

# Mesures de seguretat d’Office 365



Realitzat per : Unitat de Seguretat

Data: 8/9/2020

# Control del document

Informació general

|  |  |
| --- | --- |
| **Títol:** | Nom del document |
| **Creat per:** | Ivan Caballero |
| **A revisar per:** | Comitè Executiu de Seguretat |
| **A aprovar per:** | Comitè Executiu de Seguretat |
| **Llista de distribució:** |  |
| **Nom del document** | https://llicenciesaoc.sharepoint.com/sites/equipmotordoffice365/documents compartits/seguretat/mesures de seguretat office 365.docx |

Històric de revisions

|  |  |  |  |
| --- | --- | --- | --- |
| **Versió** | **Data** | **Autor** | **Comentaris** |
| 1.0 | 06/03/2019 | Ivan Caballero | Primera versió de document |
|  |  |  |  |
|  |  |  |  |

# Índex

Contenido

[Mesures de seguretat d’Office 365 1](https://llicenciesaoc.sharepoint.com/sites/EquipmotordOffice365/Documents%20compartits/Guia%20interna%20Treball%20Col·laboratiu%20AOC/Mesures%20de%20seguretat%20Office%20365.docx#_Toc40305403)

[1. Control del document 2](#_Toc40305404)

[2. Índex 3](#_Toc40305405)

[3. Introducció 4](#_Toc40305406)

[4. Implementació de seguretat actual 4](#_Toc40305407)

[4.1 General 4](#_Toc40305408)

[1.1.1 Sub-equips d’administració 4](#_Toc40305409)

[1.1.2 Doble factor d’autenticació 4](#_Toc40305410)

[4.2 Sharepoint i OneDrive 5](#_Toc40305411)

[1.1.3 Ús compartit extern 5](#_Toc40305412)

[1.1.4 Risc 5](#_Toc40305413)

[1.1.5 Mesures mitigatòries del risc 5](#_Toc40305414)

[4.3 Teams 7](#_Toc40305415)

[1.1.6 Acces Extern i accés de convidat 7](#_Toc40305416)

[1.1.7 Integracions amb altres serveis d’arxius al Cloud. 7](#_Toc40305417)

[1.1.8 Directives de permisos d’aplicacions 7](#_Toc40305418)

[1.1.9 Directives de reunions 8](#_Toc40305419)

[1.1.10 Stream 8](#_Toc40305420)

[1.1.11 Yammer 10](#_Toc40305421)

# Introducció

# Resum executiu

Proposta:

Doble factor obligatori per a tots el usuaris

El doble factor augmenta molt la seguretat i no és molest pels usuaris ja que si no es tanca la sessió en un dispositiu no demana el doble factor.

Problema: cal posar el telèfon de l’usuari en l’active directory d’Azure. El personal sense telèfon d’empresa pot tenir reticències en fer servir el telèfon personal.

Sharpoint i OneDrive:

* Compartició molt laxe. Risc alt, encara que les dades que nosaltres maneguem són de nivell baix (excepte RRHH) Mesures mitigatories:
  + Caducitat enllaços: aplicar una caducitat per defecte.
  + Consultar a Dani si hi ha alguna directriu que detecti Dades Personals i compartició

# Implementació de seguretat actual

## General

### Sub-equips d’administració

Es poden crear equips d’administració de les diferents aplicacions i assignar rols. El equip motor podria tenir accés (encara que sigui de lectura) al Tenant.

### Doble factor d’autenticació

El doble factor d’autenticació es pot aplicar per usuari.

Es recomana aplicar-ho com a mínim a tots els usuaris administradors.

## Sharepoint i OneDrive

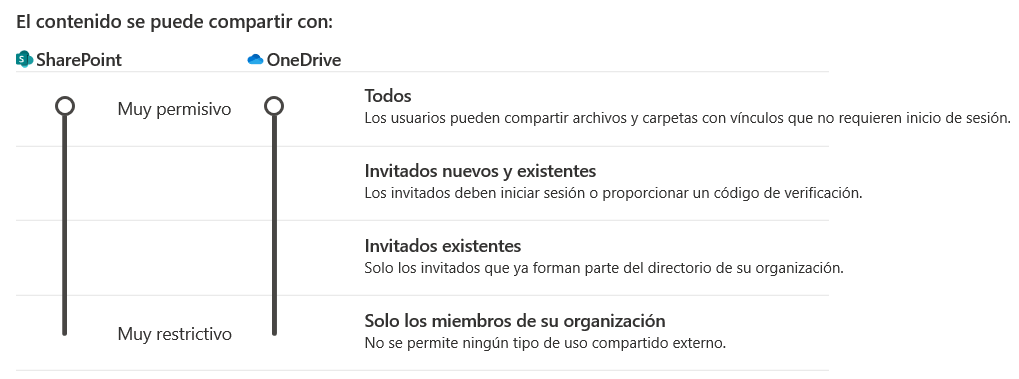
### Ús compartit extern

La configuració per a la compartició de documents marca les directrius mínimes que l’usuari pot escollir per compartir documents.

Un usuari sempre podrà escollir directrius més restrictives. Mai podrà escollir directrius menys restrictives.

Aquestes directrius apliquen per tots els sites de shrepoint i tots els usuaris de OneDrive. No es granular.

La configuració actual és la més permissiva de totes:



Es pot compartir documents amb un vincle al document. No hi ha control d’accés al document.

Es responsabilitat de l’usuari aplicar control d’accés. L’usuari pot escollir exigir control d’accés en el moment de compartir.

### Risc

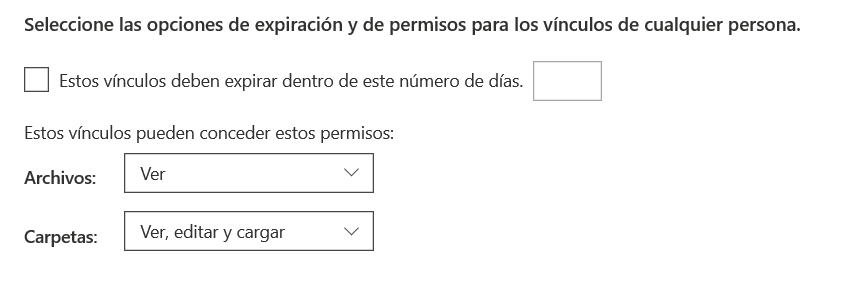
Aquesta configuració es considera que té un risc alt, ja que depèn de l’usuari exigir control d’accés o no.

Només la informació sense requeriments de CONFIDENCIALITAT, AUTENTICITAT, INTEGRITAT i TRAÇAVILITAT s’hauria de compartir sense control d’accés.

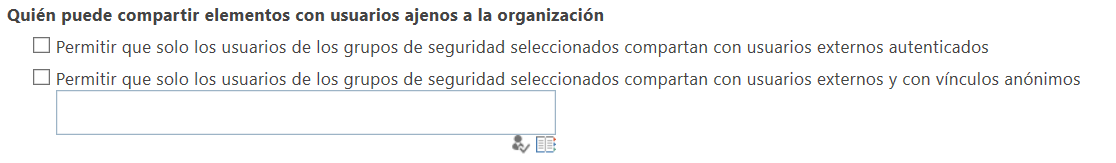
### Mesures mitigatòries del risc

#### Caducitat dels enllaços

Configurar que els enllaços caduquin en el temps.



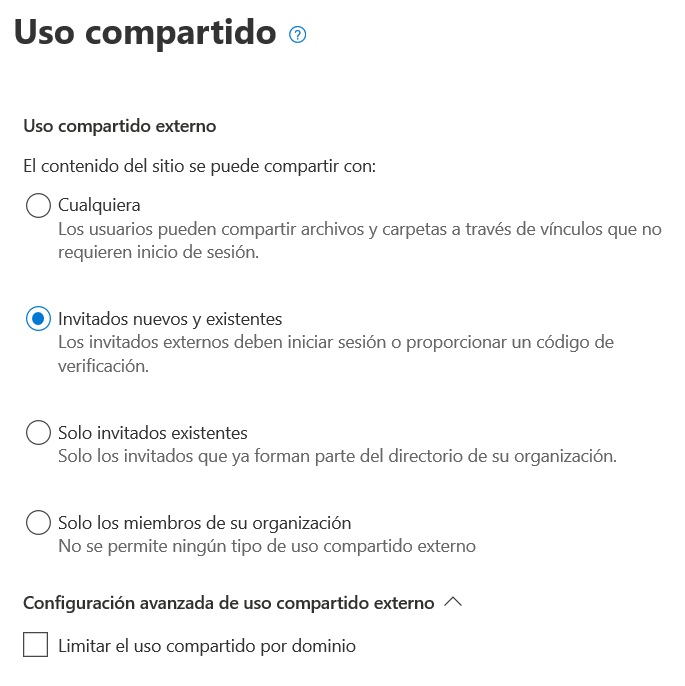
#### Restringir els enllaços anònims a un grup d’usuaris



#### Restringir que els usuaris puguin crear sites

Si la creació de sites ho fan els Administradors de Sharepoint, aquests poden imposar polítiques més restrictives per site.

Les polítiques dels sites es poden canviar en qualsevol moment:



#### Report d’arxius compartits

Pendent de veure si es possible

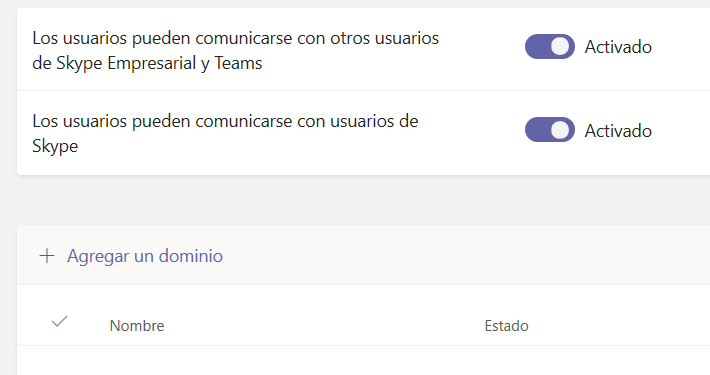
## Teams

### Acces Extern i accés de convidat

L’accés extern és poder reunir-se, trucar o chatejar amb qualsevol usuari extern. El usuaris extern no es poden afegir a equips o canals.

L’accés de convidat és l’accés de personal extern que ha sigut explícitament convidat per un usuari de l’AOC. El usuaris convidats es poden afegir a equips i canals i altres recursos.

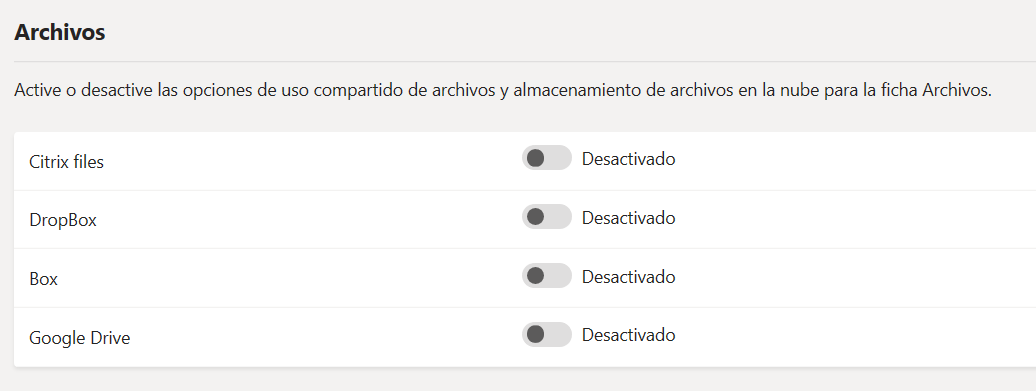
L’accés extern està permès per qualsevol domini.



L’accés de convidat està permès amb totes funcionalitats activades.

### Integracions amb altres serveis d’arxius al Cloud.

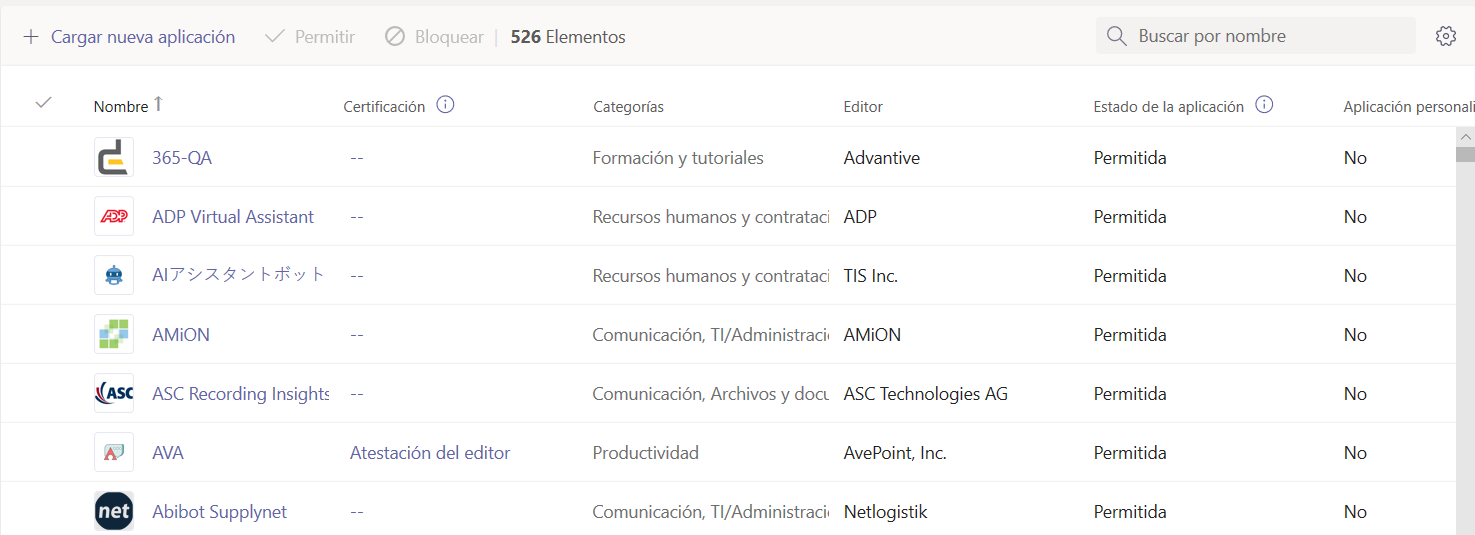
Teams es pot integrar altres serveis d’arxivament al núvol. Actualment desactivats.



Es recomana desactivar aquestes opcions donat que no són serveis corporatius

### Directives de permisos d’aplicacions

Les directives de permisos d’aplicacions controlen quines aplicacions estan disponibles pels usuaris

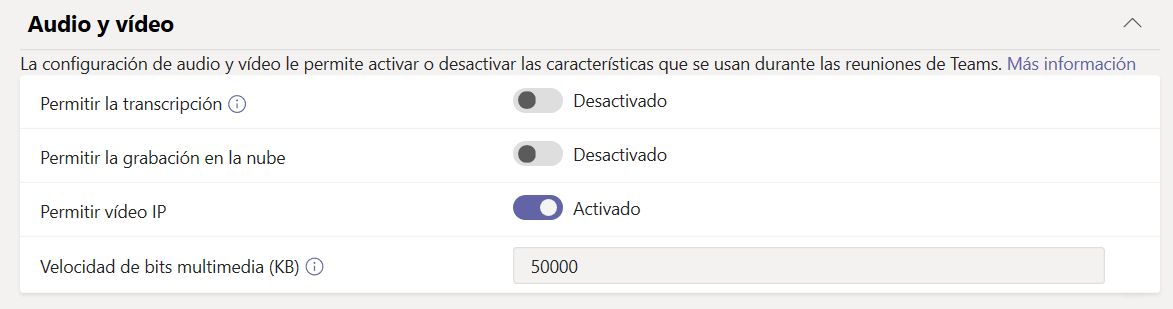


Les aplicacions poden ser de tercers. Demanen accés a les dades i tenen polítiques de privacitat pròpies. Haurien d’estar aprovades per Seguretat.

### Directives de reunions

La gravació de la reunió està desactivada.

Hauria d’estar desactivat fins que mirem con es guarden les gravacions dins de STREAM



## Stream

Consola d’administració: <https://web.microsoftstream.com/admin>

Documentació de l’aplicació: <https://docs.microsoft.com/es-es/stream/admin-overview>

Els usuaris administradors han de tenir llicència d’Offcice.

* + 1. Compartició de vídeos

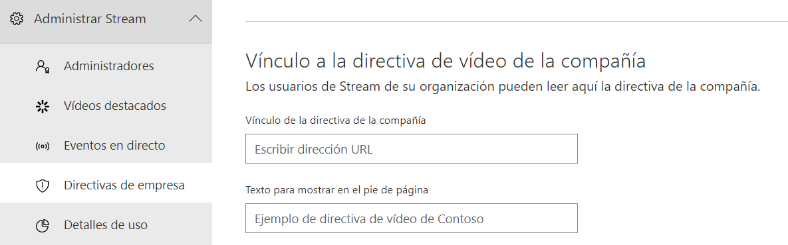
La compartició de vídeos d moment només es pot fer amb usuaris interns, segons la següent nota:

Microsoft Stream todavía no admite escenarios de uso compartido externo para invitados o personas fuera de la organización. Sabemos que estas características son muy necesarias y estamos trabajando en planes para crear estas características.

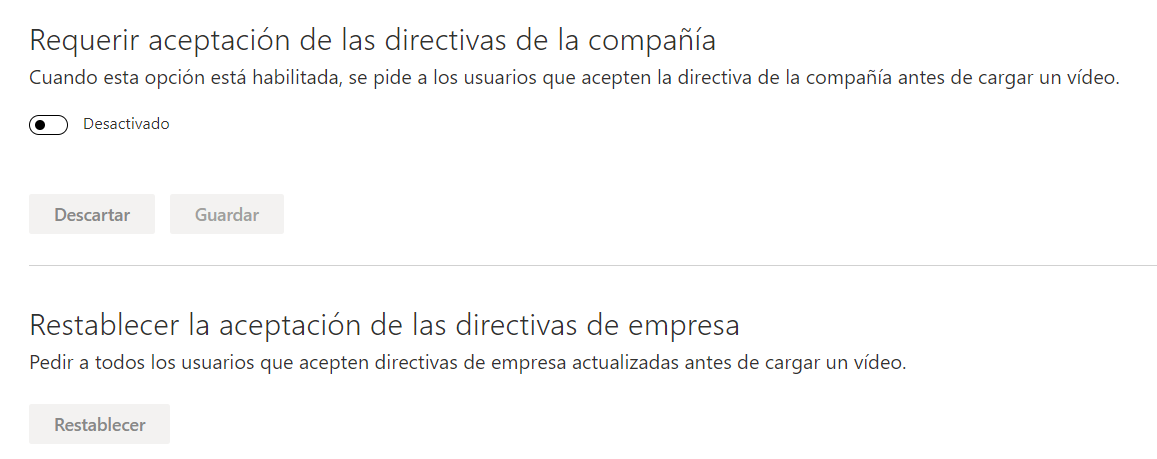
La compartició amb usuaris d’AOC es pot fer i **el vídeos són descarregables**.

* + 1. Directives d’empresa

Es pot afegir una URL de notificació de directives d’empresa

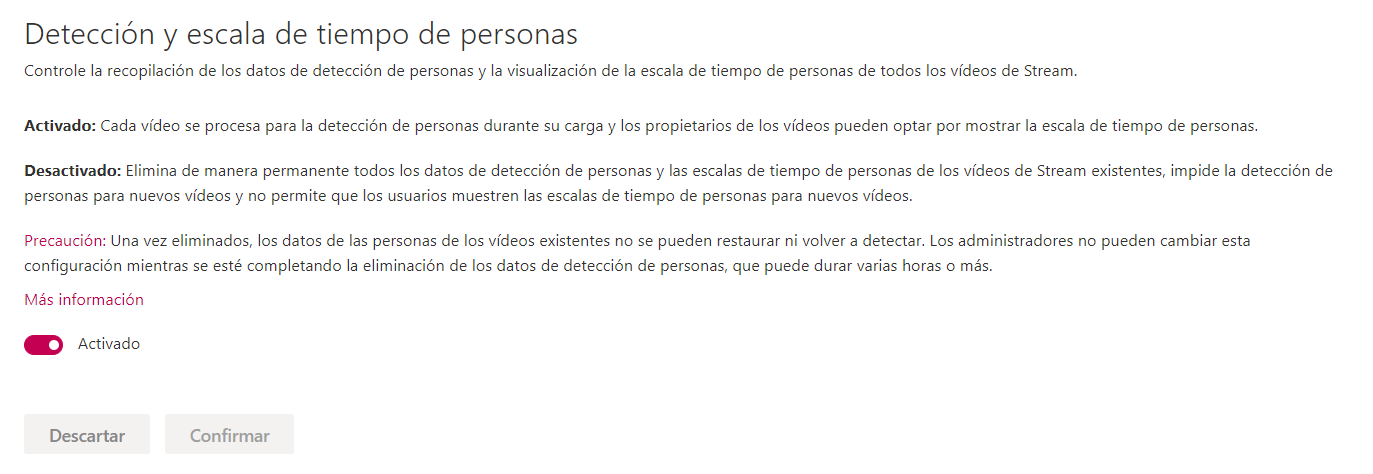


Es pot requerir l’acceptació de la directiva d’empresa abans de poder pujar un vídeo.

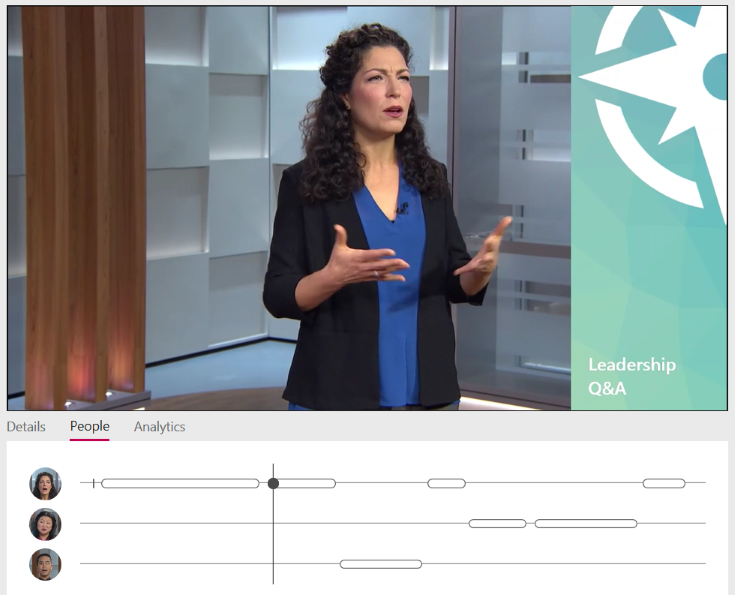


Quan un vídeo s’esborra s’envia a una paperera de reciclatge durant 30 dies.

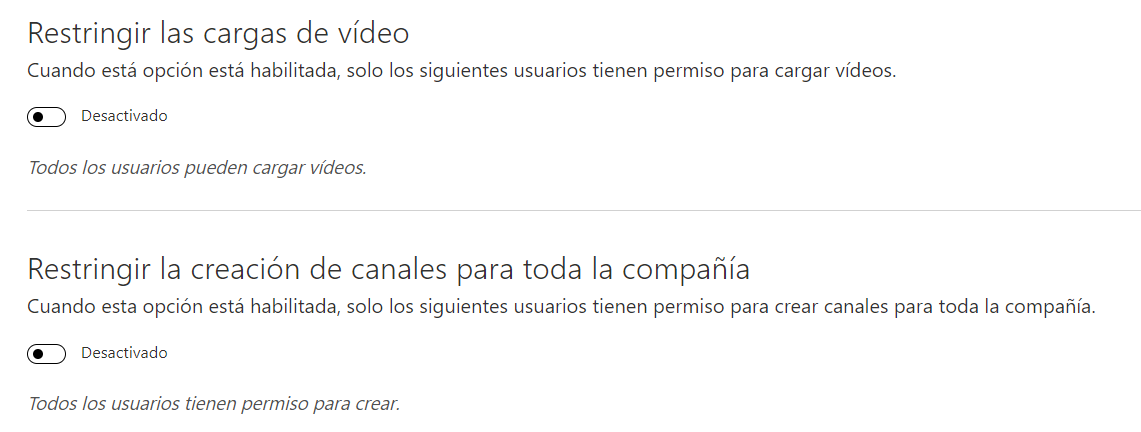
Té un sistema de identificació de persones. Els propietaris del vídeo tenen la opció de mostrar la escala de temps.



La escala de temps mostra els fragments del vídeo on intervé cada participant:



Per defecte tots el usuaris poden carregar vídeos i crear canals. Es pot restringir a uns usuaris concrets.



## Yammer