* Veure com està l'usuari Admin global del Tenant. Hauria d'estar Deshabilitat i amb la contrasenya controlada.

[Administrador@aoc.onmicrosft](mailto:Administrador@aoc.onmicrosft) 🡪 ya està deshabilitada. La restauración de la contraseña se tiene que pedir a Microsft.

* Consulta sobre obertura d'arxius ubicats al sharepoint des de pàgines web. (Veure missatge de Jordi Fernandez).
* Necessitat d'un Backup extern

Hay 2 papeleras de 1er nivel y 2o.

* Como tenemos que gestionar los grupos de TEAMS para que no se nos descontrolen. Los sitios de sharepoint también estan abriertos a los usuarios

Cuando una persona quiera crear un equipo de 365:

* Flujo de aprovadores en PowerApps. El usuario hace una petición en PowerApps y alguien la aprueba y se crea automàticament.
* Petición via tiquet

El grupo es Admins\_O365\_Groups 🡪 aquí tienen que estar como miembros los que tengan permisos para crear equipos de 365 (Teams, Sharepoint, etc.)

*Nota: los grupos de Seguridad se creac en el centro de administración, no en el Azure.*

* Avís a usuaris per missatges a la cua de quarantena

Repositori de RRHH seguretat ampliada.

El repositori de RRHH és el que té dades més sensibles del Consorci AOC.

Quina configuració de seguretat ampliada es proposa? Per exemple:

* Accés només pel grup de RRHH.
* Administració només pel grup de RRHH. En cas de necessiten que ens puguin donar accés temporal.
* Que els documents no puguin sortir de sharepoint. Que no es puguin compartir.
* Traçabilitat d'accessos

Les carpetes de RRHH són les següents:

Les més crítiques:

* Expedients personals
* Nomines
* Regim Disciplinari
* Relacions laborals

Propostes dels manuals de CCN

Se recomienda la detección de amenazas en tiempo real, accesible desde el Centro de Seguridad y cumplimiento de Office 365.

Se ha activado el registro de auditoría.

Como evitar que los usuaris instalen aplicaciones de terceros en el TEAMS?

En la directives està que solo se pueden añadir aplicaciones de Microsoft. Las de terceros estan desactivades.

Cerrar sesiones inactivas en Sharepoint. 🡪 ya està activado. En Directivas – control de acceso. Se cierra en 30 minutos.

Seguridad:

Se ha activado el paquete de Seguridad:

[Administrar programaciones - Centro de seguridad y cumplimiento (office.com)](https://protection.office.com/insightdashboard)

En alertas està loqui se tiene que tratar:

[Panel - Cloud App Security - Microsoft Cloud App Security](https://llicenciesaoc.portal.cloudappsecurity.com/#/dashboard)

Esta consola se puede ver por la licencia: Microsoft 365 E5 Security

La licencia Microsoft 365 E5 Security da estas propiedades:

Azure Active Directory Premium P2

Microsoft 365 Defender

**Microsoft Cloud App Security 🡪 hay otra licencia que tiene esta característica per va a caducar.**

Microsoft Defender For Endpoint

Microsoft Defender for Identity

Microsoft Defender for Office 365 (Plan 2)

Office 365 SafeDocs

Se puede añadir eventos de otros dispositives de Seguridad, correla los eventos y da un informe mas completo. És la creación de instantaneas:

[Crear nuevo informe de instantáneas - Cloud App Security - Microsoft Cloud App Security](https://llicenciesaoc.portal.cloudappsecurity.com/#/discovery/create-new-report/)

En “Investigar” estan las cosas que se tienen que mirar.

En Directivas està lo que

Consejos:

Las consolas de Security y Cloud Prtections son las mas usades:

[Security recommendations - Seguridad de Microsoft 365](https://security.microsoft.com/security-recommendations)

El de cloud security engloba los 3 centros de Seguridad.