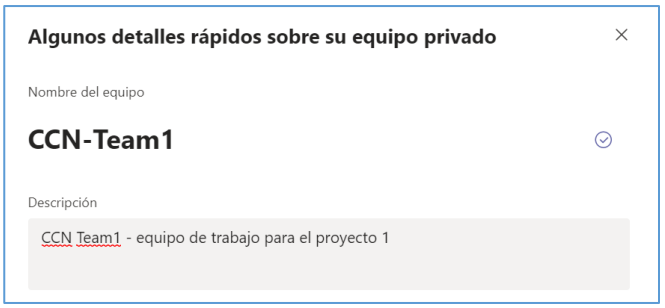
- A new group of Office 365.
- A SharePoint Online site and document library to store the computer files.
- A shared Exchange Online mailbox and calendar.
- A OneNote notebook.
- Relationships with other O365 applications, such as Planner and Power BI.

1. Press the button "Generate a device from scratch".
2. Choose whether it is public or private.



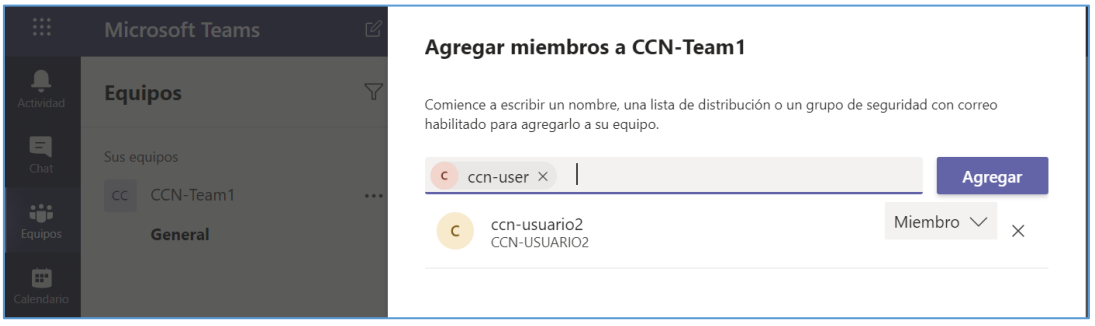
The actions for creating a *private team* are described below, i.e. people on the team will need a code to join.

3. Assign a *name* to the team and press the "Create" button.



If you press the "Create" button, the team will be created in Teams and you will go to the next step.

4. Adding *members to* the team.



5. Check the team's configuration and perform further operations if necessary.

In the example, the *unit* "CCN-Team1" and an associated *channel* "General" (default) have been created.

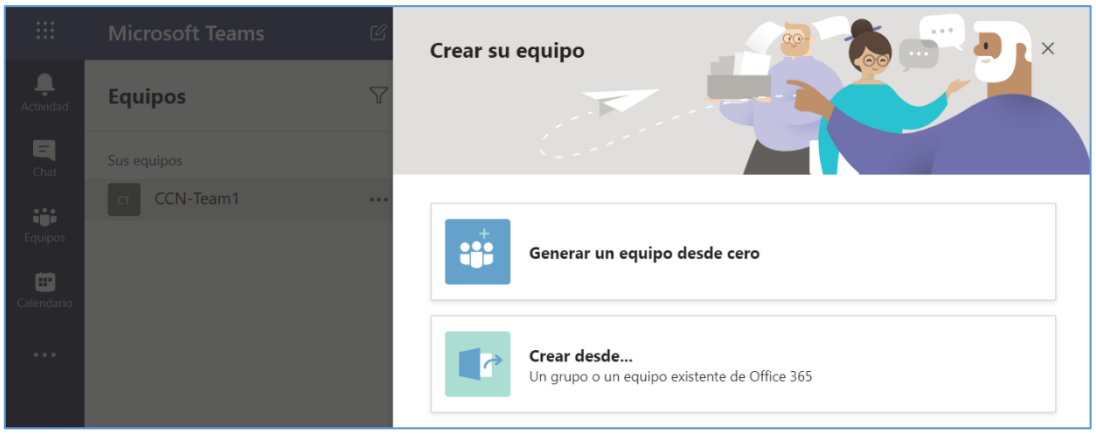
Clicking on the "More options" menu of the team displays multiple options:

The "Manage Team" option, which is the most interesting option from a security point of view, is described below.

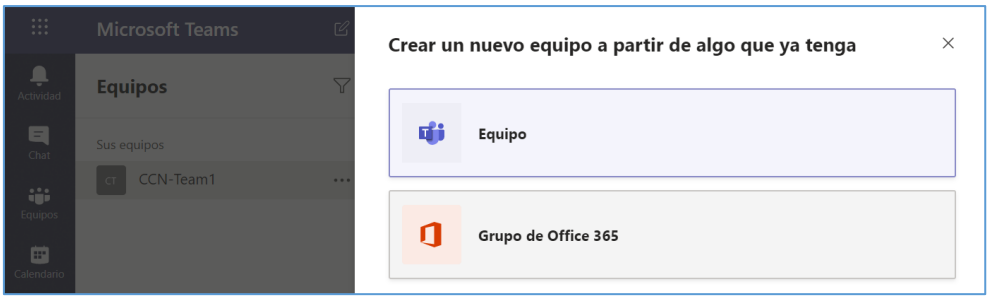
Create a team from an existing group in Office 365

When a team is created from an existing group, the group membership, site, mailbox, and notepad are displayed in Teams.

1. From the left side menu of Teams, "Teams", "Create Team" button.
2. Press the "Create from..." button.

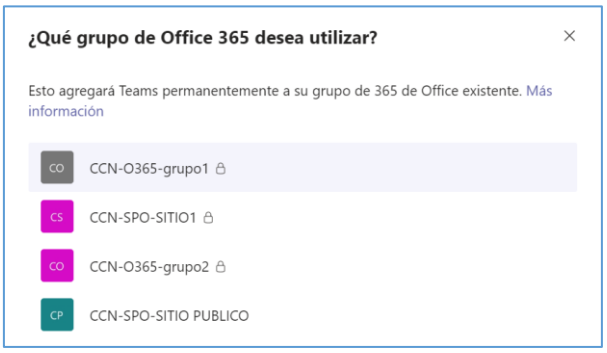


3. Choose the previous element to create the team: team of teams or Office 365 group.



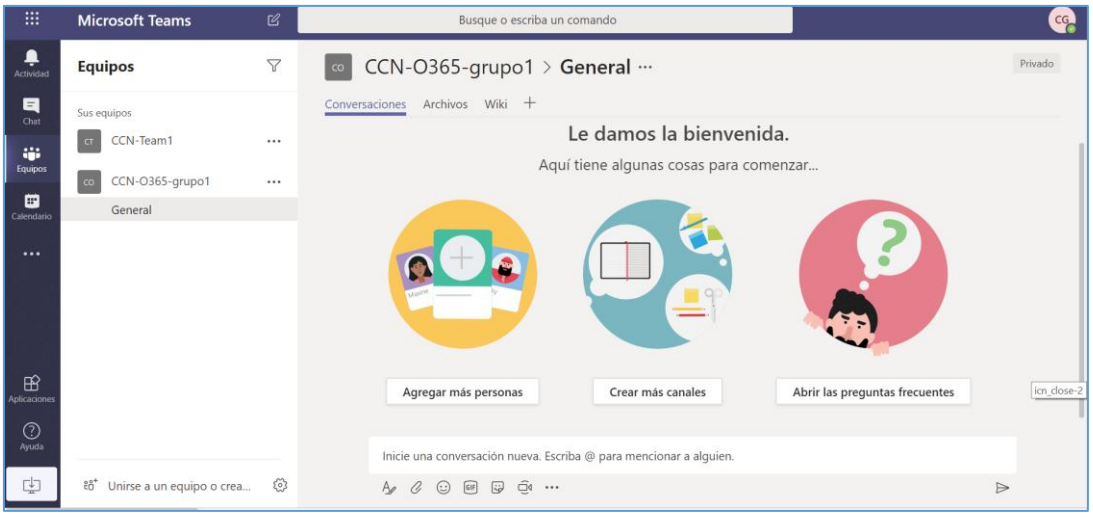
In this example choose "Office 365 Group".

4. Choose the Office 365 group to use.



In this example, choose the group created from Sharepoint "CCN-O365-group1". See information on creating Sharepoint groups in the guide [CCN-STIC-885B - Secure Configuration Guide for Sharepoint Online].

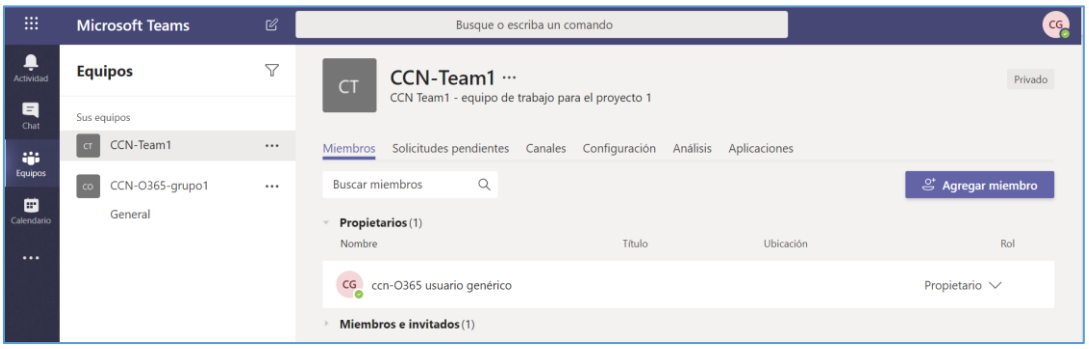
5. Check team settings and perform further operations if necessary.



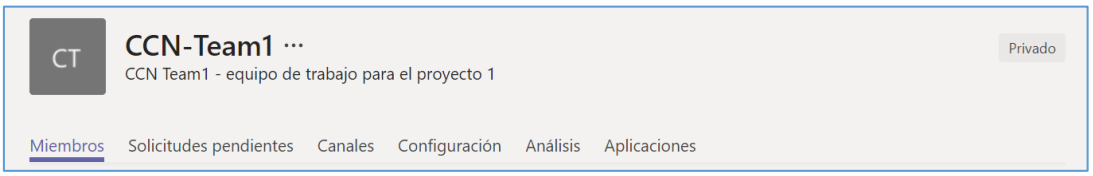
Manage Teams

1. Select the team from the team drop-down list and press the "More options" button.

2. Select the item "Manage team".



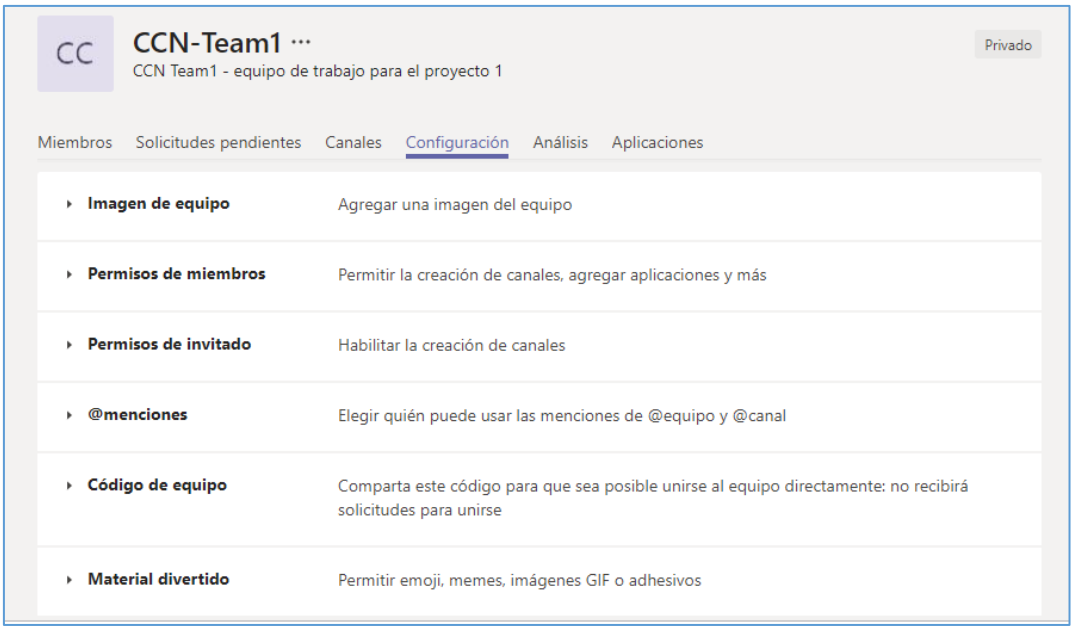
A screen with several tabs is displayed:



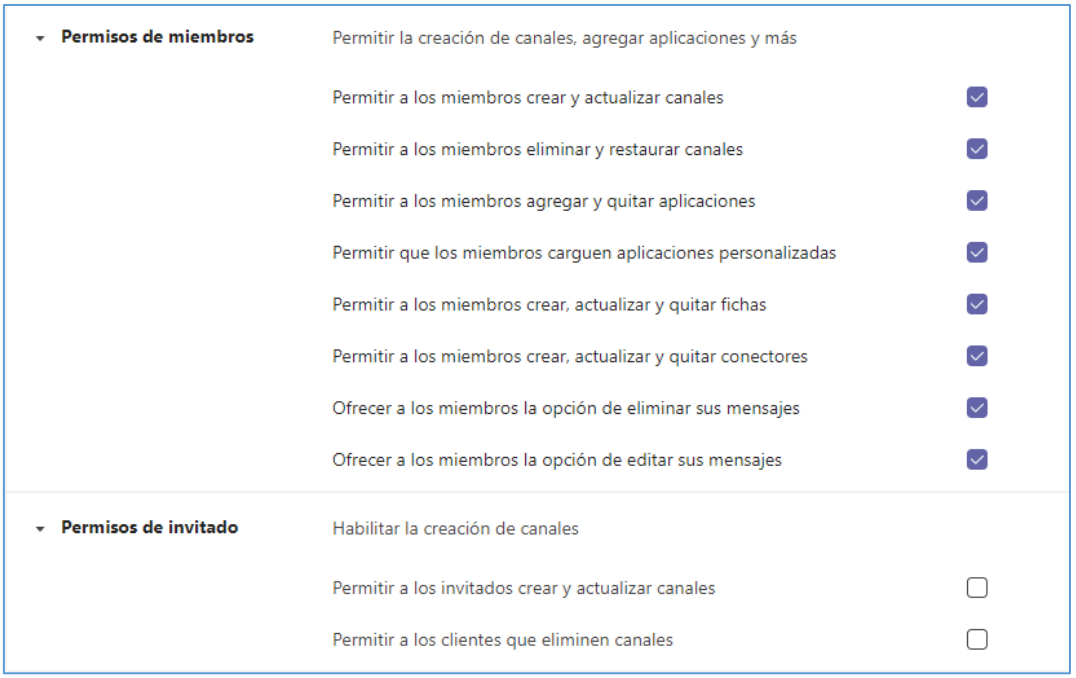
The [Members] tab shows all the team members and their corresponding roles. The team owner can change the **role** of each member from the drop-down list in the *role* column.

The [Settings] tab shows different options, the most important from a security point of view are:

- ***Member permissions***: allow the creation of channels, add applications and more.
- ***Guest permissions*:** allow guests to take action on channels.
- ***Team code***: code to share and to be able to join the team directly (no application needed to join).



The permissions on members and guests are:



To see how to manage permissions on the team and associated channels, see section [3.1.1.2 Access requirements].

3. MICROSOFT TEAMS CONFIGURATION

The configuration of the *Microsoft Teams* service will then be addressed, focusing on complying with the requirements of the National Security Framework that apply exclusively to this service.

3.1 Operational Framework

3.1.1 Access Control

3.1.1.1 Identification

Microsoft Teams Identity Management is common to all Office 365 applications and is described in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

3.1.1.2 Entry requirements

This section discusses the existing permission levels on a team and a channel, and how access rights are granted to different members.

Owners and members

In Microsoft Teams there are two *levels of user permissions*: **owner** and **member**. By default, a user who creates a new computer is granted the owner status. In addition, owners and members can have moderating capabilities for a channel (provided that moderation has been set up). If a team is created from an existing Office 365 group, permissions are inherited.

The table below shows the difference between an owner and a member:

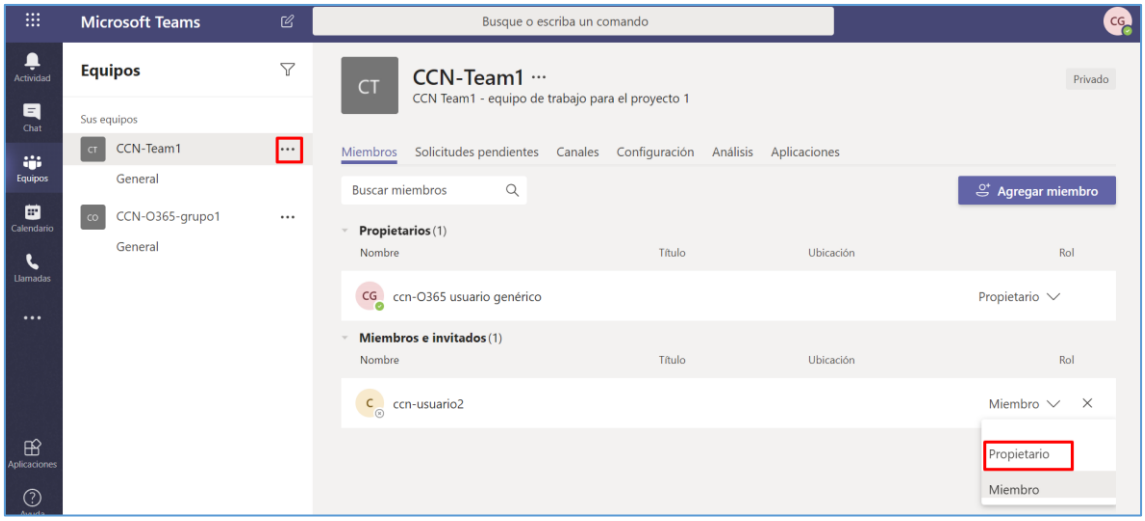
	Team Owner	**Group member**
Create a team	Yes1	No
Leave the team	Yes	Yes
Edit the name or description of the team	No	No
Remove team	No	No
Add channel	Yes	Yes2
Edit name or description of the channel	Yes	Yes2
Delete channel	Yes	Yes2
Add members	Yes3	No 4
Application to add members	N/A	Yes5
Adding files	Yes	Yes2
Adding connectors	Yes	Yes2
Adding bots	Yes	Yes2

[1] Team owners can create teams unless they don't have permission to do so.

[2] An owner can disable these items at the team level, in which case the members would not have access to them.

[3] After adding a member to a team, an owner can also promote a member to owner status. The owner can also downgrade his or her own status to member.
[4] Team members can add other members to a public team.
[5] Although a team member cannot directly add members to a private team, he or she can request to add a person to a team of which he or she is already a member. When a member requests to add a person to a team, team owners are alerted that they have a pending request that they can accept or deny.

Owners can turn other team members into owners, as described in section [2.2. End user – first steps]. A team can have up to 100 owners. It is recommended to have at least two owners to avoid having orphaned groups if one owner leaves the team.



3.1.1.3 Segregation of functions and tasks

Microsoft Teams has several **management roles** focused on managing different parts and elements of the service:

- *Teams Service Administrator is* responsible for managing the Microsoft Teams service, as well as managing and creating Office 365 Groups.
- *Teams Communications Administrator* manages the calling and meeting features within the Microsoft Teams service.
- *Teams Communications Support Engineer is in* charge of *troubleshooting* communications problems in Teams using advanced tools.
- *Teams communications technical support specialist* is responsible for *troubleshooting* communications problems in Teams using basic tools.

The generic role of *Teams Manager* can be assigned from the *Microsoft Administration Center 365*. To assign the specific roles described above, you must

use Azure AD. Refer to the guide [CCN-STIC-884A - Secure Configuration Guide for Azure].

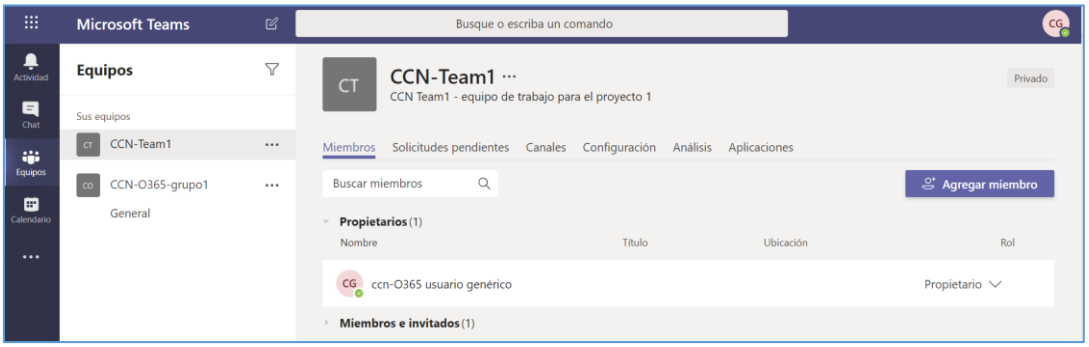
3.1.1.4 Access rights management process

This section describes how an owner can assign permissions to other members over the team itself or associated channels.

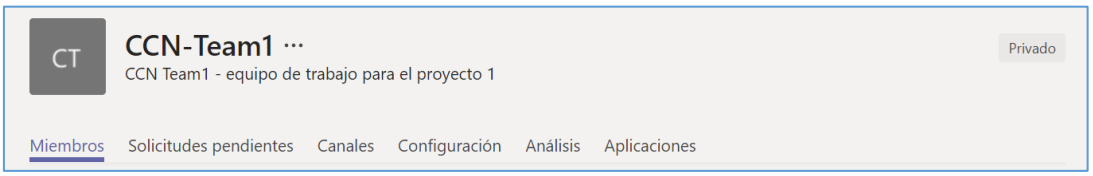
Administrating Teams by an Owner

1. Select the team from the team drop-down list and press the "More options" button.

2. Select the item "Manage team".



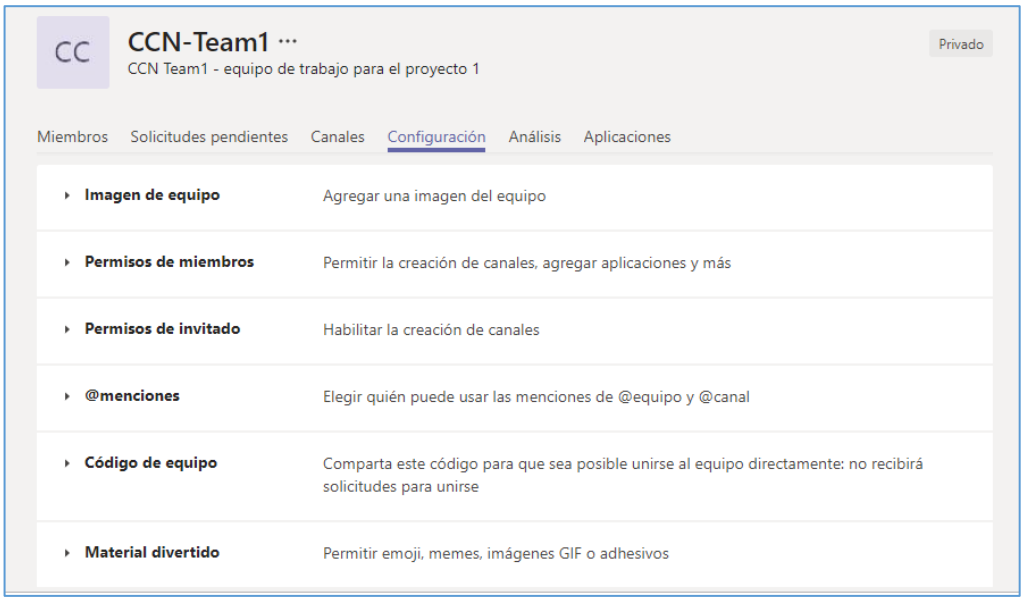
A screen with several tabs is displayed:



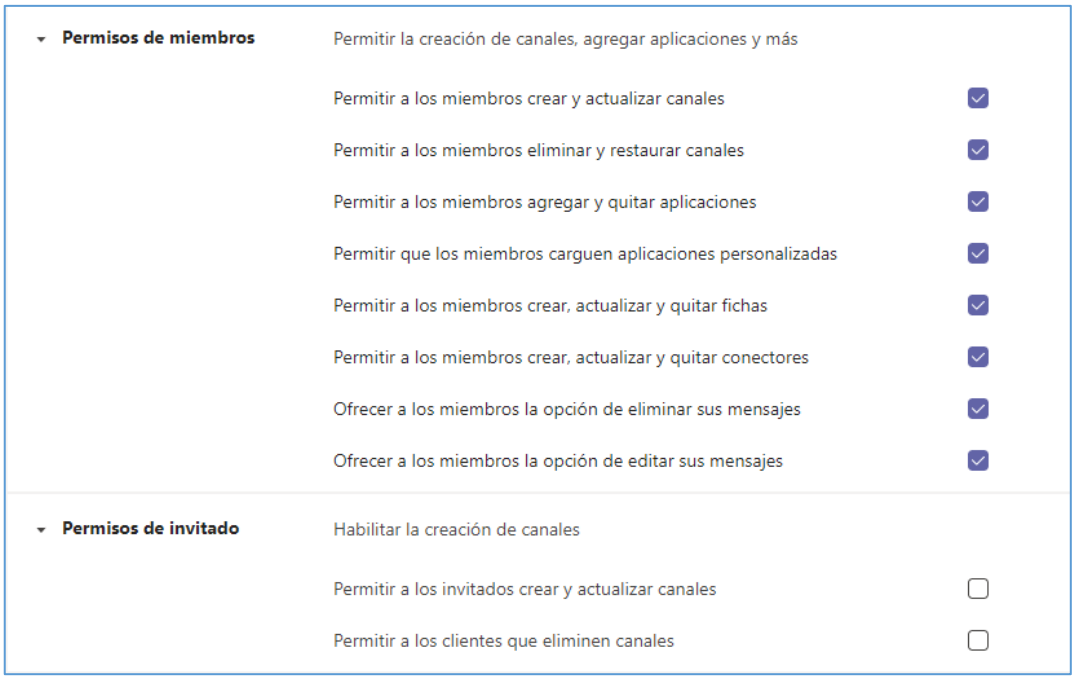
The [Members] tab shows all the team members and their corresponding role. The team owner can change the **role** of each member from the drop-down list in the *role* column.

The [Settings] tab contains various options, the most important from the security point of view are:

- *Member permissions*: allow the creation of channels, add applications and more.
- *Guest permissions*: allow guests to take action on channels.
- *Team code*: code to share and to be able to join the team directly (no application needed to join).



The permissions on members and guests are:

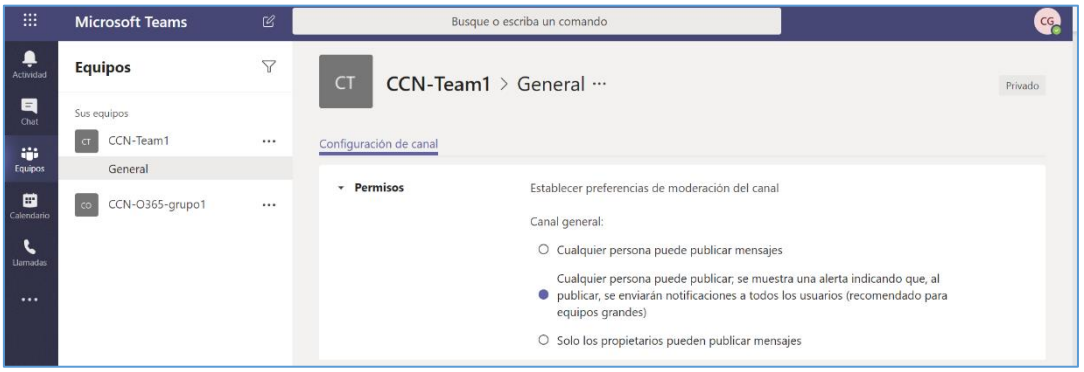


Assigning permissions in the configuration of a channel by an owner

In addition to other functions, team owners and members may have **moderating** capabilities for **a channel** (provided moderation is enabled for a team). Moderators can initiate new posts in a channel and control whether team members can respond to existing channel messages. They can also control whether bots and connectors can send channel messages.

To manage channel moderation (by a team owner):

1. In Teams, select a channel from a team and click on the "More options" icon.
2. Click on "Manage Channel" in the drop-down menu.
3. Manage the permits.



3.1.1.5 Authentication mechanisms

Information about password policies, MFA authentication and other authentication issues is shown in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

Microsoft Teams uses modern authentication to make the sign-in experience simple and secure. Modern authentication is a process that lets computers know that users have already typed in their credentials (such as work email and password) elsewhere and do not need to retype them to start the application.

3.1.1.6 Local access

It is understood as *local access* to the access from the corporate network or authorized locations.

It requires the establishment of a "multi-factor authentication" (MFA) and an appropriate credential management policy, which are described in section [3.1.1.5 Authentication mechanisms]. A record of successful and unsuccessful system access attempts is also required, as described in section [3.1.2.2 Activity Log]. Additionally, access to Office 365 can be controlled by conditional access policies or rules in ADFS, as described in the [CCN-STIC-884A - Secure Configuration Guide for Azure] guide.

3.1.1.7 Remote Access

Remote access is understood as access from the Internet (any IP). It is recommended to reinforce security when accessed from the Internet (*only managed computers*, *MFA*, *device compliance,* etc.). Everything can be managed from the *Azure AD's portal.* See guide [CCN-STIC-884A - Secure Configuration Guide for Azure].

It should be noted at this point that Office 365 is a *cloud* solution accessible by the end user through the Internet. Data encryption will be applied as described in section [3.2.3.2 Encryption] of the [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide.

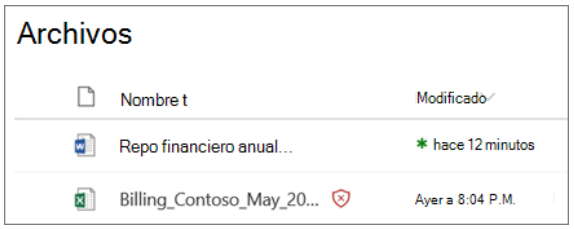
3.1.2 Exploitation

Microsoft Teams **will always be updated**. That is, the service is permanently maintained by Microsoft, taking care of updates and patches, as well as establishing the mechanisms for detection and protection against threats, complying with the *National Security Framework* in its High category.

3.1.2.1 Protection against malware

If your organization has *Office 365 Advanced Threat Protection (Office 365* ATP), you will have a real-time discovery browser, accessible from the *Office 365 Security and Compliance Center*. See the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

Note that when a file in *SharePoint Online*, *OneDrive For Business,* or *Microsoft Teams* is identified as malicious, ATP blocks the file.



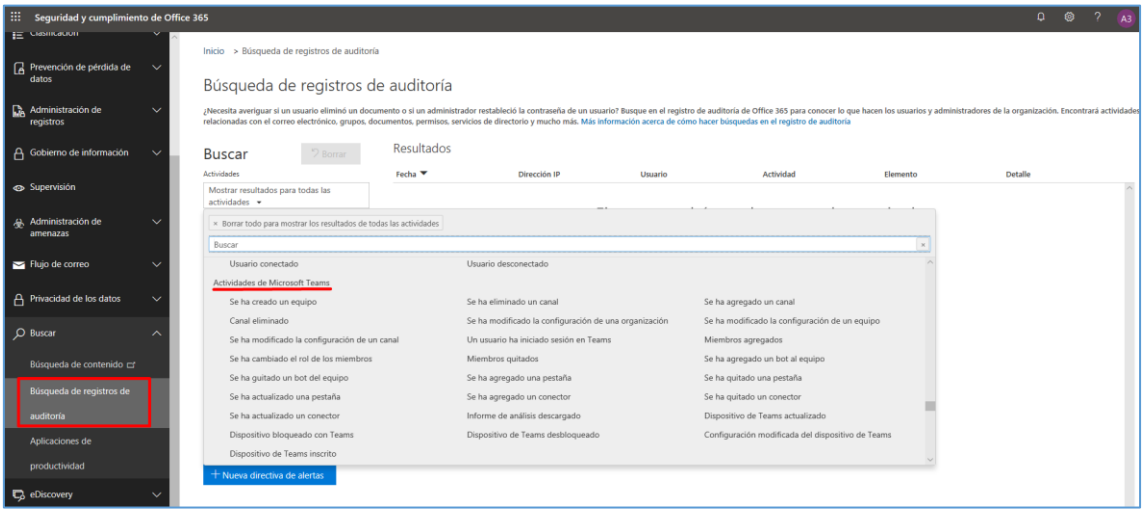
The image shows an example of a malicious file detected in a library. You can see that the file is there, but it is blocked and shows a warning icon next to it.

The most secure option is to **delete the file**.

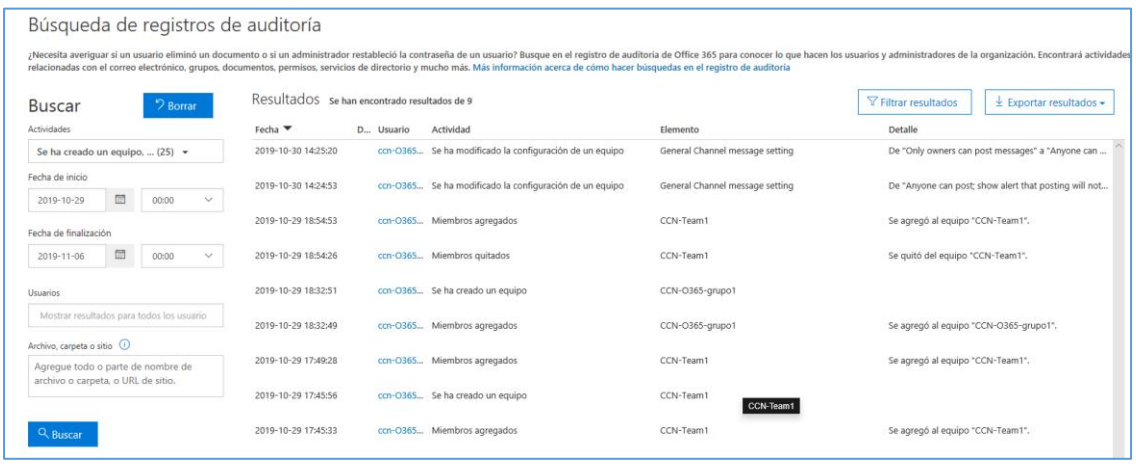
3.1.2.2 Activity log

To configure activity log of the Teams service, you will need to make use of the Audit functionality available through the *Office 365 Security and Compliance Center*. More information in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

Also mention that there are many activities related to Teams in the audit log, accessible from the *Office 365 Security and Compliance Center* menu [Search/Audit Logs]:



As an example of such consultations:



3.1.2.3 Incident Management

See section [3.1.2.1 Protection against malicious code] of the [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide for how to access "Threat Management" reports.

3.2 Protection measures

3.2.1 Protection of communications

In terms of communications protection, it should be noted that the cryptographic protocols for TLS connections, which are automatically integrated into Office 365, are used. This is true when:

- Users work with files stored in *OneDrive For Business* or SharePoint Online.
- Users share files in online meetings and instant messaging conversations.

In fact, all Office 365 communications are encrypted: Mail Clients (POP, IMAP, SMTP-TLS), Outlook Clients (MAPI-HTTPS), Browsers (Web HTTPS), Mobile Devices (ActiveSync HTTPS), Teams and Skype (SIP-TLS). No additional configuration is required, but it is important to note that as of June 2020, TLS 1.0 and 1.1 support will be removed. This has direct implications for customers.

https://docs.microsoft.com/en-us/office365/troubleshoot/security/prepare-tls-1.2-in-office-365

3.2.2 System monitoring

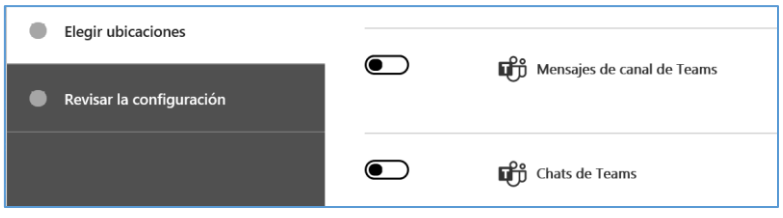
Refer to the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365] for the various service monitoring mechanisms, and section [3.1.2.2 Activity Log] of this guide.

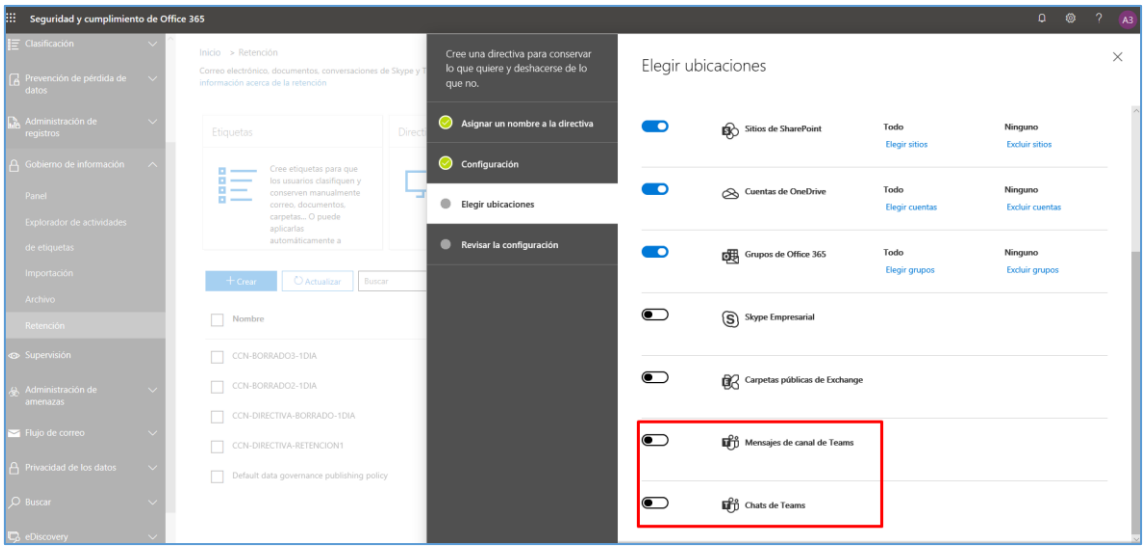
3.2.3 Protection of information

3.2.3.1 Rating of information

Office 365 has several mechanisms for qualifying information, as explained in section [3.2.3.1 Qualifying Information] of the [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide.

Regarding retention labels for Teams, from the *Security and Compliance Center in Office 365* it is possible to establish as locations in retention policies, both "Teams' Channel Messages" and "Teams' Chats". That is, you can act proactively in deciding whether to retain and/or remove content based on the length of time, both in conversations, chats and channel messages.





3.2.3.2 Encryption

Refer to the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365] for the generic encryption mechanism of Office 365, specifically encryption of **data at rest** and **in transit**.

Teams' files are stored on SharePoint and are backed up by SharePoint encryption. See the guide [CCN-STIC-8xx APPENDIX X - Secure Configuration Guide for Sharepoint Online].

3.2.3.3 Cleaning of documents

When sharing an electronic copy of certain Office 365 documents or posting certain documentation on the Internet, it is a good practice to review the document for hidden data, personal information, and generally any associated metadata. It is possible to remove this information through the ***Document Inspector,*** *a* feature accessed from within Word, Excel, PowerPoint or Visio applications.

3.2.3.4 Backup copies

There is no global solution for backing up Office 365.

Although a mechanism based on "retention policies" in certain cases may be sufficient to ensure the backup of information. See section [3.2.3.1 Qualification of Information] for how they apply to a document and how they can serve to protect it from deletion.

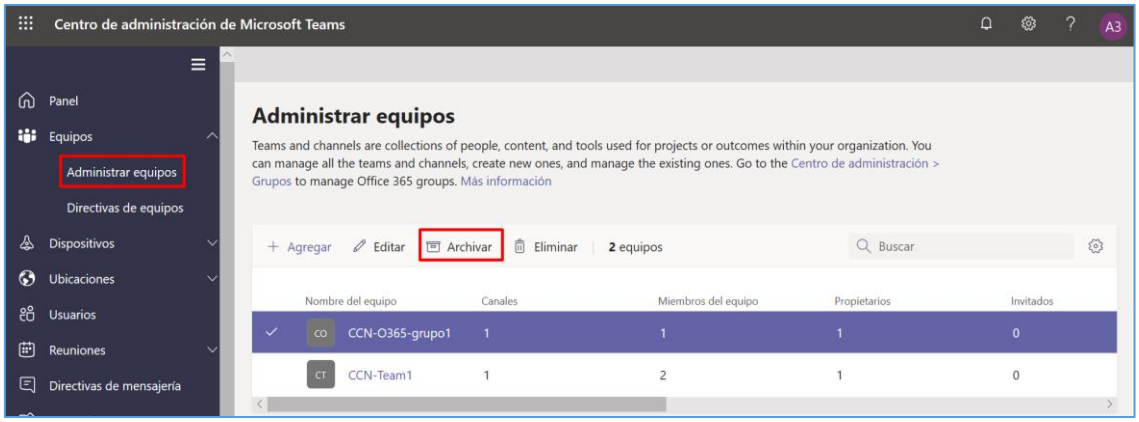
An interesting option related to backup mechanisms is "**Archiving**". Over time, a computer created in Microsoft Teams may become obsolete or you may want to archive or delete a computer at the end of a project.

Archiving a *team in* Microsoft Teams

When you archive a *file,* all activity on that team stops. Archiving a team also archives private channels and their associated site collections. However, you can still add or

remove members and update roles, and you can still view all activity of the team on standard and private channels, archives, and chats.

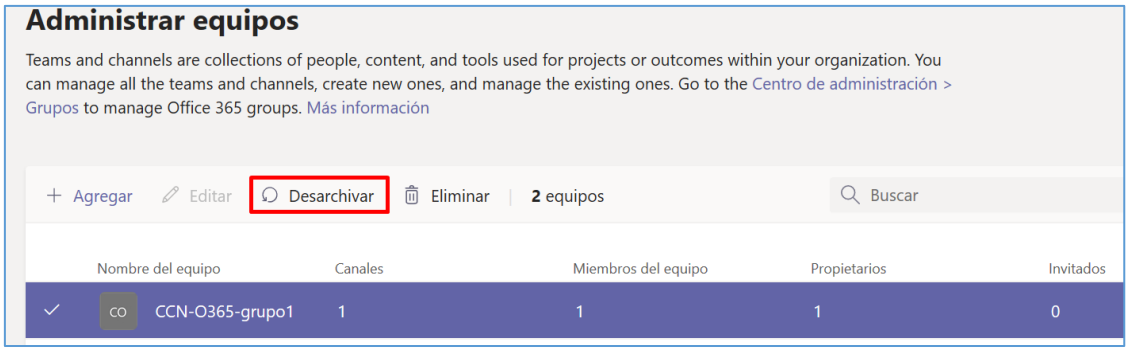
1. In the Microsoft Teams Management Center, select [Teams\Manage tems].
2. Select a team by clicking on the computer name.
3. Choose ***Archive***.



And the following message will appear:

By clicking on "Archive" the status associated to the device will change from "Active" to "Archived".

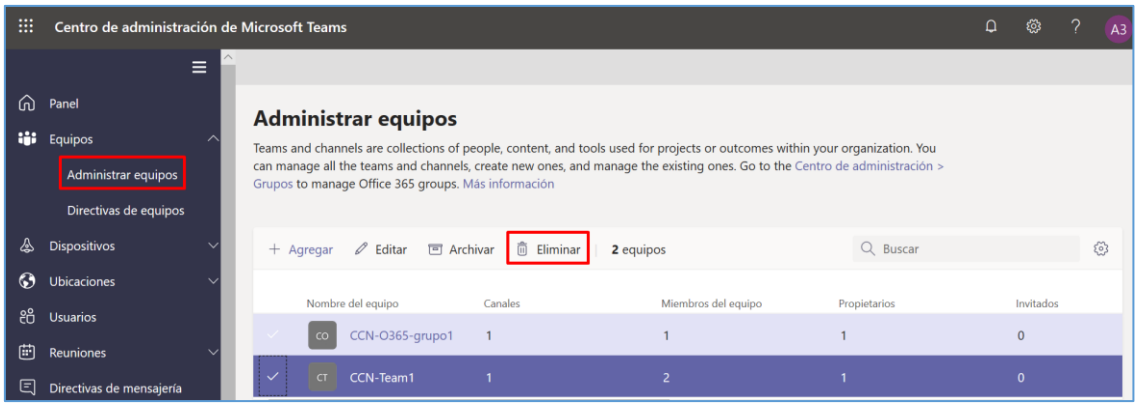
You can undo the operation at any time with the "Unarchive" option:



Remove a *computer* in Microsoft Teams

If the team will not be needed in the future, it can be deleted instead of archived.

1. In the Microsoft Teams Management Center, select [Teams\Manage tems].
2. Select a *team* by clicking on the team's name.
3. Select "Delete". A confirmation message will be displayed.



The operation of **restoring** a team is done by restoring the Office 365 group associated with the team. Restoring the Office 365 group of a team restores the contents of the team, including tabs, standard channels, private channels, and their associated site collections.

By default, a deleted Office 365 group is kept for 30 days.

3.2.4 Protection of services

3.2.4.1 Protection against denial of service

Office 365 provides advanced **threat detection** and **mitigation systems** to protect the underlying infrastructure from *denial of service (*DoS) attacks and prevent customer disruption.

Azure's DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure *tenants*. Exchange Online and SharePoint Online request limitation mechanisms are part of a multi-layered approach to defend themselves against DoS attacks.

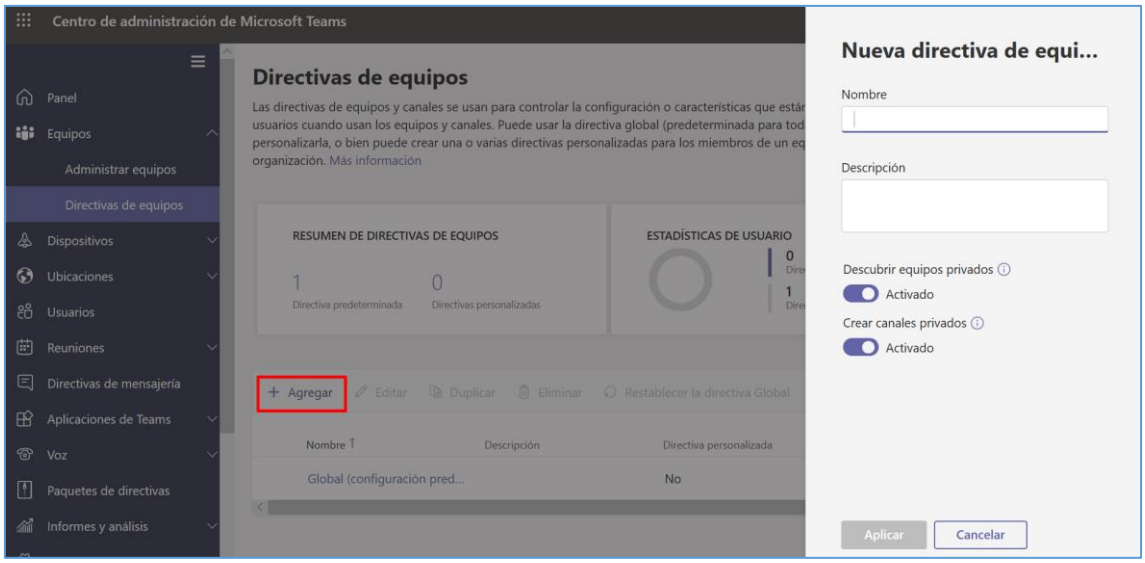
Refer to the guide [CCN-STIC-884A - Secure Configuration Guide for Azure] for more information on *Azure's DDoS defense system*.

4. OTHER SECURITY CONCERNS

From the *Microsoft Teams Administration Center,* you can configure policies of teams, messaging, meetings, applications and voice and control to which users in your organization should be applied. Below are those features that have some relevance to security.

4.1 Teams Policy

Teams and channel policies are used to control the settings or features that are available to users when using teams and channels. You can use global policy (the default for your entire organization) and customize it, or you can create one or more custom policies for members of a team or channel in your organization.



- Discover private teams: Enable this option to allow users to detect private teams in the search results and in the computer gallery.
- Create private channels: Activate this option to allow users to create channels.

4.2 Messaging policies

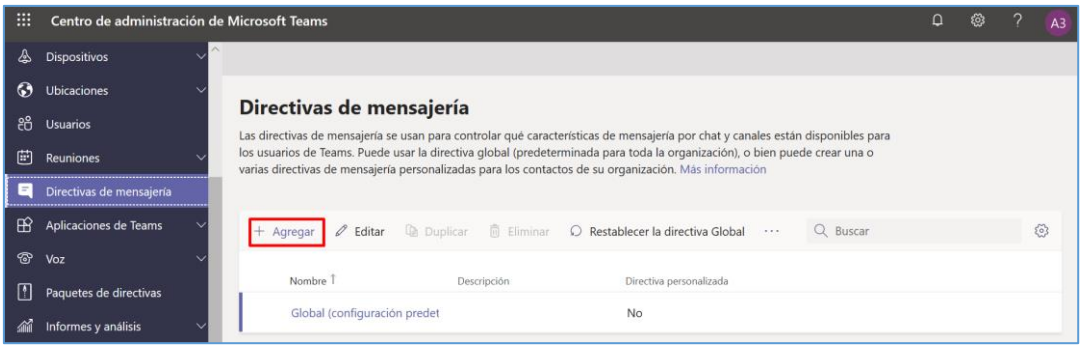
Messaging policies are used to control which chat and channel messaging features are available to Teams' users. You can use the global policy (the default for your entire organization), or you can create one or more custom messaging policies for your organization's contacts.

By default, a **global** policy is created (the default option for the entire organization). All users in your organization will be assigned this messaging policy by default. You can make changes to this policy, or you can create one or more custom policies and assign users to them.

For example, suppose you want to make sure that sent messages are not deleted or modified by users. You should create a new custom policy called "hold sent messages" with the following settings:

- Owners can delete sent messages.
- Users can NOT delete sent messages
- Users can NOT edit sent messages

1. Access the *Microsoft Teams Administration Center. The* [Messaging Policies] menu.
2. Press the "Add" button.

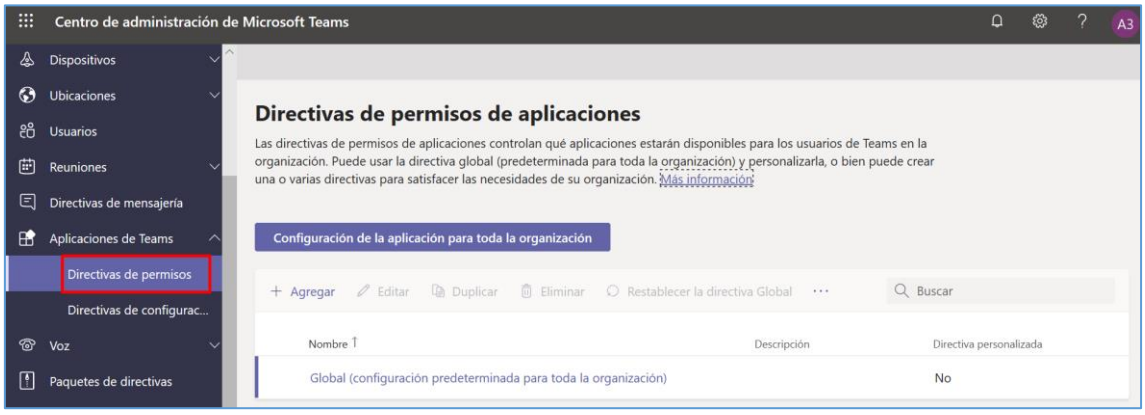


3. Set the options and "Save".

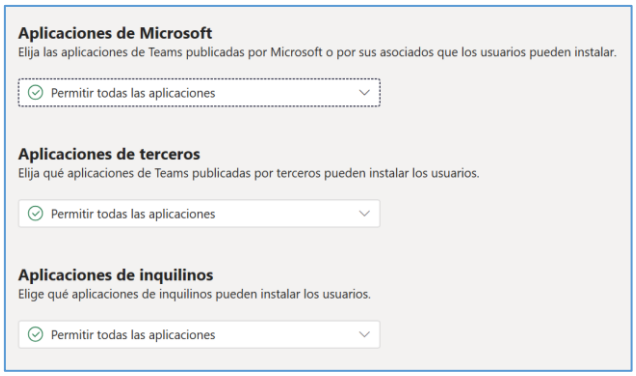
4.3 Application permission policies

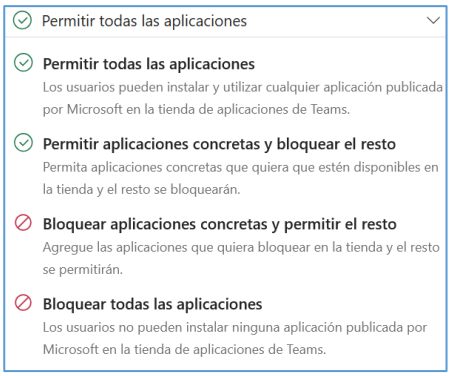
Application permission policies control which applications will be available to Teams' users in the organization. You can use the global policy (default for the entire organization) and customize it, or you can create one or more policies to comply the needs of your organization.

It is accessed from the *Microsoft Teams Administration Center. The* [Teams Applications\Permissions policies] menu.



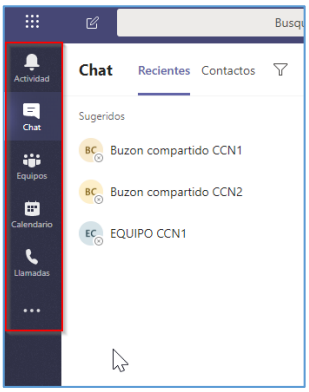
It allows you to configure which Microsoft, third-party, and *Tenant* applications can install the users. It is recommended to enable only those applications that have been tested and authorized by your organization and maintain control over the applications that are published in the store.





4.4 Application Configuration Policies

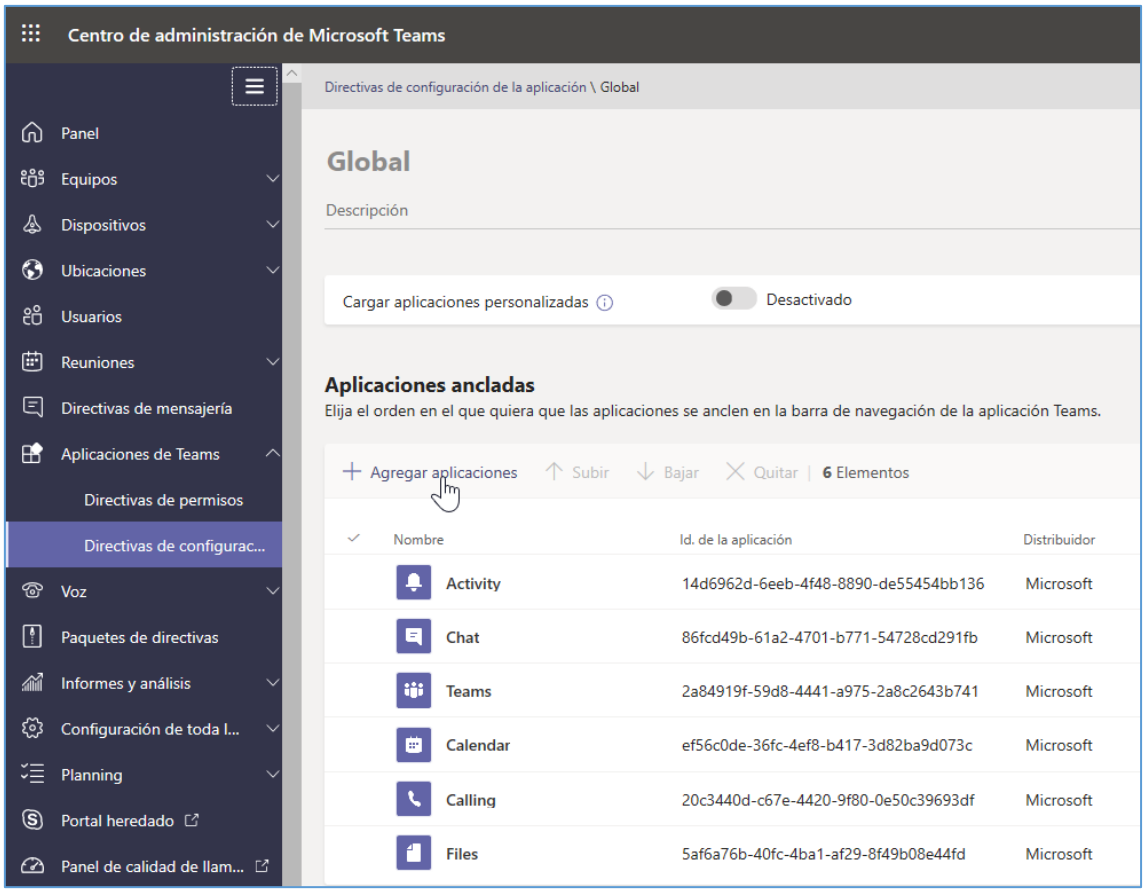
Application configuration policies control how applications are available to the user with the Teams application.



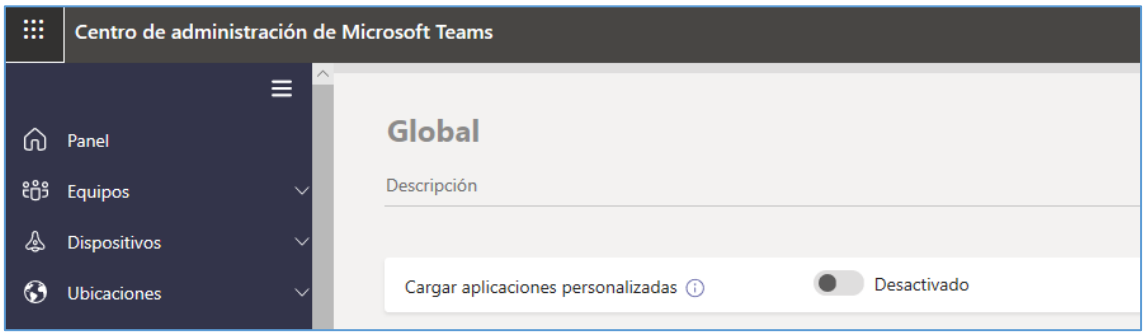
Applications are anchored to the application bar. This is the bar on the side of the Teams desktop client and at the bottom of Teams mobile clients (iOS and Android).

You can use the global policy (the default for the entire organization) and customize it, or you can create custom policies and assign them to a set of users.

It is accessed from the *Microsoft Teams Administration Center. The* [Teams Applications\Configuration policies] menu.



It is recommended to NOT allow "custom application loading".



4.5 Voice Policies

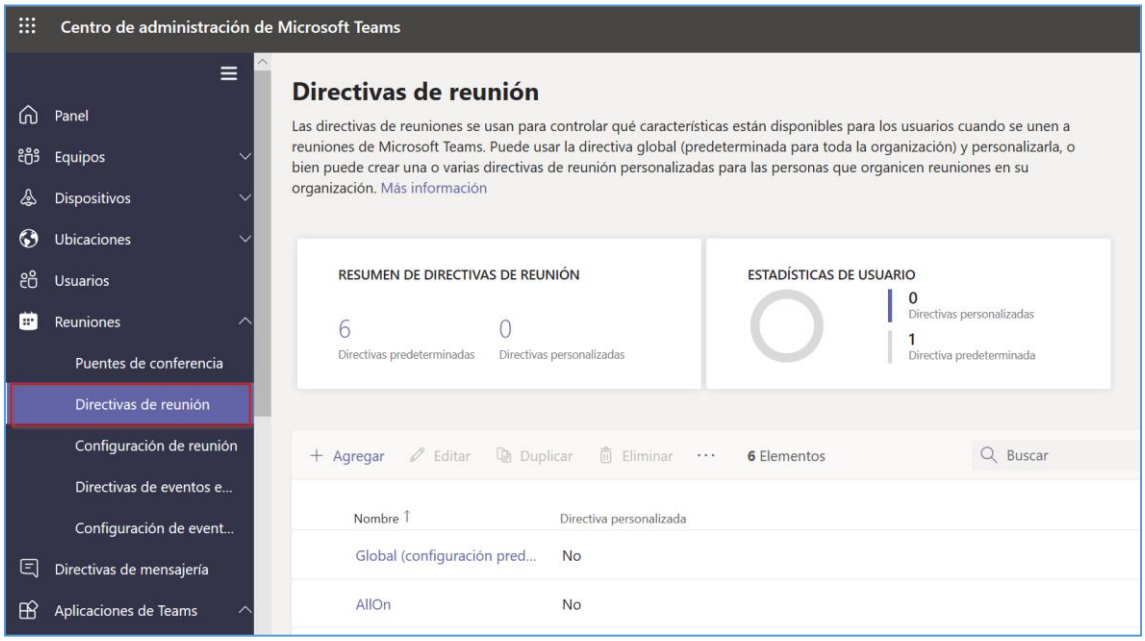
In Microsoft Teams, calling policies control which calling and call forwarding features are available to users. Calling policies determine whether a user can make private calls, use call forwarding or simultaneous ringing to other users or external phone numbers, route calls to voicemail, send calls to Call Groups, use delegation for inbound and outbound calls, and so on.

Note: Microsoft Teams allows to connect the Online service to a local or cloud PBX (Private Branch Exchange), through direct routing. A supported Session Border Controller (SBC) is required. From the security point of view, if your organization plans to integrate this service, you must ensure that SIP communication is encrypted with TLS 1.2.

4.6 Meeting guidelines

Meeting policies are used to control what features are available to users when they join Microsoft Teams meetings.

It is accessed from the *Microsoft Teams Administration Center. The* [Meetings\ Meeting Policies] menu.



You can use the Gobal policy (Org-wide default) and customize it, or you can create one or more custom meeting policies for people who host meetings in your organization.

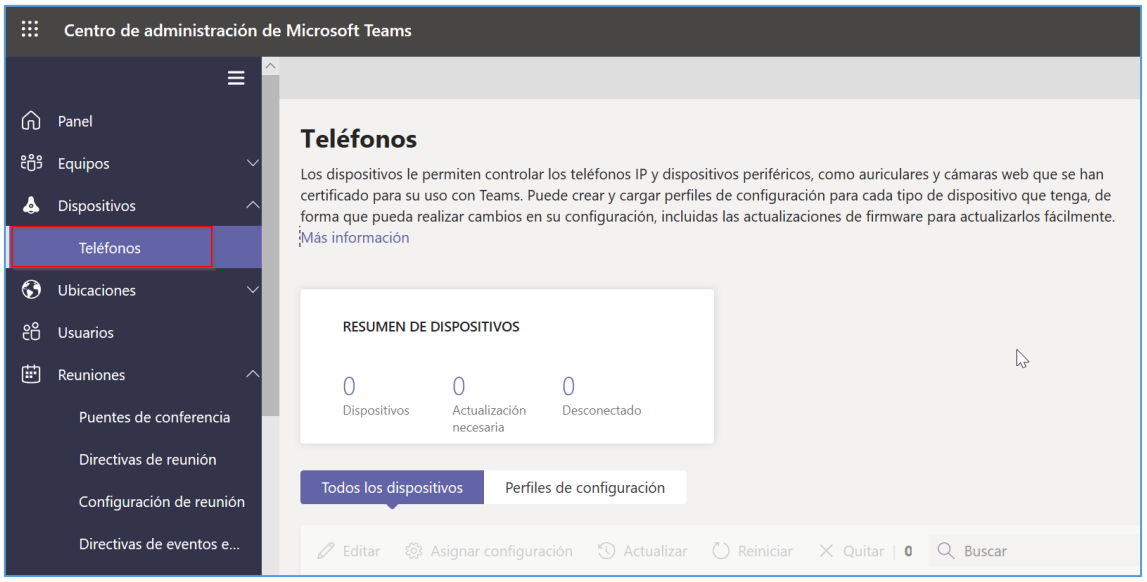
With these policies you can set, for example, blocking for anonymous users, allowing or blocking recording, allowing sharing, etc.

4.7 Device directives

Teams allows to connect devices (IP phones) directly to the service. It is becoming increasingly common to see conference devices and phones being used with Teams.

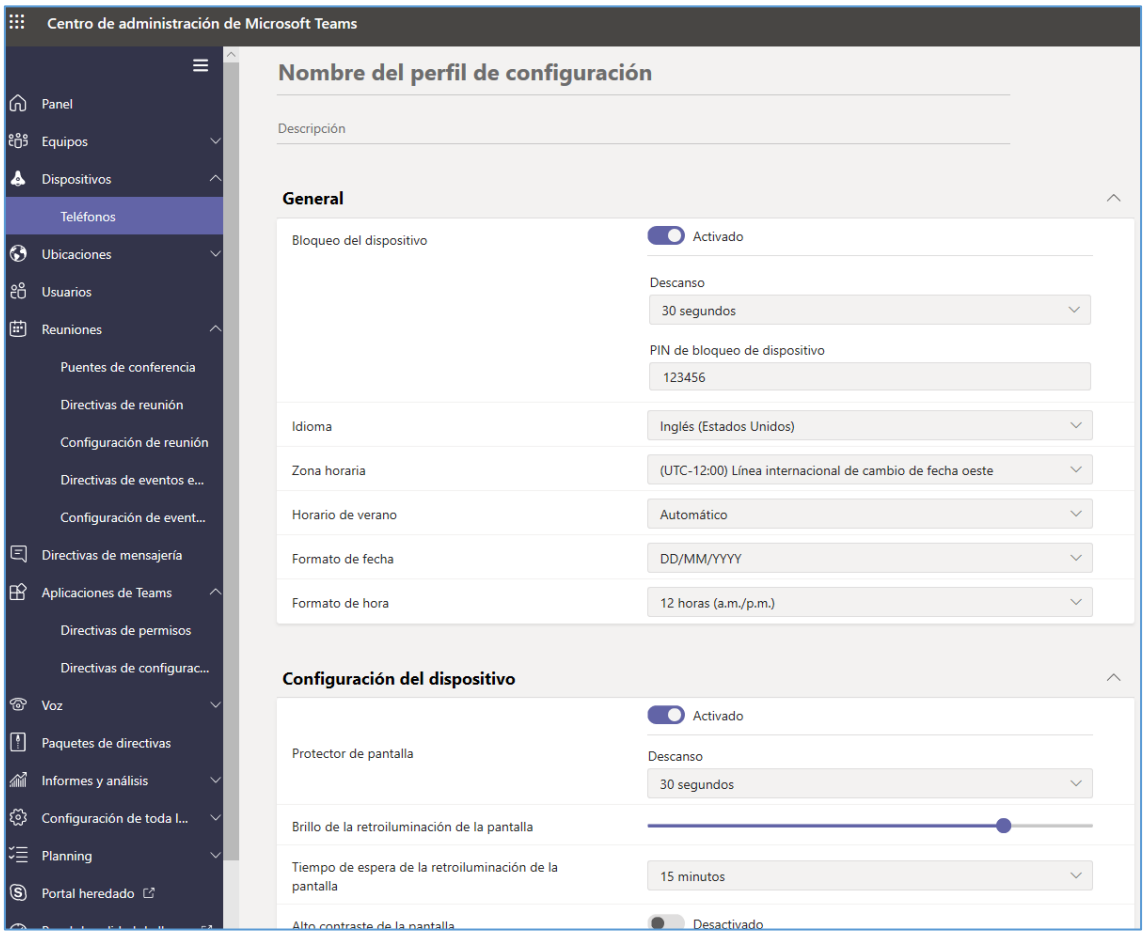
IP phones and peripheral devices such as headsets and webcams that have been certified for use with Teams can be monitored. Configuration profiles can be created and loaded for each type of device in the organization so that changes can be made to their settings.

It is accessed from the Microsoft Teams Administration Center. Menu [Devices\ Phones].



Configuration profiles

From the "Configuration Profiles" tab it is possible to control security options of the device (IP phone) such as lock, PIN, screen saver, logs, etc.



5. SUMMARY TABLE OF SECURITY MEASURES

The following is a summary table of configurations to be applied for the protection of the service, where the organization will be able to evaluate which measures of the proposals are fulfilled.

<table>
<tr><th>ENS Control</th><th colspan="3">Configuration</th><th>Status</th></tr>
<tr><td>op</td><td colspan="4">Operational Framework</td></tr>
<tr><td>op.acc</td><td colspan="4">Access Control</td></tr>
<tr><td rowspan="3">op.acc.1</td><td colspan="4">Identification</td></tr>
<tr><td colspan="2" rowspan="2">The use of accounts and assignment of licenses to users has been configured.
Following the recommendations of Office 365 based on the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365]</td><td>It applies:
☐ Yes ☐ No</td><td>It complies:
☐ Yes ☐ No</td></tr>
<tr><td>Evidence collected:
☐ Yes ☐ No</td><td>Comments:</td></tr>
<tr><td>Op.acc.2</td><td colspan="4">Entry Requirements</td></tr>
</table>

	Resource *permission levels* have been checked: owners and members.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.acc.3	**Segregation of functions and tasks**		
	The administrator roles have been properly assigned (in case a delegation has been established for this service). Following the recommendations of section 3.1.1.3 Segregation of functions and tasks in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365]	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.acc. 4	**Access rights management process**		

	The specific permissions on each of the users of the created computers have been reviewed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.acc.5	**Authentication mechanism**		
	Multi-Factor Authentication (MFA) has been enabled for users in the organization. *Following the recommendations of 3.1.1.5 Authentication Mechanisms in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365]*	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.acc.6	**Local access**		

	The "multi-factor authentication" and/or conditional access policies are enabled, as described in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.acc.6	**Local access**		
	A record of successful and unsuccessful access attempts to the system is available.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.acc.7	**Remote Access**		
	Conditional access policies have been configured for remote access, as described in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No

		Evidence collected: ☐ Yes ☐ No	**Comments:**
op.exp	**Exploitation**		
op.exp.6	**Protection against malware**		
	Real time threat detection, accessible from the *Office 365 Security and Compliance Center,* is checked regularly and a report is generated. * If the organization has *Office 365 Advanced Threat Protection* (Office 365 ATP).	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
op.exp. 8	**Recording user activity**		
	The audit log has been activated.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected:	**Comments:**

		☐ Yes ☐ No	
op.exp. 10	**Protection of activity logs**		
	Consultation of the activity log has been secured by establishing the appropriate roles. *Following the recommendations of section 3.1.2.4 Protection of activity logs in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].*	**It applies:** ☐ Yes ☐ No **Evidence collected:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No **Comments:**
op.mon	**System monitoring**		
	Alerts have been set up in the *Office 365 Security and Compliance Center.* *Following the recommendations of section 3.2.2 System Monitoring in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].*	**It applies:** ☐ Yes ☐ No **Evidence collected:** Yes No	**It complies:** ☐ Yes ☐ No **Comments:**

		☐ ☐	
mp	**Protective Measures**		
mp.info	**Protection of information**		
mp.info.2	**Rating of information**		
	Retention policies have been implemented.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
mp.info.2	**Rating of information**		
	DLP policies have been implemented. *Following the recommendations of section 3.2.3.1.2 DLPs (Data Loss Prevention) in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].*	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected:	**Comments:**

		☐ Yes ☐ No	
mp.info.2	**Rating of information**		
	Sensitivity labels have been applied. *Following the recommendations of section 3.2.3.1 Qualification of information in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365]*	**It applies:** ☐ Yes ☐ No **Evidence collected:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No **Comments:**
mp.info.9	**Backup copies**		
	Archived/deleted *teams* have been checked in Microsoft Teams.	**It applies:** ☐ Yes ☐ No **Evidence collected:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No **Comments:**

mp.s	**Protection of services**		
mp.s.8	**Protection against denial of service**		
	The detailed information in the [CCN-STIC-884A - Azure Secure Configuration Guide] guide on *Azure's DDoS defense system* has been taken into account.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
	OTHER SECURITY CONCERNS		
	Teams policies		
	The teams policies have been reviewed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected:	**Comments:**

		☐ Yes ☐ No	
	Messaging policies		
	The messaging policies have been reviewed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
	Application permission policies		
	The configuration and application permission policies have been reviewed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**

	Meeting policies		
	The meeting policies have been reviewed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
	Device policies		
	The device policies have been reviewed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**