centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 885ES

ESCENARIO DE NUBE PARA EL MANEJO DE INFORMACIÓN SENSIBLE EN MICROSOFT OFFICE 365

OCTUBRE 2021

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.10.01 13:19:51 +02'00'

P.º de la Castellana 109, 28046 Madrid

NIPO: 083-21-175-6

Fecha de Edición: octubre de 2021
Plain Concepts y Sidertia han participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

octubre de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

La aparición y uso de nuevas tecnologías emergentes que permiten la implementación de las Tecnologías de la Información y las Comunicaciones (TIC), en adelante sistemas, en escenarios basados en nube has provocado que su implementación en esta modalidad se vuelva crítica en todos sus ámbitos.

Las amenazas asociadas a un sistema, que pueden afectar a la confidencialidad, integridad y disponibilidad de la información manejada, o a la propia integridad y disponibilidad del sistema, son tenidas en cuenta a la hora de establecer los requisitos de seguridad mínimos, de tal manera, que las medidas de protección que se implementan tienen por objeto hacer frente a dichas amenazas reduciendo la superficie de exposición y minimizando el impacto de estas.

La seguridad se tratará desde la fase de diseño del sistema, donde se definirán las salvaguardas a implementar, permitiendo de esta manera que el análisis y gestión de riesgos de seguridad estén presentes en el proceso de desarrollo del sistema.

2. OBJETO

El presente documento tiene como finalidad establecer las medidas de seguridad específicas que se requieren para implementación de un entorno seguro de Microsoft 365.

Durante el desarrollo de la presente guía de implementación se proporcionarás aspectos específicos de aplicación, recomendaciones de seguridad y buenas prácticas, necesarias para la prevención de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestas las infraestructuras y sistemas implementados basados en servicios de nube.

3. ALCANCE

Para el desarrollo del presente documento se toma como base la aplicación de medidas de seguridad sobre Microsoft 365, concretamente sobre el uso de diversas funcionalidades y/o productos relacionados con esta línea de servicios por suscripción.

Durante los siguientes apartados se definirá de forma específica todo el proceso de despliegue, implementación y configuración de seguridad de todos los productos de los cuales ser hará uso teniendo en consideración su aplicación y funcionalidad.

Este manual contempla la implementación de una PoC (Proof of Concept.) de aprovisionamiento y configuración segura de un entorno basado de forma exclusiva en la nube (Cloud).

Durante el desarrollo de la PoC se tratará de automatizar no solo el despliegue si no también la configuración de los servicios, siempre que la tecnología lo permita, con el objetivo de establecer un modelo de implementación que pueda ser trasladado a otros organismos de la manera más rápida y organizada posible. Por ello, junto al presente manual se anexan scripts, plantillas e indicaciones que permitan esta labor.

3.1 DESCRIPCIÓN DE CASOS DE USO

Para el desarrollo, implementación y aplicación de medidas de seguridad de los diversos productos y servicios es necesario poner en contexto el uso que van a proporcionar. Las utilidades y funcionalidades que pueden aportar los servicios de Microsoft 365 pueden ser muy

variados y diversos. No obstante, esta guía de implementación y configuración de seguridad se ceñirá a unas necesidades y casos de uso concretos.

Nota: Esta guía no contempla el uso de los servicios de Microsoft 365 fuera de los escenarios que se presentan a continuación.

3.1.1 COLABORACIÓN CON EMPRESAS, AAPP, UNIVERSIDADES

En la Institución hay organismos que se encargan de ejecutar proyectos, y éstos necesitan colaborar con empresas. Adicionalmente, hay organismos que mantienen relaciones de colaboración con Universidades y AAPP. De este tipo de relaciones, surgen necesidades de mantener una agenda común, un lugar donde poder subir ficheros y poder trabajar con ellos de forma colaborativa, mantener conversaciones en común, intercambiar correo y coordinar eventos y videoconferencias. La ubicuidad en el acceso a estos servicios se convierte en fundamental (podrían hacerlo mediante un móvil corporativo allá donde estén) y los servicios de TEAMS pueden mejorar la situación actual.			
Situación actual	Solución	Valor	Partes interesadas
Actualmente esta gestión se realiza desde un puesto de usuario en una red desconectada de Internet. La salida del correo es auditada y tiene que ser aprobada por una cadena de aprobación. En todo caso, este intercambio es lento y tedioso. Adicionalmente no existe una agenda común, ni la posibilidad de editar los ficheros de forma colaborativa. La convocatoria de eventos se realiza con un sistema de videoconferencia centralizado y desconectado en el sentido de que se realizan con cuentas independientes al correo de colaboración.	Tener un Equipo y un Canal en TEAMS y poder Invitar a una empresa externa, podría facilitar la comunicación, la integración y la inmediatez de la colaboración.	Beneficio probable del usuario y beneficio para la Institución: – Rapidez en las comunicaciones. – Ubicuidad. – Mayor capacidad de coordinación y organización. – Gestionan y mantener menos infraestructura para colaborar en Internet.	Empresas colaboradoras Organismos de ejecución. Instituciones y AAPP. Organismos de formación.

A continuación, se describen los requisitos funcionales para el desarrollo del caso de uso presentado:

a) Existe un usuario avanzado de la Institución que lidera un grupo de colaboración.

b) Esta colaboración está sustentada en un Canal de TEAMS.

c) Existen N usuarios estándar de la Institución que van a colaborar.

d) Existen N usuarios externos invitados, no pertenecientes a la Institución que van a colaborar.

e) El usuario avanzado necesita ayuda de un miembro de IT para crear un Equipo y un Canal.

f) El usuario avanzado puede añadir miembros al canal, pero para invitar a un usuario externo al TENANT, necesita ayuda de un miembro de IT.

g) El usuario avanzado tiene capacidad de invitar tanto a otros usuarios como a invitados externos al Canal.

h) El usuario avanzado puede configurar el canal para añadir un sitio de intercambio de ficheros, comunicaciones y anuncios, planificación de tareas y eventos comunes, conversación del canal.

i) Los usuarios pueden formar un Equipo. Estos usuarios tienen permiso en N canales y pueden pertenecer a M equipos.

j) Los invitados pueden formar o no otro Equipo.

k) Existe un canal creado donde los usuarios y los invitados pueden subir ficheros, añadir comunicaciones, establecer tareas en una agenda común y mantener conversaciones en el canal.

l) En este canal se pueden convocar audio/Videoconferencias.

3.1.2 SOPORTE

Uno de los tipos de colaboración con empresas más habitual es la gestión de trabajos, no sólo en proyectos, sino también en contratos de soporte y mantenimiento de instalaciones o gestión TIC. En TEAMS existen aplicaciones y posibilidades de utilizar workflows que de forma colaborativa permitirían a las empresas, ofrecer a la Institución información actualizada sobre el progreso de su proyecto o trabajo. La Institución a su vez, podría poner incidencias o peticiones de servicio a las empresas por TEAMS.			
Situación actual	Solución	Valor	Partes interesadas
No existe nada parecido. Se envían documentos ofimáticos por correo en una gestión totalmente offline. Hay empresas que tienen sitios donde tramitar casos de soporte, pero no todas tienen esa infraestructura, y las que disponen de ella, esta infraestructura está compartida por el resto de los usuarios de sus servicios, obligando a realizar tareas de sanitización profunda de la información.	Tener un canal asociado a un servicio de una empresa. En este canal se puede establecer agenda, comunicación de incidencias, eventos, avisos, etc. Así mismo los usuarios de la institución podrían abrir incidencias o peticiones de servicio a las empresas y ver su progreso en tiempo real.	Beneficio probable del usuario y beneficio de la Institución: – Estado de los trabajos en tiempo real. – Ubicuidad. – Mejor coordinación y organización. – No hay que mantener un sitio de ticketing por cada empresa.	Empresas. Organismos ejecutantes.

A continuación, se describen los requisitos funcionales para el desarrollo del caso de uso presentado:

a) Existe un usuario avanzado de la Institución que lidera un grupo de soporte.

b) Este soporte está sustentado en un canal de TEAMS.

c) Existen N usuarios estándar de la Institución que van a tener acceso.

d) Existen N usuarios externos invitados, no pertenecientes a la Institución que van a colaborar.

e) El usuario avanzado necesita ayuda de un miembro de IT para crear un Equipo y un Canal.

f) El usuario avanzado puede añadir miembros al canal, pero para invitar a un usuario externo al TENANT, necesita ayuda de un miembro de IT.

g) El usuario avanzado tiene capacidad de invitar tanto a otros usuarios como a invitados

externos al Canal.

h) El usuario avanzado puede configurar el canal para añadir un sitio de intercambio de ficheros, comunicaciones y anuncios, planificación de tareas y eventos comunes, conversación del canal y ticketing.

i) Los usuarios pueden formar un Equipo. Estos usuarios tienen permiso en N canales y pueden pertenecer a M equipos.

j) Los invitados pueden formar o no otro Equipo.

k) Existe un canal creado donde los usuarios y los invitados pueden subir ficheros, añadir comunicaciones, establecer tareas en una agenda común y mantener conversaciones en el canal.

l) Los usuarios estándar del canal pueden abrir incidencias y peticiones de servicio a la empresa. Los usuarios invitados reciben una notificación de la incidencia.

m) Todos los usuarios pueden listar las incidencias del servicio y consultar el estado de las peticiones de servicio realizadas.

n) Los invitados pueden crear avisos de servicio y asociarlos a eventos de la agenda, lanzando las correspondientes notificaciones a los usuarios.

o) En este canal se pueden convocar audio/Videoconferencias.

3.1.3 FORMACIÓN

La Institución tiene un grupo dedicado de personas a gestionar, coordinar y planificar las actividades formativas. Este grupo establece colaboraciones con fines formativos con Organismos públicos y con instituciones académicas públicas y privadas. A raíz de esas colaboraciones aparece la posibilidad de organizar un curso de formación tanto a usuarios externos como internos de la Institución, así como poder examinarlos y llevar un control de asistencia. También es posible organizar cursos a usuarios externos pertenecientes a otras AAPP o Instituciones académicas.			
Situación actual	Solución	Valor	Partes interesadas
Actualmente existen dos escenarios distintos: cursos que un profesor externo da al personal de la Institución y cursos que el personal de la Institución ofrece a personal externo (otras AAPP, instituciones y empresas). En los cursos actuales el personal externo tiene que desplazarse a las instalaciones de la Institución, tanto si va a dar como recibir formación. Asimismo, los cursos sólo son accesibles desde el puesto de usuario de la Institución, no estando accesibles desde sus móviles o tablets. Por otra parte, para dar cursos a usuarios externos, éstos tienen que desplazarse a las instalaciones de la Institución. Por todo lo anterior, se necesita no sólo evitar los desplazamientos, sino poder hacer uso de los cursos en todo momento, en cualquier lugar.	Dar la posibilidad de materializar un curso en TEAMS.	Beneficio probable del usuario y beneficio para la institución: – Inmediatez y autonomía del uso de medios. – Ubicuidad. – Menos desplazamientos físicos. – Menos mantenimiento de infraestructura infrautilizada.	Personal de Formación. Personal de otras instituciones públicas y académicas. Usuarios.

A continuación, se describen los requisitos funcionales para el desarrollo del caso de uso presentado:

a) Existe un usuario avanzado de la Institución que va a organizar un curso de formación.

b) La formación debe estar implementada en un Canal de TEAMS.

c) Existen N usuarios estándar de la Institución que van a participar en el curso.

d) Existen N usuarios externos invitados, no pertenecientes a la Institución que van a participar en el curso.

e) El usuario avanzado necesita ayuda de un miembro de IT para crear un Canal para el curso.

f) El usuario avanzado puede añadir miembros al canal, pero para invitar a un usuario externo al TENANT, necesita ayuda de un miembro de IT.

g) El usuario avanzado tiene capacidad de invitar tanto a otros usuarios como a invitados externos al Canal.

h) Existe la figura del profesor. En caso de ser un curso dado por personal de la Institución (usuario del TENANT) puede ser el mismo que el usuario avanzado. En caso contrario, el profesor sería un usuario invitado.

i) El curso tendrá cinco etapas diferenciadas en su gestión: preparación, bienvenida, ejecución, examen.

j) PREPARACION: El usuario avanzado genera la plantilla del curso y la estructura general y coordina con el profesor las siguientes acciones:

   i. Crear el contenido del curso en TEAMS.

   ii. Crear exámenes con Forms.

   iii. Definir los equipos de trabajo.

   iv. Configurar el entorno de TEAMS.

k) A modo de ejemplo de lo anterior: el profesor puede configurar el canal del curso para añadir pestañas por cada día del curso y por cada equipo del curso. Ejemplo:

   i. General.

   ii. Día 1.

   iii. Dia 2.

   iv. Dia N.

   v. Equipo 1.

   vi. Equipo 2.

   vii. Equipo N.

l) BIENVENIDA: El usuario avanzado y el profesor coordinan la realización de las siguientes acciones:

   i. Enviar invitaciones al curso.

   ii. Configurar mensaje de Bienvenida al curso en TEAMS.

   iii. Enviar los prerrequisitos del curso.

   iv. Contestar y atender preguntas antes del curso.

m) El usuario avanzado y el profesor coordinan la realización de las siguientes acciones:

i. Establecer la agenda del curso y crear el aula virtual principal.
ii. Crear el aula virtual de cada equipo del curso (opcional) para que los equipos queden cada día.
iii. Lanzar las invitaciones.
iv. Crear encuestas o Forms para tener datos de partida de los participantes.
v. Utilizar ONENOTE de TEAMS para compartir datos sobre el curso.
vi. Utilizar el chat de la reunión para interactuar con los participantes.
vii. Utilizar el botón de 'People' para visualizar participantes y habilitar/deshabilitar el audio.
viii. Interactuar con el botón de 'Shared screen'.
ix. Grabar las sesiones para tenerlas guardadas para futuras sesiones.
x. Guardar la asistencia al curso con el plugin 'Attendance Report' o utilizando el Attendance PowerApp.

n) EXAMEN: el profesor puede considerar que el curso necesita un examen. Para ello seguirá las siguientes etapas:
i. Preparar un examen con el plugin 'Forms' y configurando sus opciones (aleatorizar orden, bolsa de preguntas, puntos, preguntas abiertas, establecer la duración del examen, etc.).
ii. Establecer la videoconferencia en el aula virtual principal para poder ver y oír a todos los alumnos.
iii. Invitar a todos los participantes a entrar en el aula virtual principal.
iv. Asegurarse de que todos tienen el micro y la cámara encendidos.
v. Lanzar el examen: añadir una pestaña en el subcanal general que enlace con el Forms y lanzar un aviso general a los alumnos.
vi. POSIBILIDAD: utilizar la APP 'Take a Test' de Windows 10, que bloquea el equipo para mostrar sólo el Test.
vii. POSIBILIDAD: utilizar el 'TEAMS CARROUSEL', que permite ir visualizando las cámaras de los participantes uno a uno cada X segundos.
viii. Corregir el examen, ver estadísticas y publicar los resultados a los participantes opcionalmente.

3.1.4 ENTREVISTAS Y PRUEBAS

El personal de la institución tiene la necesidad de convocar y organizar entrevistas a uno o varios usuarios invitados. Estas entrevistas se realizarían mediante audio/videoconferencia con una o varias aulas virtuales simultáneas. En otras palabras: se necesita organizar un gran número de entrevistas y pruebas, que además necesitarían ser convocados con anterioridad para poder planificar las tareas y el personal de la Institución que lo atiende. Es importante que el usuario invitado conozca qué entrevistas tienen en el día/semana. También es necesario que durante la entrevista se puedan realizar pruebas, intercambiar archivos con trabajos a realizar y visualizar la correcta ejecución de los mismos.

El personal de la institución tiene la necesidad de convocar y organizar entrevistas a uno o varios usuarios invitados. Estas entrevistas se realizarían mediante audio/videoconferencia con una o varias aulas virtuales simultáneas. En otras palabras: se necesita organizar un gran número de entrevistas y pruebas, que además necesitarían ser convocados con anterioridad para poder planificar las tareas y el personal de la Institución que lo atiende. Es importante que el usuario invitado conozca qué entrevistas tienen en el día/semana. También es necesario que durante la entrevista se puedan realizar pruebas, intercambiar archivos con trabajos a realizar y visualizar la correcta ejecución de los mismos.			
Situación actual	Solución	Valor	Partes interesadas
Hasta ahora las entrevistas con el personal externo se realizan de forma virtual, pero con un sistema de videoconferencia, una agenda global en papel y un sistema de intercambio de archivos y un sistema de realización de exámenes, todo ello con sistemas distintos.	Mediante un canal de TEAMS con capacidad de invitar a usuarios externos, organizar una agenda, asignar tareas a los invitados y crear audio/videoconferencias para tener entrevistas con ellos. Asimismo, mediante una aplicación de tareas, se puede llevar una hoja de control de las tareas pendientes por interno y una planificación en la vista de calendario de la aplicación de tareas. Adicionalmente, con el plugin de Microsoft Forms integrado en TEAMS u otro equivalente, se pueden hacer exámenes integrados en la gestión del proceso de selección en TEAMS.	Beneficio probable del usuario y beneficio de la Institución: – Se evitan desplazamientos innecesarios. – Mejora la organización. – Mejora la capacidad de reacción. – Ubicuidad. – Abaratamiento de medios. – Menor coste.	Personal de la Institución. Personal externo.

A continuación, se describen los requisitos funcionales para el desarrollo del caso de uso presentado:

a) Existe un usuario avanzado de la Institución que va a organizar una tanda de entrevistas y pruebas.

b) El usuario avanzado debe poder implementarlo todo en un Canal de TEAMS.

c) Existen N usuarios estándar de la Institución que van a participar como entrevistadores: realizando las entrevistas y vigilando las pruebas.

d) Existen N usuarios externos invitados, no pertenecientes a la Institución, que van a participar.

e) El usuario avanzado necesita ayuda de un miembro de IT para crear un Canal.

f) El usuario avanzado puede añadir miembros al canal, incluso para invitar a un usuario externo al TENANT.

g) Las pruebas tendrán cinco etapas diferenciadas en su gestión: preparación, bienvenida, ejecución del test, ejecución de entrevistas y ejecución de pruebas por equipos.

h) PREPARACION: El usuario avanzado genera la plantilla del curso y la estructura general y coordina con los entrevistadores las siguientes acciones:

   i. Configurar el entorno de TEAMS.

   ii. Definir los equipos de trabajo.

   iii. Establecer tareas con planner para cada uno de los entrevistadores (posiblemente los siguientes pasos sean tareas).

   iv. Crear el contenido de las pruebas en TEAMS.

   v. Preparar un test con el plugin 'Forms' configurando sus opciones (aleatorizar orden, bolsa de preguntas, puntos, preguntas abiertas, establecer la duración del examen, etc.).

   vi. Crear las aulas virtuales.

i) A modo de ejemplo de lo anterior: el usuario avanzado puede configurar el canal del curso para añadir pestañas por cada día de las pruebas y por cada equipo del curso. Ejemplo:

   i. General.

   ii. Día 1.

   iii. Dia 2.

   iv. Dia N.

   v. Equipo 1.

   vi. Equipo 2.

   vii. Equipo N.

j) BIENVENIDA: El usuario avanzado y el entrevistador coordinan la realización de las siguientes acciones:

   i. Enviar invitaciones a los participantes en las pruebas.

   ii. Configurar mensaje de Bienvenida en TEAMS.

   iii. Enviar los prerrequisitos y las indicaciones de las pruebas.

   iv. Contestar y atender preguntas antes de los participantes antes de las pruebas.

v. Revisar la agenda global de las pruebas y las individuales de los participantes.

k) EJECUCIÓN del TEST: El usuario avanzado y el entrevistador, ejecutan las siguientes acciones:

i. Establecer la videoconferencia en el aula virtual principal para poder ver y oír a todos los alumnos.

ii. Invitar a todos los participantes a entrar en el aula virtual principal.

iii. Asegurarse de que todos tienen el micro y la cámara encendidos.

iv. Lanzar el test: una pestaña en el subcanal general que enlace con el Forms y lanzar un aviso general a los participantes.

v. POSIBILIDAD: utilizar la APP 'Take a Test' de Windows 10, que bloquea el equipo para mostrar sólo el Test.

vi. POSIBILIDAD: utilizar el 'TEAMS CARROUSEL', que permite ir visualizando las cámaras de los participantes uno a uno cada X segundos.

vii. Corregir el examen, ver estadísticas y enviar los resultados a los participantes opcionalmente.

viii. Utilizar ONENOTE de TEAMS para compartir indicaciones sobre la prueba.

ix. Utilizar el chat del aula para interactuar con los participantes.

x. Los participantes no pueden chatear entre ellos.

xi. Utilizar el botón de 'People' para visualizar participantes y habilitar/deshabilitar el audio.

l) EJECUCIÓN DE ENTREVISTAS: el usuario avanzado y los entrevistadores ejecutan las siguientes etapas:

i. Establecer la agenda de las entrevistas e iniciar el aula virtual general y las aulas auxiliares.

ii. Lanzar las invitaciones y verificar que las agendas son correctas sin solapes.

iii. Los participantes van siendo convocados a cada aula auxiliar, cuando terminan la entrevista, vuelven al aula general.

iv. Utilizar el chat de la reunión para interactuar con los participantes.

v. Utilizar el botón de 'People' para visualizar participantes y habilitar/deshabilitar el audio.

vi. Interactuar con el botón de 'Shared screen'.

vii. (opcional) Grabar las entrevistas para tenerlas guardadas para futuras sesiones.

m) EJECUCIÓN DE PRUEBAS EN GRUPO: el usuario avanzado y los entrevistadores ejecutan las siguientes etapas:

i. Definir grupos de participantes.

ii. Crear las asignaciones a las pestañas de 'Equipo N' a cada grupo.

iii. Crear las aulas virtuales para cada grupo.

iv. Utilizar ONENOTE de TEAMS para compartir indicaciones sobre la prueba.

v. Utilizar el chat del aula para interactuar con los participantes.

vi. Lanzar un aviso a los participantes para que comiencen las pruebas.

vii. Utilizar el botón de 'People' para visualizar participantes y habilitar/deshabilitar el audio.

viii. (opcional) Grabar las entrevistas para tenerlas guardadas para futuras sesiones.

3.1.5 AUDITORÍA

En un momento dado puede existir la necesidad de realizar un seguimiento de las actividades de un usuario sobre el TENANT de TEAMS. En este caso los administradores de seguridad deben tener la posibilidad de gestionar (iniciar/verificar/terminar) un caso de seguridad con acceso al máximo de información posible. Adicionalmente, sería necesario una generación de alertas con envío de notificaciones a la Red Corporativa			
Situación actual	Solución	Valor	Partes interesadas
Actualmente las actividades de un usuario se pueden auditar en los sistemas de la Institución. En TEAMS no se dispondría acceso a estos datos puesto que los tiene Microsoft.	Configurar las opciones de DLP y eDiscovery para que los administradores de seguridad puedan detectar una anomalía y en su caso, empezar una investigación.	Beneficio probable del usuario y beneficio para la Institución: – Monitorización de seguridad sin implementar infraestructura propia. – Reducción de los recursos necesarios en la operación de la seguridad.	Administradores de seguridad.

3.1.6 INTERCAMBIO DE INFORMACIÓN CON LA RED CORPORATIVA

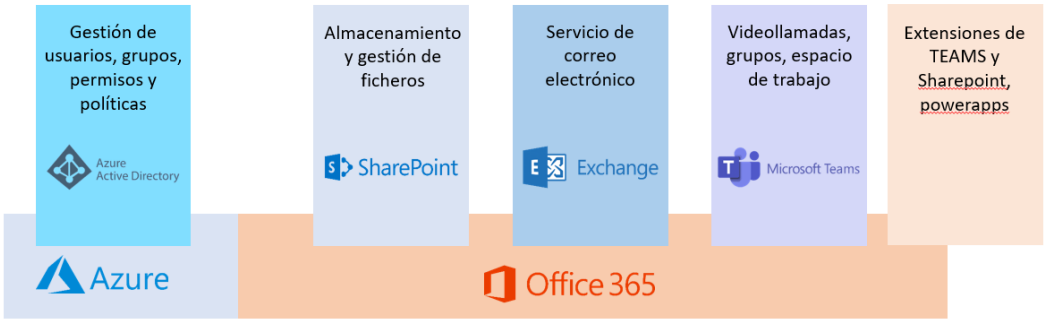
La red Corporativa de la Institución está aislada de Internet de manera que un usuario desde su puesto de trabajo no puede hacer login en TEAMS. Adicionalmente, en TEAMS los ficheros deben estar cifrados por IRM, por lo que si se envían ficheros de TEAMS hacia la red corporativa, utilizando los mecanismos actuales, el usuario no podrá abrir sus documentos en la red corporativa. Los usuarios de la red corporativa tienen que ser capaces de acceder en la Red corporativa a información de TEAMS de forma ágil.			
Situación actual	Solución	Valor	Partes interesadas

La red Corporativa de la Institución está aislada de Internet de manera que un usuario desde su puesto de trabajo no puede hacer login en TEAMS. Adicionalmente, en TEAMS los ficheros deben estar cifrados por IRM, por lo que si se envían ficheros de TEAMS hacia la red corporativa, utilizando los mecanismos actuales, el usuario no podrá abrir sus documentos en la red corporativa. Los usuarios de la red corporativa tienen que ser capaces de acceder en la Red corporativa a información de TEAMS de forma ágil.			
Los ficheros se introducen en la red corporativa mediante mecanismos desconectados y de auditoría. Existe la posibilidad de en un equipo de Internet, mover un archivo a una carpeta y que este archivo sea trasladado automáticamente a la red corporativa.	Tiene que existir una correspondencia entre la identidad del usuario de TEAMS y el usuario de la red Corporativa. El usuario de la Red Corporativa puede cifrar y descifrar. El usuario de TEAMS puede descifrar según las reglas del IRM sólo cuando las reglas del administrador de seguridad lo determinen.	Beneficio probable del usuario y beneficio de la Institución: – Seguridad de la información. – Habilita el uso de la nube de forma ágil. – Control sobre quién tiene acceso a la información.	Usuarios generales. Administradores de seguridad.

3.2 DESCRIPCIÓN DE SERVICIOS CONTEMPLADOS

Para el desarrollo de los diferentes casos de uso expuestos con anterioridad, dentro de los múltiples servicios que ofrece Microsoft 365 se hará uso de forma principal de la plataforma Teams. Este servicio es dependiente de otros, por lo que no se implementará ni trabajará de forma independiente si no que hará uso de otros servicios, como Azure, SharePoint Online y Exchange Online.

Las configuraciones aplicadas sobre estos servicios se basan en las guías de configuración segura del CCN-CERT, concretamente sobre las guías de la serie 800, orientadas a la configuración de seguridad para el cumplimento del ENS.



4. CONFIGURACIONES DE SEGURIDAD DE MICROSOFT 365

Teniendo en consideración el objetivo de la implementación y las tecnologías participantes dentro de la PoC, se describen a continuación todas las medidas de seguridad a aplicar por cada uno de los servicios desplegados.

Las medidas recogidas en esta guía representan un compendio de las recogidas en el conjunto de guías CCN-STIC 884 y CCN-STIC 885 relativas a la configuración de seguridad de servicios de Azure y Office 365.

Nota: Bajo el documento "CCN- Nube Sensible - Despliegue - Tareas v1.0" se definen de forma más amplia las medidas aplicadas y consideraciones a tener en cuenta.

4.1 TENANT

A continuación, se exponen todas las medidas de aplicación sobre el tenant de Azure.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Configuración de Azure AD	Habilitar cierre de sesión por inactividad	Habilitado a 30 minutos.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Bloquear el acceso al portal Azure de los usuarios	Bloqueado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Registro de aplicaciones	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Conexiones con cuenta de Linkedin	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Usuarios invitados pueden invitar a otros usuarios.	Solo los usuarios asignados a roles de administrador específicos pueden invitar a otros usuarios.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Restricciones de colaboración	Permitir que se envíen invitaciones solo a dominios específicos.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Los usuarios pueden restablecer su propia contraseña	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Los usuarios pueden crear grupos de seguridad en los portales de Azure	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Aplicaciones empresariales	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Aplicaciones empresariales	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Configuración de Azure AD	Configuración del dispositivo	Un miembro de IT.	El valor recomendado no interfiere con ningún caso de uso.
Configuración de Azure AD	Configuración del dispositivo	Habilitado.	El valor recomendado no interfiere con ningún caso de uso.
Identidades	Aprovisionamiento de cuentas de ADMINISTRADORES	Todas las cuentas de administrador tendrán MFA activado.	El valor recomendado no interfiere con ningún caso de uso.
Identidades	Aprovisionamiento de cuentas de USUARIOS INTERNOS	Todas las cuentas de usuario tendrán MFA activado y un nivel de licencia adecuado a sus funciones.	El valor recomendado no interfiere con ningún caso de uso.
Identidades	Asignación de licencias a usuarios	Asignación de licencias en función de las necesidades, intentando que las funcionalidades se ajusten a la función a realizar por el usuario	El valor recomendado no interfiere con ningún caso de uso.
Inicio de sesión	Usuarios creados automáticamente por el sistema	Deshabilitar el inicio de sesión en cuentas sin licencia.	El valor recomendado no interfiere con ningún caso de uso.
Mecanismo de autenticación	Configuración métodos de MFA	Microsoft authenticator y mensaje de texto	El valor recomendado no interfiere con ningún caso de uso.
Mecanismo de autenticación	Asignación MFA	Todos los usuarios, tanto internos como externos tendrán Microsoft Authenticator y mensaje de texto.	El valor recomendado no interfiere con ningún caso de uso.
Contraseñas	Definición políticas de contraseñas	No expirarán nunca.	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Contraseñas	Definición políticas de contraseñas	Mínimo 9 caracteres, mayúsculas y minúsculas, un número y un carácter especial.	El valor recomendado no interfiere con ningún caso de uso.
Segregación de funciones	Asignación de roles a usuarios	Se utilizará el principio del menor privilegio. No es necesario crear roles adicionales, sino asignar los ya existentes en función de las necesidades.	El valor recomendado no interfiere con ningún caso de uso.
Control de tiempo de acceso	Acortar el tiempo de validez del token de autenticación	Habilitar la evaluación continua del acceso(CAE)	El valor recomendado no interfiere con ningún caso de uso.
Monitorización	Periodicidad de revisión de reports y logs	Semanalmente: Intentos de sesión fallidos, usos de aplicación, reseteos de contraseña, cambios en grupos de roles, reglas de reenvío de correos, grupo de administradores no globales y dominios suplantados. Bisemanalmente: Acceso al correo por parte de no propietarios, malware, registros de aprovisionamiento.	El valor recomendado no interfiere con ningún caso de uso.
Monitorización	Creación de alertas	Es recomendable usar todas las políticas de alertas predefinidas, además de definir específicas en función de las necesidades.	El valor recomendado no interfiere con ningún caso de uso.
Registro de actividad de los usuarios	Activación del registro de auditoría	Habilitado	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Registro de actividad de los usuarios	Activación del registro de auditoría en los buzones	Habilitado	El valor recomendado no interfiere con ningún caso de uso.
Calificación de la información	Retención	Habilitado	El valor recomendado no interfiere con ningún caso de uso.
Calificación de la información	Prevención de pérdida de datos	Habilitado	El valor recomendado no interfiere con ningún caso de uso.
Calificación de la información	Sensitivity labels	Creación de etiquetas automáticas además de algunas que cumplan con algunos requisitos como x tipo de información confidencial(DNIs, CIFS, que aparezcan ciertas palabras, etc.)	El valor recomendado no interfiere con ningún caso de uso.
Cifrado	Sensitivity labels que apliquen cifrado	Se recomienda la utilización de etiquetas, configurando estas mismas para que cifren los archivos y los marquen añadiendo encabezados, marcas de agua etc	El valor recomendado no interfiere con ningún caso de uso.
Protocolos	Protocolos básicos de autenticación	Habilitar protocolos modernos, deshabilitando los básicos.	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Configurar idioma y zona horaria	UTC + 01:00	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Activar caja de seguridad de Microsoft	Habilitado.	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Configuración del tenant	Compartición externa	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Aplicaciones accesibles a los usuarios en el portal	Todas bloqueadas salvo Teams y Outlook.	Para los casos de uso de formación y entrevistas será necesario habilitar One Note y Forms.
Configuración del tenant	Branding de marca	Añadir un logo corporativo y sustituir el de 365 por defecto.	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Servicios y complementos		
Configuración del tenant	Aplicaciones de terceros que requieren consentimiento del usuario	Desactivar que los usuarios puedan consentir que aplicaciones tengan acceso a datos de la organización	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Permitir que los usuarios compartan su calendario con personas ajenas	Deshabilitado.	Para los casos de uso entrevistas y pruebas y colaboración se podría compartir el calendario con unos niveles de detalles específicos, por ejemplo: Compartir un evento en concreto, hora y lugar o compartir el calendario completo.
Configuración del tenant	Activar enlaces seguros	Habilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Activar adjuntos seguros	Habilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Aplicaciones y servicios que son propiedad del usuario	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Aplicaciones y servicios que son propiedad del usuario	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Configuración del tenant	Office en la web	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.

4.2 SHAREPOINT ONLINE

A continuación, se exponen todas las medidas de aplicación sobre SharePoint.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Segregación de funciones	Asignar rol de Admin a un usuario administrador de SharePoint		El valor recomendado no interfiere con ningún caso de uso.
Proceso de gestión de derechos de acceso	Crear “niveles de permisos” específicos para la organización		El valor recomendado no interfiere con ningún caso de uso.
Autenticación	Bloquear autenticación legacy para SharePoint	Bloquear	El valor recomendado no interfiere con ningún caso de uso.
Protección frente a código dañino	Bloquear que los usuarios puedan ejecutar scripts personalizados en sitios personales y en sitios creados por ellos mismos.	Bloquear	El valor recomendado no interfiere con ningún caso de uso.
Protección frente a código dañino	Configuración parámetros ATP	Habilitado.	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido externo	Limitar el uso compartido externo por dominio.	Activado, solo se añadirán excepciones cuando se necesite en los casos de uso.	Para los casos de uso que requieran compartición externa, se agregarán los dominios a la whitelist hasta que termine la colaboración, una vez finalizada, sería necesario borrar la autorización.
Uso compartido externo	El contenido se puede compartir con	Invitados existentes.	Habría que crear cuentas de invitado para dar acceso a los usuarios autorizados para los casos de uso.
Uso compartido externo	Permitir que sólo los usuarios de grupos de seguridad específicos puedan compartir.	Activado.	Habría que añadir a las cuentas que se requiera a los grupos de seguridad para poder compartir.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Uso compartido externo	Permitir a los invitados compartir elementos que no son de su propiedad.	Desactivado.	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido externo	Las personas que usan un código de verificación deben volver a autenticarse después de estos días	1	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido externo	Tipo de vínculo predeterminado	Solo miembros de su organización	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido externo	Cierre de sesión inactiva	15 minutos de inactividad	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido externo	Tipo de permisos predeterminados del vínculo	Lectura	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido externo	Aplicaciones que no usan la autenticación moderna.	Bloquear	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido externo	Permitir el acceso solo desde determinadas direcciones IP.	Configurado con las direcciones IP que sean necesarias.	Para los casos de uso que se requiera habría que agregar las direcciones IP correspondientes para evitar el bloqueo y una vez terminada la colaboración, borrar de la lista.
Integración con yammer	Bloquear la integración con Yammer	Bloquear	El valor recomendado no interfiere con ningún caso de uso.
Integración con delve	Bloquear la integración con Delve	Deshabilitar Delve y las características relacionadas	El valor recomendado no interfiere con ningún caso de uso.
Blogs personales	Crear blogs personales	Deshabilitar blogs personales	El valor recomendado no interfiere con ningún caso de uso.
Creación de sitios	Ocultar el comando de creación de sitio	No permitir crear sitios manualmente.	El valor recomendado no interfiere con ningún caso de uso.
Creación de subsitios	Ocultar el comando de creación de subsitios	No permitir crear subsitios.	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Servicios conectados	Limita las características de SharePoint que intentan conectarse a otros servicios.	Bloquear flujos de trabajo de SharePoint 2013	El valor recomendado no interfiere con ningún caso de uso.
Configuración de archivos	Sincronización de archivos	Bloquear todas excepto las necesarias.	El valor recomendado no interfiere con ningún caso de uso.

4.3 EXCHANGE ONLINE

A continuación, se exponen todas las medidas de aplicación sobre Exchange.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Protección de correo electrónico	Habilitar políticas de seguridad preestablecidas(estrictas)	Habilitadas	El valor recomendado no interfiere con ningún caso de uso.
Protección de correo electrónico	Deshabilitar autenticación básica	Deshabilitado.	El valor recomendado no interfiere con ningún caso de uso.
Protección de correo electrónico	Analizador de configuración	Adoptar las recomendaciones en modalidad de estricta	El valor recomendado no interfiere con ningún caso de uso.
Protección de correo electrónico	Bloquear la función auto reenviar correos a dominios externos.	Crear una regla que impida esta funcionalidad, además de auditar dicha regla con un grado de importancia alto o medio.	El valor recomendado no interfiere con ningún caso de uso.
Protección de correo electrónico	Configurar la autenticación de los emails.	Configurar los registros SPF y DMARC en los dominios de Exchange habilitar DKIM para los mensajes de Exchange.	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Protección de correo electrónico	Filtro de malware	Bloquear todas las extensiones que vienen por defecto además de añadir .bat, .cmd, .ps1, .ps2 y si estas son detectadas, mover a cuarentena con una alerta enviada por correo al administrador	El valor recomendado no interfiere con ningún caso de uso.
Protección de correo electrónico	Protección contra el correo no deseado	Activado, umbral 1.	El valor recomendado no interfiere con ningún caso de uso.
Protección de correo electrónico	Protección contra el phishing	Activado.	El valor recomendado no interfiere con ningún caso de uso.
Protección de correo electrónico	Instalar complemento reporte de mensaje	Instalado.	El valor recomendado no interfiere con ningún caso de uso.
Flujo de correo	Bloquear el reenvío automático de correos fuera de la organización	Creación de una regla que bloquee este comportamiento, activando una respuesta que guardará este mensaje en cuarentena y notificará al administrador de esta cuenta, además, esta regla será auditada con importancia alta.	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Flujo de correo	Bloquear el tráfico hacia fuera de la organización innecesario.	Creación de una regla que bloquee todo el tráfico a dominios externos con una whitelist donde se añadirán los dominios específicos con los que se vaya a trabajar.	Se añadirá a la whitelist los casos de colaboración que sean necesarios para los casos de uso.
Uso compartido	Uso compartido de la organización	Se añadirán solamente los dominios con los que sea necesario interactuar.	Se añadirá a la whitelist los casos de colaboración que sean necesarios para los casos de uso.

4.4 TEAMS

A continuación, se exponen todas las medidas de aplicación sobre Teams, el cual es el servicio principal de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Comunicación	Los usuarios pueden comunicarse con otros usuarios de Skype Empresarial y Teams	Desactivado	Debería estar activado para todos los casos de uso.
Comunicación	Los usuarios pueden comunicarse con usuarios de Skype	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Comunicación	Agregar un dominio	Bloquear dominios según evaluación	El valor recomendado no interfiere con ningún caso de uso.
Acceso	Permitir el acceso de invitado en Teams	Activado	Debería estar activado para todos los casos de uso.
Llamadas	Realizar llamadas privadas	Desactivado	Para el caso de uso Soporte debería estar activado, para el resto no.
Reuniones	Permitir vídeo IP	Activado	El valor recomendado no interfiere con ningún caso de uso.
Reuniones	Modo de pantalla compartida	Activado / Pantalla Completa	El valor recomendado no interfiere con ningún caso de uso.
Reuniones	Permitir Reunirse ahora	Desactivado	Para el caso de uso de colaboración, soporte debería estar habilitado.
Mensajes	Editar los mensajes enviados	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Mensajes	Eliminar los mensajes enviados	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Mensajes	Chat	Activado	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Mensajes	Usar Giphys en las conversaciones	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Mensajes	Usar Memes en las conversaciones	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Mensajes	Usar etiquetas en las conversaciones	Activado	El valor recomendado no interfiere con ningún caso de uso.
Mensajes	Permitir el lector inmersivo para ver mensajes	Desactivado	Por motivos de adaptabilidad, si existiera alguna persona que lo requiriese, habría que habilitarlo, de lo contrario, desactivado como se recomienda
Notificaciones y fuentes	Notificaciones y fuentes	Activado	El valor recomendado no interfiere con ningún caso de uso.
Etiquetado	Etiquetas	Activado	El valor recomendado no interfiere con ningún caso de uso.
Etiquetado	Las etiquetas las administra	Propietarios de equipo	El valor recomendado no interfiere con ningún caso de uso.
Etiquetado	Los propietarios del equipo pueden invalidar quién puede administrar las etiquetas	Activado	El valor recomendado no interfiere con ningún caso de uso.
Etiquetado	Etiquetas sugeridas	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Etiquetado	Permitir la creación de etiquetas personalizadas	Activado	El valor recomendado no interfiere con ningún caso de uso.
Etiquetado	Permitir que la aplicación Turnos aplique etiquetas	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Integración de correo electrónico	Los miembros del equipo pueden enviar correos electrónicos a la dirección de correo electrónico de un canal	Desactivado	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Archivos	Activar o desactivar almacenamiento de archivos externos	Desactivar todas	El valor recomendado no interfiere con ningún caso de uso.
Organización	Mostrar la ficha Organización en los chats	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Dispositivos	Se requiere un modo secundario de autenticación para obtener acceso al contenido de la reunión	Sin acceso	El valor recomendado no interfiere con ningún caso de uso.
Dispositivos	Establecer PIN de contenido	Se requiere siempre	El valor recomendado no interfiere con ningún caso de uso.
Dispositivos	Las cuentas de Surface Hub pueden enviar correos electrónicos	Desactivado	Desactivado salvo que se utilicen estos dispositivos.
Buscar por nombre	Limitar la búsqueda en el directorio mediante una directiva de libreta de direcciones de Exchange	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Modo de coexistencia	Modo de coexistencia	Teams solo	El valor recomendado no interfiere con ningún caso de uso.
Preferencias de aplicación	Descargar la aplicación de Teams en segundo plano para los usuarios de Skype Empresarial	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Directiva Global	Crear canales privados	Desactivado	Debería estar activado para todos los casos de uso, con autorización de un miembro de IT.
	Plantillas de Teams	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Propietarios pueden eliminar mensajes enviados	Activado	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Propiedades de mensaje	Eliminar mensajes enviados	Activado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Editar mensajes enviados	Activado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Confirmación de lectura	Activado para todos	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Chat	Activado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Usar imágenes Giphy en las conversaciones	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Usar Memes en las conversaciones	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Usar adhesivos en las conversaciones	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Permitir vistas previas de URL	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Traducir mensajes	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Permitir el lector inmersivo para ver mensajes	Activado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Enviar mensajes urgentes con notificaciones prioritarias	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Propiedades de mensaje	Crear mensajes de voz	Deshabilitado	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Canales	Dispositivos móviles: mostrar los canales favoritos por encima de los chats recientes	Activado	El valor recomendado no interfiere con ningún caso de uso.
Canales	Quitar usuarios de los chats grupales	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Canales	Respuestas sugeridas	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Canales	Rol de permisos de chat	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Participantes	Los usuarios *anónimos* pueden unirse a una reunión	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Participantes	Los usuarios *anónimos* pueden interactuar con aplicaciones en reuniones	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Invitación por correo electrónico		Activado	El valor recomendado no interfiere con ningún caso de uso.
Red	Insertar marcadores de calidad de servicio (QoS) para el tráfico de medios en tiempo real	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
General	Permitir la opción Reunirse ahora en canales	Activado	El valor recomendado no interfiere con ningún caso de uso.
General	Permitir el complemento de Outlook	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
General	Permitir la programación de reuniones de canal	Activado	El valor recomendado no interfiere con ningún caso de uso.
General	Permitir la programación de reuniones privadas	Activado	El valor recomendado no interfiere con ningún caso de uso.
Audio y Video	Permitir la transcripción	Desactivado	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Audio y Video	Permitir la grabación en la nube	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Audio y Video	Modo de audio por IP	Audio entrante y saliente habilitado	El valor recomendado no interfiere con ningún caso de uso.
Audio y Video	Modo para vídeo por IP	Video entrante y saliente habilitado	El valor recomendado no interfiere con ningún caso de uso.
Audio y Video	Permitir vídeo IP	Activado	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido de contenido	Modo de pantalla compartida	Toda la pantalla	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido de contenido	Permitir que un participante controle o solicite el control	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido de contenido	Permitir que un participante *externo* controle o solicite el control	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido de contenido	Permitir el uso compartido de PowerPoint	Activado	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido de contenido	Permitir la pizarra	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Uso compartido de contenido	Permitir notas compartidas	Desactivado	El valor recomendado no interfiere con ningún caso de uso, se utilizará One Note para los casos de formación.
Participantes e invitados	Permitir a personas anónimas iniciar una reunión	Desactivado	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Participantes e invitados	Admitir automáticamente personas	Todas las personas de su organización	El valor recomendado no interfiere con ningún caso de uso.
Participantes e invitados	Permitir que los usuarios de acceso telefónico omitan la sala de recepción	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Participantes e invitados	Habilitar subtítulos en directo	Deshabilitado	El valor recomendado no interfiere con ningún caso de uso.
Participantes e invitados	Permitir el chat en reuniones	Habilitado	El valor recomendado no interfiere con ningún caso de uso.
Reuniones		Reuniones de Teams	El valor recomendado no interfiere con ningún caso de uso, en caso de necesitarse un evento se podría programar de manera puntual.
Reuniones	Permitir programar	Activado	El valor recomendado no interfiere con ningún caso de uso.
Reuniones	Permitir la transcripción para los asistentes	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Reuniones	Quién puede unirse a eventos en directo programados	Usuarios o grupos específicos	El valor recomendado no interfiere con ningún caso de uso.
Reuniones	Quién puede grabar un evento	El organizador puede grabar o no	El valor recomendado no interfiere con ningún caso de uso.

TIPO	CONFIGURACIÓN	VALOR RECOMENDADO	CASOS DE USO
Aplicaciones	Aplicaciones de Microsoft	Permitir aplicaciones concretas y bloquear el resto	El valor recomendado no interfiere con ningún caso de uso.
Aplicaciones	Aplicaciones de terceros	Bloquear todas las aplicaciones	El valor recomendado no interfiere con ningún caso de uso.
Aplicaciones	Aplicaciones personalizadas	Bloquear todas las aplicaciones	El valor recomendado no interfiere con ningún caso de uso.
Aplicaciones		Activado, ancladas.	El valor recomendado no interfiere con ningún caso de uso.
Aplicaciones	Cargar aplicaciones personalizadas	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Aplicaciones	Permitir que los usuarios anclen aplicaciones	Desactivado	El valor recomendado no interfiere con ningún caso de uso.
Permisos de creación	Restringir la creación de *Teams* (equipos) por parte de los usuarios	Deshabilitar la creación de Grupos de Office 365 en todas las aplicaciones para todos los usuarios, y permitirlo para un grupo de seguridad	El valor recomendado no interfiere con ningún caso de uso.

5. DESPLIEGUE AUTOMÁTICO DE MICROSOFT 365

5.1 ARQUITECTURA DE LA SOLUCIÓN

Nota: Los ficheros adicionales necesarios para el despliegue automático del tenant están disponibles como elementos anexos a esta guía.

El entregable de despliegue automático consta de una serie de elementos que se detalla a continuación:

a) Scripts de configuración del tenant y de los distintos servicios implicados.

b) Módulos de PowerShell de los servicios a configurar.

c) Plantillas para el aprovisionamiento del piloto: usuarios, grupos, roles, Teams y canales.

La solución consta de tres scripts que deben ejecutarse en orden para el despliegue automático: setting del tenant y servicios implicados, aprovisionamiento y configuración de los casos de uso del piloto.

El scripting incluido en esta solución hace referencia a:

a) Scripting Tenant configuration based on CCN-STIC 884/885 guidelines

b) Scripting Identities

c) Scripting Authentication mechanisms

d) Scripting Segregation of functions and tasks

e) Scripting User Activity Log

f) Scripting Monitoring

g) Scripting Information Protection

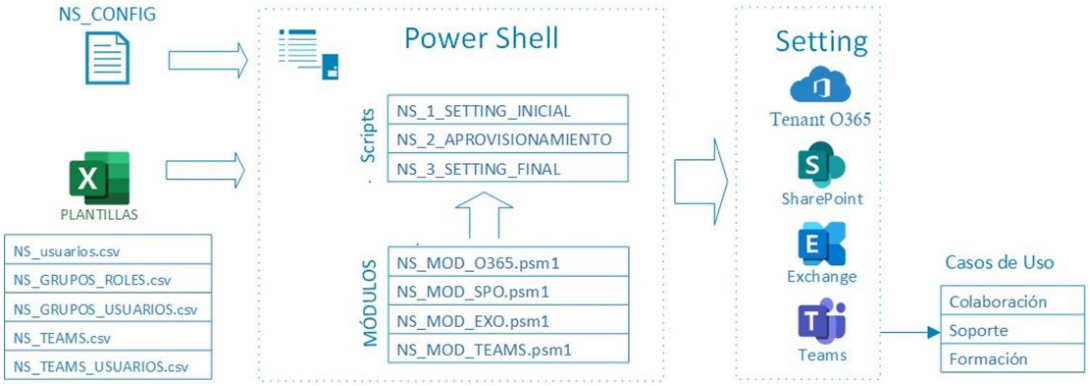
h) Scripting Encryption

i) Scripting Teams Settings

j) Scripting SPO Settings

k) Scripting EXO Settings

Arquitectura de la solución:



Los scripts a ejecutar se corresponden con las siguientes 3 fases para el despliegue:

FASE	TIPO SCRIPT	NOMBRE	DESCRIPCIÓN
FASE I		NS_1_SETTING_INICIAL.ps1	Script para la configuración inicial del tenant de la organización y de los distintos servicios: SPO, EXO y Teams.
FASE II		NS_2_APROVISIONAMIENTO.ps1	Aprovisionamiento de usuarios, grupos, roles y Teams, en base a las plantillas definidas en la carpeta de Aprovisionamiento.

FASE	TIPO SCRIPT	NOMBRE	DESCRIPCIÓN
FASE III		NS_3_SETTING_FINAL.ps1	Script para la configuración final en base a ciertos elementos creados en la fase de aprovisionamiento o de elementos concretos (buzones o sitios).

Módulos desarrollados para cada servicio con los comandos necesarios para la configuración:

TIPO SCRIPT	NOMBRE	DESCRIPCIÓN
	NS_MOD_O365.psm1	Comandos para configuración del tenant y aprovisionamiento
	NS_MOD_SPO.psm1	Comandos para configuración del servicio de SharePoint Online
	NS_MOD_EXO.psm1	Comandos para configuración del servicio de Exchange Online
	NS_MOD_TEAMS.psm1	Comandos para configuración del servicio de Microsoft Teams

Plantillas para el aprovisionamiento:

TIPO FICHERO	NOMBRE	DESCRIPCIÓN
	NS_usuarios.csv	Plantilla con todos los usuarios para el aprovisionamiento de los casos de uso
	NS_GRUPOS_ROLES.csv	Plantilla para el aprovisionamiento de grupos con los roles de las especificaciones
	NS_GRUPOS_USUARIOS.csv	Plantilla de asociación de usuarios a grupos
	NS_TEAMS.csv	Plantilla de creación de Teams y sus canales
	NS_TEAMS_USUARIOS.csv	Asociación de usuarios a Teams y canales y especificación de los roles de pertenencia

Fichero CONFIG con datos genéricos para el despliegue:

```
#Path root de la aplicacion
pathRoot=C:\CCN

# 1. DOMINIO DEL TENANT
cloudDomain=xxxx.onmicrosoft.com

# 2. LICENCIAS
#SkuIds de la licencias a asignar a los usuarios.
skuIds=710779e8-3d4a-4c88-adb9-386c958d1fxx

# 3. LISTAS BLANCAS

#whitelist de dominios externos permitidos para correo.
domainWhiteList=fabrikam.com,contoso.com

#whitelist de dominios externos permitidos para compartición de calendario
calendarWhiteList=fabrikam.com,contoso.com

#whitelist de dominios externos permitidos para compartición de ficheros SPO
sharingWhiteList=fabrikam.com,contoso.com

#Lista de direcciones IP permitidas.
IPAddressAllowList=

# 4. LISTAS NEGRAS

#Lista de extensiones de archivos para bloquear en la sincronizacion.
fileExtensionsBlackList=PST,EXE
```

5.2 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL

PowerShell de Office 365 permite administrar la configuración de Office 365 desde la línea de comandos. Conectarse a PowerShell de Office 365 es un proceso sencillo que consiste en instalar el software necesario y conectarse a la organización de Office 365.

Se utilizan los siguientes módulos de PowerShell:

a) Azure Active Directory PowerShell para Graph (los cmdlets incluyen Azure AD en su nombre).

b) Módulo Microsoft Azure Active Directory para Windows PowerShell (los cmdlets incluyen MSOL en su nombre).

c) Módulo de SharePoint Online: Microsoft.Online.SharePoint.PowerShell

d) Módulos de Microsoft Teams:

   i. MicrosoftTeams versión 1.1.9-Preview

   ii. MicrosoftTeams versión 2.3.1

Requerimientos previos

Usar una versión de 64 bits de Windows. La compatibilidad con la versión de 32 bits del Módulo de Microsoft Azure Active Directory para Windows PowerShell se descontinuó en octubre de 2014. Es necesario así mismo, usar la versión 5.1 o posterior de PowerShell. Más información sobre requerimientos previos de plataformas en: https://docs.microsoft.com/es-es/office365/enterprise/powershell/connect-to-office-365-powershell.

Instalar módulo de PowerShell de Azure Active Directory para Graph

a) Instalar el software necesario

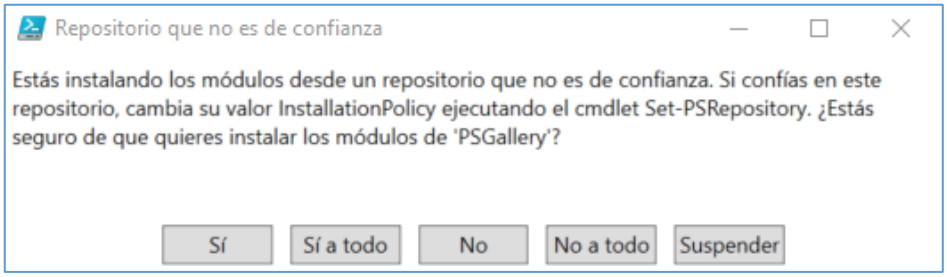
   Estos pasos son necesarios una sola vez en el equipo físico desde cual se va a administrador el tenant de Office 365, no cada vez que se conecta.

i. Abrir un símbolo del sistema de Windows PowerShell con privilegios elevados (ejecutar Windows PowerShell como administrador).

ii. En la ventana de comandos de Windows PowerShell (como administrador), ejecutar este comando:

```
#   Install-Module -Name AzureAD
```

Si se pregunta si se quiere instalar un módulo desde un repositorio que no es de confianza, escribir "Y" y presionar ENTRAR.



Esto ocurre porque de forma predeterminada, la Galería de PowerShell no está configurada como un repositorio de confianza. Responder Sí o Sí a todo.

Para actualizar una nueva versión del módulo ejecutar el comando anterior con el parámetro Force:

```
#   Install-Module -Name AzureAD -Force
```

b) Conectarse a Azure AD para la suscripción de Office 365

Para conectarse a Azure AD para la suscripción de Office 365 con un nombre de cuenta y contraseña o con la autenticación multifactor (MFA), ejecutar este comando desde un símbolo del sistema de Windows PowerShell:

```
#   Connect-AzureAD
```

En la sección [3.1. Administrador – configuración inicial] se explica cómo obtener las credenciales de acceso de administración.

Instalar módulo Microsoft Azure Active Directory para Windows PowerShell

Los comandos del Módulo Microsoft Azure Active Directory para Windows PowerShell tienen Msol en el nombre de su cmdlet.

a) Instalar el software necesario

Estos pasos son necesarios una sola vez en el equipo, no cada vez que se conecta. Sin embargo, probablemente se necesitará instalar las versiones más recientes de software periódicamente.

i. Instalar la versión de 64 bits de Microsoft Online Services - Ayudante para el inicio de sesión: Ayudante para el inicio de sesión de Microsoft Online Services para profesionales de TI (RTW).

ii. Instalar el Módulo Microsoft Azure Active Directory para Windows PowerShell siguiendo estos pasos:

– Abrir un símbolo del sistema de Windows PowerShell con privilegios elevados (ejecute Windows PowerShell como administrador).

– Ejecutar el comando:

```
#   Install-Module MSOnline
```

Aceptar la instalación del proveedor de NuGet.

Aceptar la instalación del módulo desde PSGallery.

Para actualizar una nueva versión del módulo ejecutar el comando anterior con el parámetro Force:

```
#   Install-Module MSOnline -Force
```

b) Conectarse a Azure AD para la suscripción de Office 365

Para conectarse a Azure AD para la suscripción de Office 365 con un nombre de cuenta y contraseña o con la autenticación multifactor (MFA), ejecutar este comando desde un símbolo del sistema de Windows PowerShell

```
#   Connect-MsolService
```

Instalar módulo Microsoft.Online.SharePoint.PowerShell

a) Instalar el software necesario

Ejecutar el comando:

```
#   Install-Module -Name Microsoft.Online.SharePoint.PowerShell
```

Para **actualizar** una nueva versión del módulo ejecutar el comando anterior con el parámetro *Force*:

```
#   Install-Module -Name Microsoft.Online.SharePoint.PowerShell -Force
```

b) Conectarse al módulo de SharePoint Online

Para conectarse al módulo, ejecutar este comando desde un símbolo del sistema de Windows PowerShell:

```
#   Connect-SPOService -Url $SPOurl
```

– *Donde $SPOurl es la url de conexión al SPO del tenant: https://$d-admin.sharepoint.com

Instalar módulos de Microsoft Teams

a) Instalar el software necesario

Para la ejecución de los scripts es necesario la instalación de dos módulos de Microsoft Teams:

i. MicrosoftTeams versión 1.1.9-Preview

ii. MicrosoftTeams versión 2.3.1

Ejecutar el comando:

```
#   Install-Module -Name MicrosoftTeams -RequiredVersion 1.1.5-preview -AllowPrerelease

#   Install-Module -Name MicrosoftTeams -RequiredVersion 2.3.1
```

– Para que funcione la promoción de usuarios de un canal a propietario se necesita la versión 1.1.9-Preview

b) Conectarse al módulo de Microsoft Teams

Para conectarse al módulo, ejecutar este comando desde un símbolo del sistema de Windows PowerShell:

```
#   Connect-MicrosoftTeams
```

5.3 CARACTERÍSTICAS SOFTWARE DE LA SOLUCIÓN

5.3.1 MÓDULOS DESARROLLADOS

Se ha desarrollado un módulo para cada uno de los servicios a configurar, más un módulo para configuración de características a nivel de tenant y aprovisionamiento:

TIPO SCRIPT	NOMBRE	DESCRIPCIÓN
	NS_MOD_O365.psm1	Comandos para configuración del tenant y aprovisionamiento
	NS_MOD_SPO.psm1	Comandos para configuración del servicio de SharePoint Online
	NS_MOD_EXO.psm1	Comandos para configuración del servicio de Exchange Online
	NS_MOD_TEAMS.psm1	Comandos para configuración del servicio de Microsoft Teams

5.3.1.1 NS_MOD_O365

Relación de comandos implementados en el módulo de Nube Sensible a nivel de Tenant:

COD.	NIVEL	SCRIPT	TAREA
AD-CONF-7	TENANT	NS-AADSetting	Los usuarios pueden restablecer su propia contraseña
TN-ID-1	Usuario	NS-accountProvisioning NS-groupUserAssigment	Aprovisionamiento de cuentas de ADMINISTRADORES
TN-ID-2	Usuario	NS-accountProvisioning	Aprovisionamiento de cuentas de USUARIOS INTERNOS
TN-ID-3	Usuario	NS-accountProvisioning	Asignación de licencias a usuarios
TN-IS-1	TENANT	NS-LoginSetting	Usuarios creados automáticamente por el sistema
TN-MC-2	TENANT	NS-AuthenticationSetting	Asignación MFA

COD.	NIVEL	SCRIPT	TAREA
TN-PW-1	TENANT	NS-PasswordSetting	Definición políticas de contraseñas
TN-SF-1	USUARIO	NS-groupsRolesProvisioning NS-groupUserAssigment	Asignación de roles a usuarios
TEN-RAU-1	TENANT	NS-ActivityRegisterSetting	Activación del registro de auditoría
TEN-RAU-2	BUZON	NS-MailboxActivityRegisterSetting	Activación del registro de auditoría en los buzones
TEN-PROT-1	GRUPO	NS-ProtocolSetting	Protocolos básicos de autenticación
TN-CT-2	TENANT	NS-CustomerLockBoxEnabling	Activar caja de seguridad de Microsoft
TN-CT-7	TENANT	NS-AuthorizationAppsSetting	Aplicaciones de terceros que requieren consentimiento del usuario
TN-CT-8	TENANT	NS-CalendarSharingPolicyDisabling	Permitir que los usuarios compartan su calendario con personas ajenas
TN-CT-9	TENANT	NS-SafeLinksSetting	Activar enlaces seguros
TN-CT-10	TENANT	NS-SafeDocsSetting	Activar adjuntos seguros

5.3.1.2 NS_MOD_SPO

Relación de comandos implementados en el módulo de Nube Sensible para el servicio de SharePoint Online:

COD.	NIVEL	SCRIPT	TAREA
MS-CA-1	TENANT	NS-SPOTenantSetting	Bloquear autenticación legacy para SharePoint
MS-PFCD-1	SITIO	NS-SPOSitesCustomScriptDisabling	Bloquear que los usuarios puedan ejecutar scripts personalizados en sitios personales y en sitios creados por ellos mismos.
MS-USE-1	TENANT	NS-SPOExternalDomainSharingSetting	Limitar el uso compartido externo por dominio.
MS-USE-2	TENANT SITIO	NS-SPOSharingSetting NS-SPOSitesSharingSetting	El contenido se puede compartir con
MS-USE-4	TENANT	NS-SPOPreventExternalUsersFromResharing	Permitir a los invitados compartir elementos que no son de su propiedad.
MS-USE-6	TENANT	NS-SPODefaultSharingLinkTypeSetting	Tipo de vínculo predeterminado
MS-USE-7	TENANT	NS-SPOBrowserIdleSignOutSetting	Cierre de sesión inactiva

COD.	NIVEL	SCRIPT	TAREA
MS-USE-8	TENANT	NS-SPODefaultLinkPermissionSetting	Tipo de permisos predeterminados del vínculo
MS-USE-9	TENANT	NS-SPOLegacyAuthProtocolsDisabling	Aplicaciones que no usan la autenticación moderna.
MS-USE-10	TENANT	NS-SPOIPAddressAllowListEnabling	Permitir el acceso solo desde determinadas direcciones IP.
FL-ONE-01	TENANT	NS-SPOTenantSyncClientRestrictionSetting	Sincronización de archivos

5.3.1.3 NS_MOD_EXO

Relación de comandos implementados en el módulo de Nube Sensible para el servicio de Exchange Online:

COD.	NIVEL	SCRIPT	TAREA
ME-PCE-4	TENANT	NS-BlockAutoForwardingExternalDomainsSetting	Bloquear la función auto reenviar correos a dominios externos.
ME-PCE-5	TENANT	NS-EmailAuthenticationSetting	Configurar la autenticación de los emails.
ME-PCE-6	TENANT	NS-MalwareFilterSetting	Filtro de malware
ME-PCE-7	TENANT	NS-AntispamFilterSetting	Protección contra el correo no deseado
ME-PCE-8	TENANT	NS-AntiPhishFilterSetting	Protección contra el phishing
ME-FC-1	TENANT	NS-BlockAutoForwardingExternalDomainsSetting	Bloquear el reenvío automático de correos fuera de la organización
ME-FC-2	TENANT	NS-ExternalDomainsOutboundTrafficSetting	Bloquear el tráfico hacia fuera de la organización innecesario.
ME-UC-01	TENANT	NS-CalendarSharing	Uso compartido de la organización

5.3.1.4 NS_MOD_TEAMS

Relación de comandos implementados en el módulo de Nube Sensible para el servicio de Microsoft Teams:

COD.	NIVEL	SCRIPT	TAREA

COD.	NIVEL	SCRIPT	TAREA
MT-AE-01	TENANT	NS-ExternalAccessSetting	Los usuarios pueden comunicarse con otros usuarios de Skype Empresarial y Teams
MT-AE-02	TENANT	NS-ExternalAccessSetting	Los usuarios pueden comunicarse con usuarios de Skype
MT-AI-01	TENANT	NS-GuestAccessEnabling	Permitir el acceso de invitado en Teams
MT-AI-02	TENANT	NS-GuestCallingSetting	Realizar llamadas privadas
MT-AI-03	TENANT	NS-GuestMeetingSetting	Permitir vídeo IP
MT-AI-04	TENANT	NS-GuestMeetingSetting	Modo de pantalla compartida
MT-AI-05	TENANT	NS-GuestMeetingSetting	Permitir Reunirse ahora
MT-AI-06	TENANT	NS-GuestMessagingSetting	Editar los mensajes enviados
MT-AI-07	TENANT	NS-GuestMessagingSetting	Eliminar los mensajes enviados
MT-AI-08	TENANT	NS-GuestMessagingSetting	Chat
MT-AI-09	TENANT	NS-GuestMessagingSetting	Usar Giphys en las conversaciones
MT-AI-10	TENANT	NS-GuestMessagingSetting	Usar Memes en las conversaciones
MT-AI-12	TENANT	NS-GuestMessagingSetting	Permitir el lector inmersivo para ver mensajes
MT-MCX-01	TENANT	NS-TeamsUpgradeSetting	Modo de coexistencia
MT-PRAPP-01	TENANT	NS-TeamsUpgradeSetting	Descargar la aplicación de Teams en segundo plano para los usuarios de Skype Empresarial
MT-DG-01	TENANT	NS-TeamsChannelsSetting	Crear canales privados
MT-DMEN-01	TENANT	NS-TeamsMessagingSetting	Propietarios pueden eliminar mensajes enviados
MT-DMEN-02	TENANT	NS-TeamsMessagingSetting	Eliminar mensajes enviados
MT-DMEN-03	TENANT	NS-TeamsMessagingSetting	Editar mensajes enviados
MT-DMEN-04	TENANT	NS-TeamsMessagingSetting	Confirmación de lectura
MT-DMEN-05	TENANT	NS-TeamsMessagingSetting	Chat
MT-DMEN-06	TENANT	NS-TeamsMessagingSetting	Usar imágenes Giphy en las conversaciones
MT-DMEN-07	TENANT	NS-TeamsMessagingSetting	Usar Memes en las conversaciones

COD.	NIVEL	SCRIPT	TAREA
MT-DMEN-08	TENANT	NS-TeamsMessagingSetting	Usar adhesivos en las conversaciones
MT-DMEN-09	TENANT	NS-TeamsMessagingSetting	Permitir vistas previas de URL
MT-DMEN-10	TENANT	NS-TeamsMessagingSetting	Traducir mensajes
MT-DMEN-11	TENANT	NS-TeamsMessagingSetting	Permitir el lector inmersivo para ver mensajes
MT-DMEN-12	TENANT	NS-TeamsMessagingSetting	Enviar mensajes urgentes con notificaciones prioritarias
MT-DMEN-13	TENANT	NS-TeamsMessagingSetting	Crear mensajes de voz
MT-DMEN-14	TENANT	NS-TeamsMessagingSetting	Dispositivos móviles: mostrar los canales favoritos por encima de los chats recientes
MT-DMEN-15	TENANT	NS-TeamsMessagingSetting	Quitar usuarios de los chats grupales
MT-DMEN-16	TENANT	NS-TeamsMessagingSetting	Respuestas sugeridas
MT-CONRE-01	TENANT	NS-TeamsMeetingConfiguration	Los usuarios anónimos pueden unirse a una reunión
MT-CONRE-02	TENANT	NS-TeamsMeetingConfiguration	Los usuarios anónimos pueden interactuar con aplicaciones en reuniones
MT-CONRE-04	TENANT	NS-TeamsMeetingConfiguration	Insertar marcadores de calidad de servicio (QoS) para el tráfico de medios en tiempo real
MT-DR-01	TENANT	NS-TeamsMeetingSetting	Permitir la opción Reunirse ahora en canales
MT-DR-02	TENANT	NS-TeamsMeetingSetting	Permitir el complemento de Outlook
MT-DR-03	TENANT	NS-TeamsMeetingSetting	Permitir la programación de reuniones de canal
MT-DR-04	TENANT	NS-TeamsMeetingSetting	Permitir la programación de reuniones privadas
MT-DR-05	TENANT	NS-TeamsMeetingSetting	Permitir la transcripción
MT-DR-06	TENANT	NS-TeamsMeetingSetting	Permitir la grabación en la nube
MT-DR-07	TENANT	NS-TeamsMeetingSetting	Modo de audio por IP
MT-DR-08	TENANT	NS-TeamsMeetingSetting	Modo para vídeo por IP
MT-DR-09	TENANT	NS-TeamsMeetingSetting	Permitir vídeo IP

COD.	NIVEL	SCRIPT	TAREA
MT-DR-10	TENANT	NS-TeamsMeetingSetting	Modo de pantalla compartida
MT-DR-11	TENANT	NS-TeamsMeetingSetting	Permitir que un participante controle o solicite el control
MT-DR-12	TENANT	NS-TeamsMeetingSetting	Permitir que un participante externo controle o solicite el control
MT-DR-13	TENANT	NS-TeamsMeetingSetting	Permitir el uso compartido de PowerPoint
MT-DR-14	TENANT	NS-TeamsMeetingSetting	Permitir la pizarra
MT-DR-15	TENANT	NS-TeamsMeetingSetting	Permitir notas compartidas
MT-DR-16	TENANT	NS-TeamsMeetingSetting	Permitir a personas anónimas iniciar una reunión
MT-DR-17	TENANT	NS-TeamsMeetingSetting	Admitir automáticamente personas
MT-DR-18	TENANT	NS-TeamsMeetingSetting	Permitir que los usuarios de acceso telefónico omitan la sala de recepción
MT-DR-19	TENANT	NS-TeamsMeetingSetting	Habilitar subtítulos en directo
MT-DR-20	TENANT	NS-TeamsMeetingSetting	Permitir el chat en reuniones
MT-DED-02	TENANT	NS-TeamsMeetingBroadcastSetting	Permitir programar
MT-DED-03	TENANT	NS-TeamsMeetingBroadcastSetting	Permitir la transcripción para los asistentes
MT-DED-04	TENANT	NS-TeamsMeetingBroadcastSetting	Quién puede unirse a eventos en directo programados
MT-DED-05	TENANT	NS-TeamsMeetingBroadcastSetting	Quién puede grabar un evento
MT-DCA-02	TENANT	NS-TeamsAppSetup	Cargar aplicaciones personalizadas
MT-DCA-03	TENANT	NS-TeamsAppSetup	Permitir que los usuarios anclen aplicaciones

5.4 PLANTILLAS PARA EL APROVISIONAMIENTO

Se han desarrollado una serie de plantillas, en formato CSV, para el aprovisionamiento de usuarios, grupos, roles y creación de Teams y canales para los distintos casos de uso.

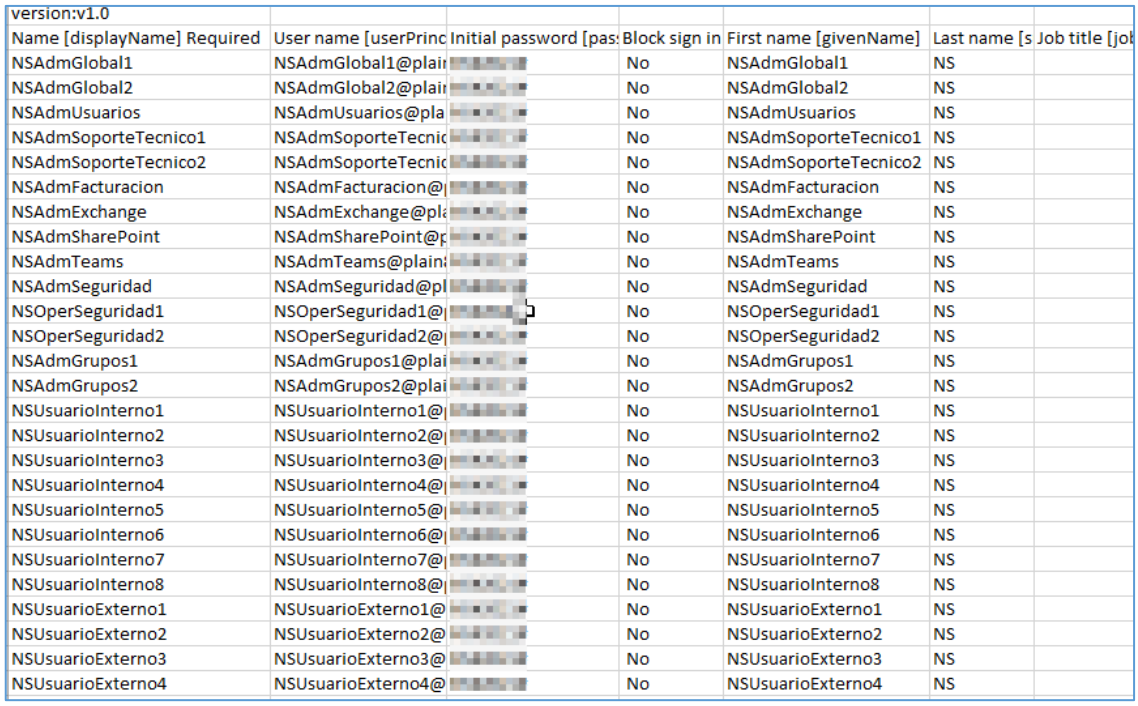
TIPO FICHERO	NOMBRE	DESCRIPCIÓN
	NS_usuarios.csv	Plantilla con todos los usuarios para el aprovisionamiento de los casos de uso
	NS_GRUPOS_ROLES.csv	Plantilla para el aprovisionamiento de grupos con los roles de las especificaciones
	NS_GRUPOS_USUARIOS.csv	Plantilla de asociación de usuarios a grupos
	NS_TEAMS.csv	Plantilla de creación de Teams y sus canales
	NS_TEAMS_USUARIOS.csv	Asociación de usuarios a Teams y canales y especificación de los roles de pertenencia

5.4.1 PLANTILLA DE USUARIOS

Plantilla con los datos de los usuarios a incorporar al directorio activo.

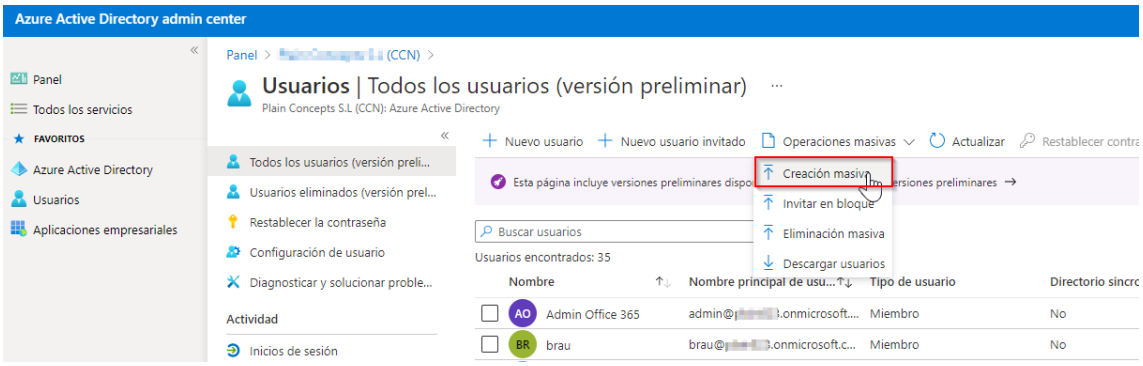
Esta plantilla puede usarse aprovisionar los usuarios desde el programa de despliegue y también desde el portal de Azure.

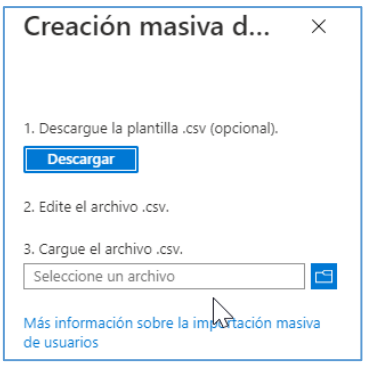
Nota: Es recomendable cambiar las contraseñas iniciales suministradas por defecto.



version:v1.0						
Name [displayName] Required	User name [userPrinc	Initial password [pas	Block sign in	First name [givenName]	Last name [s	Job title [jo
NSAdmGlobal1	NSAdmGlobal1@plair		No	NSAdmGlobal1	NS	
NSAdmGlobal2	NSAdmGlobal2@plair		No	NSAdmGlobal2	NS	
NSAdmUsuarios	NSAdmUsuarios@pla		No	NSAdmUsuarios	NS	
NSAdmSoporteTecnico1	NSAdmSoporteTecnic		No	NSAdmSoporteTecnico1	NS	
NSAdmSoporteTecnico2	NSAdmSoporteTecnic		No	NSAdmSoporteTecnico2	NS	
NSAdmFacturacion	NSAdmFacturacion@		No	NSAdmFacturacion	NS	
NSAdmExchange	NSAdmExchange@pla		No	NSAdmExchange	NS	
NSAdmSharePoint	NSAdmSharePoint@p		No	NSAdmSharePoint	NS	
NSAdmTeams	NSAdmTeams@plain		No	NSAdmTeams	NS	
NSAdmSeguridad	NSAdmSeguridad@pl		No	NSAdmSeguridad	NS	
NSOperSeguridad1	NSOperSeguridad1@		No	NSOperSeguridad1	NS	
NSOperSeguridad2	NSOperSeguridad2@		No	NSOperSeguridad2	NS	
NSAdmGrupos1	NSAdmGrupos1@plai		No	NSAdmGrupos1	NS	
NSAdmGrupos2	NSAdmGrupos2@plai		No	NSAdmGrupos2	NS	
NSUsuarioInterno1	NSUsuarioInterno1@		No	NSUsuarioInterno1	NS	
NSUsuarioInterno2	NSUsuarioInterno2@		No	NSUsuarioInterno2	NS	
NSUsuarioInterno3	NSUsuarioInterno3@		No	NSUsuarioInterno3	NS	
NSUsuarioInterno4	NSUsuarioInterno4@		No	NSUsuarioInterno4	NS	
NSUsuarioInterno5	NSUsuarioInterno5@		No	NSUsuarioInterno5	NS	
NSUsuarioInterno6	NSUsuarioInterno6@		No	NSUsuarioInterno6	NS	
NSUsuarioInterno7	NSUsuarioInterno7@		No	NSUsuarioInterno7	NS	
NSUsuarioInterno8	NSUsuarioInterno8@		No	NSUsuarioInterno8	NS	
NSUsuarioExterno1	NSUsuarioExterno1@		No	NSUsuarioExterno1	NS	
NSUsuarioExterno2	NSUsuarioExterno2@		No	NSUsuarioExterno2	NS	
NSUsuarioExterno3	NSUsuarioExterno3@		No	NSUsuarioExterno3	NS	
NSUsuarioExterno4	NSUsuarioExterno4@		No	NSUsuarioExterno4	NS	

Desde el portal de Azure:





5.4.2 PLANTILLA DE GRUPOS Y ROLES

Plantilla para el aprovisionamiento de grupos y la asignación de roles a dichos grupos.

TIPO	GRUPO	DES_GRUPO	ROL_AZURE
SEGURIDAD	NS_GR_AdmGlobal	ADMINISTRADOR GLOBAL	Global Administrator
SEGURIDAD	NS_GR_AdmUsuarios	ADMINISTRADOR USUARIOS	User Administrator
SEGURIDAD	NS_GR_AdmSoporteTecnico	ADMINISTRADOR SOPORTE TÉCNICO	Helpdesk Administrator
SEGURIDAD	NS_GR_AdmFacturacion	ADMINISTRADOR FACTURACION	Billing Administrator
SEGURIDAD	NS_GR_AdmExchange	ADMINISTRADOR EXCHANGE	Exchange Administrator
SEGURIDAD	NS_GR_AdmSharePoint	ADMINISTRADOR SHAREPOINT	SharePoint Administrator
SEGURIDAD	NS_GR_AdmTeams	ADMINISTRADOR TEAMS	Teams Administrator

La plantilla consta de otras columnas de descripción, pero que no afectan al aprovisionamiento.

TIPO	GRUPO	DES_GRUPO	ROL_AZURE	DESC_ROL_AZURE	ACCIONES
SEGURIDAD	NS_GR_AdmGlobal	ADMINISTRADOR GLOBAL	Global Administrator	Puede administrar todos los aspectos de los servicios de Azure AD y Microsoft que usan identidades de Azure AD.	Administrador global
SEGURIDAD	NS_GR_AdmUsuarios	ADMINISTRADOR USUARIOS	User Administrator	Puede administrar todos los aspectos de usuarios y grupos	Administrar de usuarios y grupos
SEGURIDAD	NS_GR_AdmSoporteTecnico	ADMINISTRADOR SOPORTE TÉCNICO	Helpdesk Administrator	Puede cambiar contraseñas, invalidar tokens de actualización, administrar solicitudes de servicio y monitorear el estado del servicio	Restablecer contraseñas Forzar a los usuarios a cerrar sesión Administrar solicitudes de servicio Supervisar el estado del servicio
SEGURIDAD	NS_GR_AdmFacturacion	ADMINISTRADOR FACTURACION	Billing Administrator	Realiza compras, gestiona suscripciones, gestiona tickets de soporte y supervisa el estado del servicio.	Administrar todos los aspectos de la facturación del Tenant Relación con soporte técnico Microsoft
SEGURIDAD	NS_GR_AdmExchange	ADMINISTRADOR EXCHANGE	Exchange Administrator	Tienen permisos globales dentro de Microsoft Exchange Online, cuando el servicio está presente, así como la capacidad de crear y administrar todos los grupos de Microsoft 365, administrar tickets de soporte y monitorear el estado del servicio.	Establecer configuración global del servicio Exchange Permisos de administración completa sobre Exchange
SEGURIDAD	NS_GR_AdmSharePoint	ADMINISTRADOR SHAREPOINT	SharePoint Administrator	Tienen permisos globales dentro de Microsoft SharePoint Online, cuando el servicio está presente, así como la capacidad de crear y administrar todos los grupos de Microsoft 365, administrar tickets de soporte y monitorear el estado del servicio.	Establecer configuración global del servicio SharePoint Permisos de administración completa sobre SharePoint
SEGURIDAD	NS_GR_AdmTeams	ADMINISTRADOR TEAMS	Teams Administrator	Los usuarios en este rol pueden administrar todos los aspectos de la carga de trabajo de Microsoft Teams a través del centro de administración de Microsoft Teams y Skype for Business y los respectivos módulos de PowerShell. Esto incluye, entre otras áreas, todas las herramientas de gestión relacionadas con la telefonía, la mensajería, las reuniones y los propios equipos. Este rol además otorga la capacidad de crear y administrar todos los grupos de Microsoft 365, administrar tickets de soporte y monitorear el estado del servicio.	Establecer configuración global del servicio Teams Permisos de administración completa sobre Teams
SEGURIDAD	NS_GR_AdmSeguridad	ADMINISTRADOR SEGURIDAD	Security Administrator	Los usuarios con este rol tienen permisos para administrar funciones relacionadas con la seguridad en el centro de seguridad de Microsoft 365, Azure Active Directory Identity Protection, Azure Active Directory Authentication, Azure Information Protection y Office 365 Security & Compliance Center.	Registros de auditoría Administración de dispositivos Administración de cumplimiento dlp Administración de cumplimiento de IB Administrar alertas Quarantine Administrador de seguridad Administrador de etiquetas de confidencialidad Colaborador de etiquetas Administrador de etiquetas Administrador de cumplimiento Administrador de IRM Administrador eDiscovery Administrar alertas Lector de seguridad Colaborador de etiquetas

5.4.3 PLANTILLA DE ASIGANCIÓN DE USUARIO A GRUPOS

Asignación de los usuarios a los grupos creados:

USUARIO	GRUPO_USUARIOS
NSAdmGlobal1	NS_GR_AdmGlobal
NSAdmGlobal2	NS_GR_AdmGlobal
NSAdmUsuarios	NS_GR_AdmUsuarios
NSAdmSoporteTecnico1	NS_GR_AdmSoporteTecnico
NSAdmSoporteTecnico2	NS_GR_AdmSoporteTecnico
NSAdmFacturacion	NS_GR_AdmFacturacion
NSAdmExchange	NS_GR_AdmExchange
NSAdmSharePoint	NS_GR_AdmSharePoint
NSAdmTeams	NS_GR_AdmTeams
NSAdmSeguridad	NS_GR_AdmSeguridad
NSOperSeguridad1	NS_GR_OperSeguridad
NSOperSeguridad2	NS_GR_OperSeguridad
NSAdmGrupos1	NS_GR_Grupos
NSAdmGrupos2	NS_GR_Grupos
NSUsuarioInterno1	NS_GU_USUARIOS_INTERNOS
NSUsuarioInterno2	NS_GU_USUARIOS_INTERNOS
NSUsuarioInterno3	NS_GU_USUARIOS_INTERNOS
NSUsuarioInterno4	NS_GU_USUARIOS_INTERNOS
NSUsuarioInterno5	NS_GU_USUARIOS_INTERNOS
NSUsuarioInterno6	NS_GU_USUARIOS_INTERNOS
NSUsuarioInterno7	NS_GU_USUARIOS_INTERNOS
NSUsuarioInterno8	NS_GU_USUARIOS_INTERNOS
NSUsuarioExterno1	NS_GU_USUARIOS_EXTERNOS
NSUsuarioExterno2	NS_GU_USUARIOS_EXTERNOS
NSUsuarioExterno3	NS_GU_USUARIOS_EXTERNOS
NSUsuarioExterno4	NS_GU_USUARIOS_EXTERNOS

5.4.4 PLANTILLA DE CREACIÓN DE TEAMS

Plantilla para la creación de los Teams de los casos de uso, y los canales asociados a cada team:

TEAM	DES_TEAM	CPRIVADOS	APPS
NS_GR1	TEAM GRUPO 1	CANAL1,CANAL2	
NS_GR1_P1	TEAM GRUPO 1 - PROYECTO 1	CANAL1,CANAL2,CANAL3	
NS_GR1_P2	TEAM GRUPO 1 - PROYECTO 2	CANAL1,CANAL2,CANAL3,CANAL4	
NS_GR2	TEAM GRUPO 2	CANAL1,CANAL2	
NS_GR2_P1	TEAM GRUPO 2 - PROYECTO 1	CANAL1,CANAL2,CANAL3,CANAL4	
NS_GR2_P2	TEAM GRUPO 2 - PROYECTO 2	CANAL1,CANAL2,CANAL3	

En la fase final del despliegue se configurarán los distintos Teams para adecuarlo a cada uno de los casos de uso.

5.4.5 PLANTILLA DE ASIGANCIÓN DE USUARIOS A TEAMS

Plantilla de pertenencia de los usuarios a cada team, y a cada canal privado de cada team, con el rol asociado en cada caso:

USUARIO	TEAM	ROL_TEAM	CANALES_PRIVADOS	ROL_CANALES
NSUsuarioInterno1	NS_GR1	Propietario	CANAL1,CANAL2	P,P
NSUsuarioInterno1	NS_GR1_P1	Propietario	CANAL1,CANAL2,CANAL3	P,P,P
NSUsuarioInterno1	NS_GR1_P2	Propietario	CANAL1,CANAL2,CANAL3,CANAL4	P,P,P,P
NSUsuarioInterno2	NS_GR1	Miembro	CANAL1,CANAL2	M,M
NSUsuarioInterno2	NS_GR1_P1	Miembro	CANAL1,CANAL2,CANAL3	M,M,M
NSUsuarioInterno2	NS_GR1_P2	Miembro	CANAL1,CANAL2,CANAL3,CANAL4	M,M,M,M
NSUsuarioInterno3	NS_GR1	Miembro	CANAL1,CANAL2	M,M
NSUsuarioInterno3	NS_GR1_P1	Miembro	CANAL1,CANAL2,CANAL3	M,M,M
NSUsuarioInterno4	NS_GR1	Miembro	CANAL1,CANAL2	M,M
NSUsuarioInterno4	NS_GR1_P2	Miembro	CANAL1,CANAL2,CANAL3,CANAL4	M,M,M,M
NSUsuarioInterno5	NS_GR2	Propietario	CANAL1,CANAL2	P,P
NSUsuarioInterno5	NS_GR2_P1	Propietario	CANAL1,CANAL2,CANAL3,CANAL4	P,P,P,P
NSUsuarioInterno5	NS_GR2_P2	Propietario	CANAL1,CANAL2,CANAL3	P,P,P
NSUsuarioInterno6	NS_GR2	Miembro	CANAL1,CANAL2	M,M
NSUsuarioInterno6	NS_GR2_P1	Miembro	CANAL1,CANAL2,CANAL3,CANAL4	M,M,M,M
NSUsuarioInterno6	NS_GR2_P2	Miembro	CANAL1,CANAL2,CANAL3	M,M,M
NSUsuarioInterno7	NS_GR2	Miembro	CANAL1,CANAL2	M,M
NSUsuarioInterno7	NS_GR2_P1	Miembro	CANAL1,CANAL2,CANAL3,CANAL4	M,M,M,M
NSUsuarioInterno8	NS_GR2	Miembro	CANAL1,CANAL2	M,M
NSUsuarioInterno8	NS_GR2_P2	Miembro	CANAL1,CANAL2,CANAL3	M,M,M

5.5 DESPLIEGUE

Para el despliegue de la solución “Nube Sensible” se recomienda seguir la siguiente secuencia de pasos.

5.5.1 APROVISIONAMIENTO DEL TENANT DE O365

Es necesario contar con un tenant de O365 y un usuario administrador para la configuración y el despliegue.

Nota: Se recomienda deshabilitar durante el despliegue el MFA del usuario administrador (si lo tuviera), debiendo ser reactivado una vez finalice el despliegue.

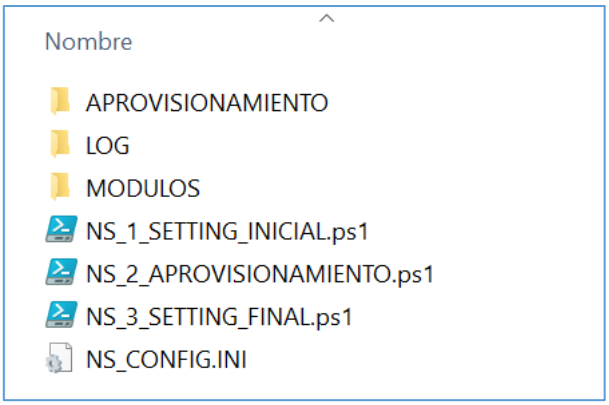
5.5.2 INSTALAR LOS MÓDULOS NECESARIOS DE POWERSHELL

En la máquina Windows a utilizar para el despliegue, es necesario instalar los módulos descritos en la sección [Prerrequisitos para el despliegue mediante PowerShell].

5.5.3 COPIAR EL SOFTWARE DE LA SOLUCIÓN

En la máquina Windows donde va a ejecutarse el código de despliegue, debe copiarse el

código a una carpeta del sistema de ficheros:



5.5.4 AJUSTAR LOS PARÁMETROS DEL FICHERO CONFIG

Fichero CONFIG con datos genéricos para el despliegue:

```
#Path root de la aplicacion
pathRoot=C:\CCN

# 1. DOMINIO DEL TENANT
cloudDomain=xxxx.onmicrosoft.com

# 2. LICENCIAS
#SkuIds de la licencias a asignar a los usuarios.
skuIds=710779e8-3d4a-4c88-adb9-386c958d1fxx

# 3. LISTAS BLANCAS

#whitelist de dominios externos permitidos para correo.
domainWhiteList=fabrikam.com,contoso.com

#whitelist de dominios externos permitidos para comparticion de calendario
calendarWhiteList=fabrikam.com,contoso.com

#whitelist de dominios externos permitidos para comparticion de ficheros SPO
sharingWhiteList=fabrikam.com,contoso.com

#Lista de direcciones IP permitidas.
IPAddressAllowList=

# 4. LISTAS NEGRAS
#Lista de extensiones de archivos para bloquear en la sincronizacion.
fileExtensionsBlackList=PST,EXE
```

a) pathRoot *

La carpeta del sistema de archivos donde se copiará el sw. de la solución.

b) cloudDomain *

Dominio del tenant que se usará para el despliegue.

c) skuIds *

sku de la licencia E5 a asignar a los usuarios. Si fuera más de una licencia se especificarían separadas por comas “,”.

d) domainWhiteList

Lista de dominios externos permitidos para los correos, separados por comas “,” y sin espacios.

e) calendarWhiteList

Lista de dominios externos permitidos para compartición de calendario, separados por comas "," y sin espacios.

f) IPAddressAllowList

Lista de direcciones IP permitidas. Separadas por comas ",". Por ejemplo: 172.16.0.0,192.168.1.0/27

Nota: Asegurarse de que se incluye la propia dirección IP actual desde donde se lanzan los scripts y de acceso al portal. En caso de duda, provisionalmente se puede dejar la lista de direcciones en blanco.

g) fileExtensionsBlackList

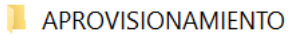
Lista de extensiones de archivos para bloquear en la sincronización. Separados por comas ",". Ejemplo: PST,EXE

Nota: Aquellos parámetros marcados con "*" son obligatorios.

5.5.5 REVISAR LAS PLANTILLAS DE APROVISIONAMIENTO

Aunque las plantillas están cumplimentadas con información de los usuarios, grupos, roles y Teams necesarios para los casos de uso, puede ser interesante en algunos casos añadir más elementos para el aprovisionamiento.

Se encuentran en la carpeta:



Nota: Por defecto, dejar las plantillas como están.

6. CONFIGURACIÓN AUTOMÁTICA DE MEDIDAS DE SEGURIDAD

6.1 LANZAMIENTO DE LOS SCRIPTS DE DESPLIEGUE

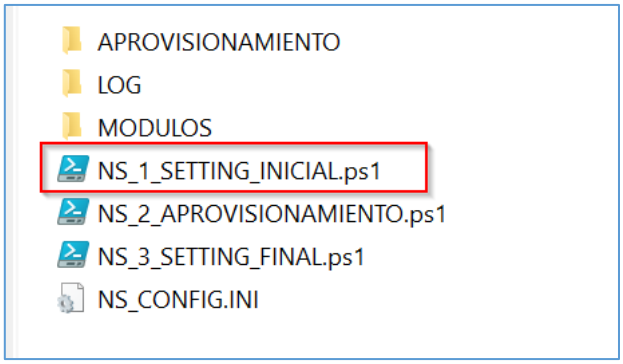
Se han desarrollado 3 scripts de despliegue, que deben ejecutarse secuencialmente.

a) Se recomienda ejecutarlo por separado, y en entorno distintos, para evitar posibles problemas con las dos versiones que se utilizan de Microsoft Teams, ya que se ha detectado que en algunas versiones de PowerShell, si no se liberan los entornos, pueden elevarse excepciones del sistema.

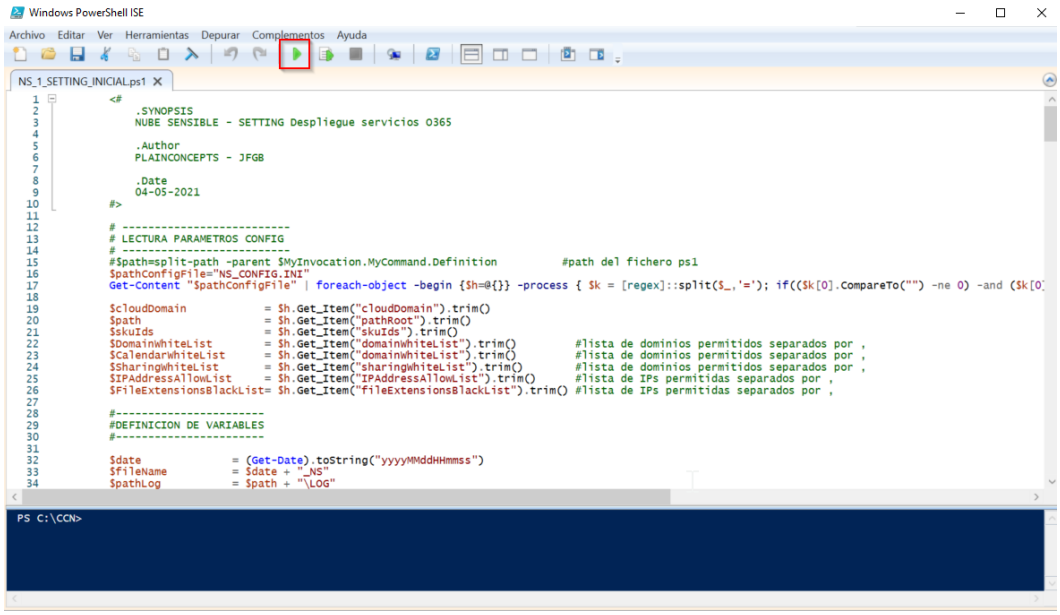
b) Se usará como ejemplo de lanzamiento el interfaz de PowerShell ISE.

6.1.1 FASE I. LANZAMIENTO DEL SCRIPT DE CONFIGURACIÓN INICIAL

a) Desde el explorador de ficheros, se navega a la carpeta donde se encuentra el código copiado en el paso 3. Y hacer doble clic sobre el fichero:



b) Desde el interfaz de PS ISE lanzar ejecutar el código:



i. El script envía información por pantalla y almacena los resultados en dos ficheros que se encuentran en la carpeta LOG. Estudiar dicha información por si se ha producido alguna incidencia.

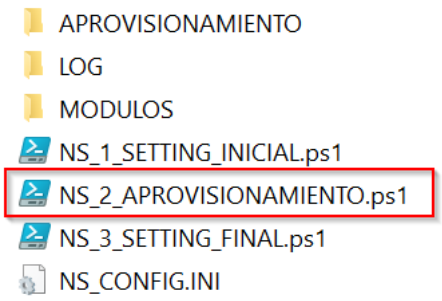
ii. Tras la ejecución con éxito del primer script ya estaría configurado el tenant y los distintos servicios, y por tanto puede pasarse a la Fase II.

iii. Cerrar la ventana del interfaz PowerShell ISE.

6.1.2 FASE II. LANZAMIENTO DEL SCRIPT DE APROVISIONAMIENTO

Al final del paso anterior se ha cerrado la ventana de PowerShell ISE para liberar las variables de entorno.

a) Desde el explorador de ficheros, se navega a la carpeta donde se encuentra el código copiado en el paso 3. Y hacer doble clic sobre el fichero:



b) Desde el interfaz de PS ISE lanzar ejecutar el código.

i. El script envía información por pantalla y almacena los resultados en dos ficheros que se encuentran en la carpeta LOG. Estudiar dicha información por si se ha producido alguna incidencia.

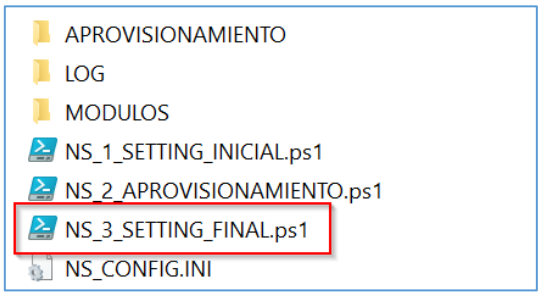
ii. Tras la ejecución con éxito del segundo script ya estaría aprovisionado el tenant y los distintos casos de uso, y por tanto puede pasarse a la Fase III.

iii. Cerrar la ventana del interfaz PowerShell ISE.

6.1.3 FASE III. LANZAMIENTO DEL SCRIPT DE CONFIGURACIÓN FINAL

Al final del paso anterior se ha cerrado la ventana de PowerShell ISE para liberar las variables de entorno.

a) Desde el explorador de ficheros, se navega a la carpeta donde se encuentra el código copiado en el paso 3. Y hacer doble clic sobre el fichero:



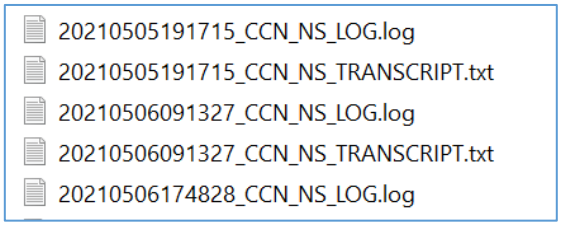
b) Desde el interfaz de PS ISE lanzar ejecutar el código.

i. El script envía información por pantalla y almacena los resultados en dos ficheros que se encuentran en la carpeta LOG. Estudiar dicha información por si se ha producido alguna incidencia.

ii. Tras la ejecución con éxito del tercer script ya estaría desplegada la configuración de "Nube Sensible" con todos los casos de uso.

6.2 COMPROBACIONES

Revisar los archivos de la carpeta LOG. En cada fase se generan dos archivos: una archivo log y un transcript con el detalle de los comandos y posibles incidencias.



7. CONFIGURACIÓN MANUAL DE MEDIDAS DE SEGURIDAD

El presente apartado tiene como objetivo ayudar a los operadores a implementar las medidas de seguridad que no pueden realizarse de forma automatizada, bien porque requieres de un análisis y parametrización concreta o bien porque no es posible su realización por medio de scripts de configuración.

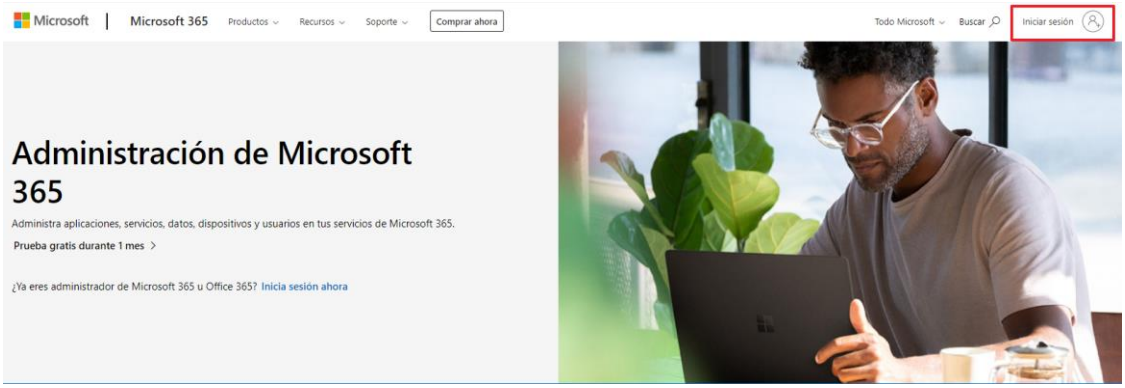
Dentro de todas las medidas definidas en el punto 4, solo se reflejarán en este punto aquellas que su configuración sea manual.

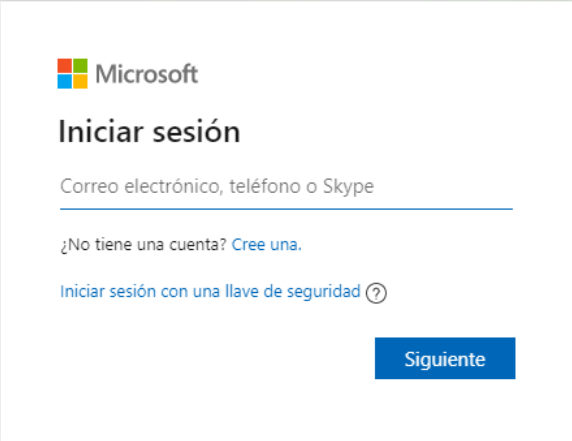
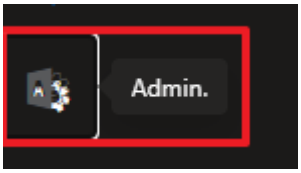
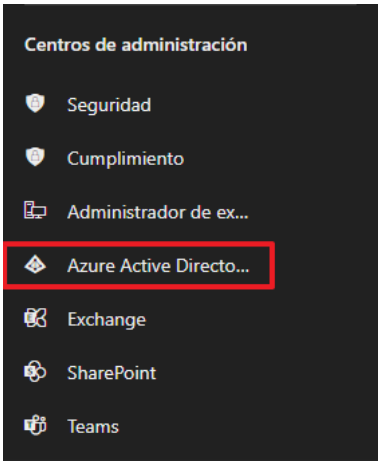
Nota: Bajo el documento "CCN- Nube Sensible - Despliegue - Tareas v1.0" se definen de forma más amplia las medidas aplicadas y consideraciones a tener en cuenta, así como las medidas que son de ejecución manual por medio de la columna "TDES".
En el mismo documento indicado anteriormente existen configuraciones manuales las cuales requieren de criterios y procedimientos que se adecuen a cada organismo. Por ello, deberán revisarse y adaptarse según las necesidades.

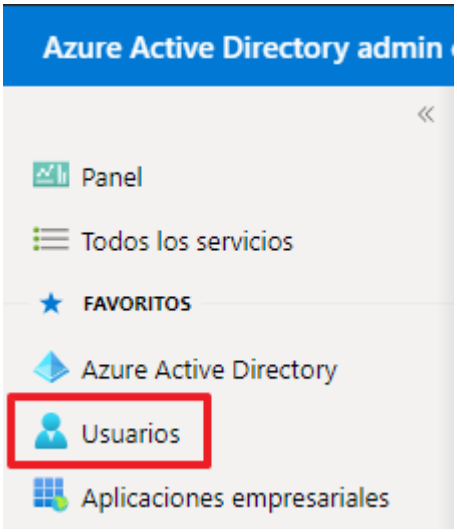
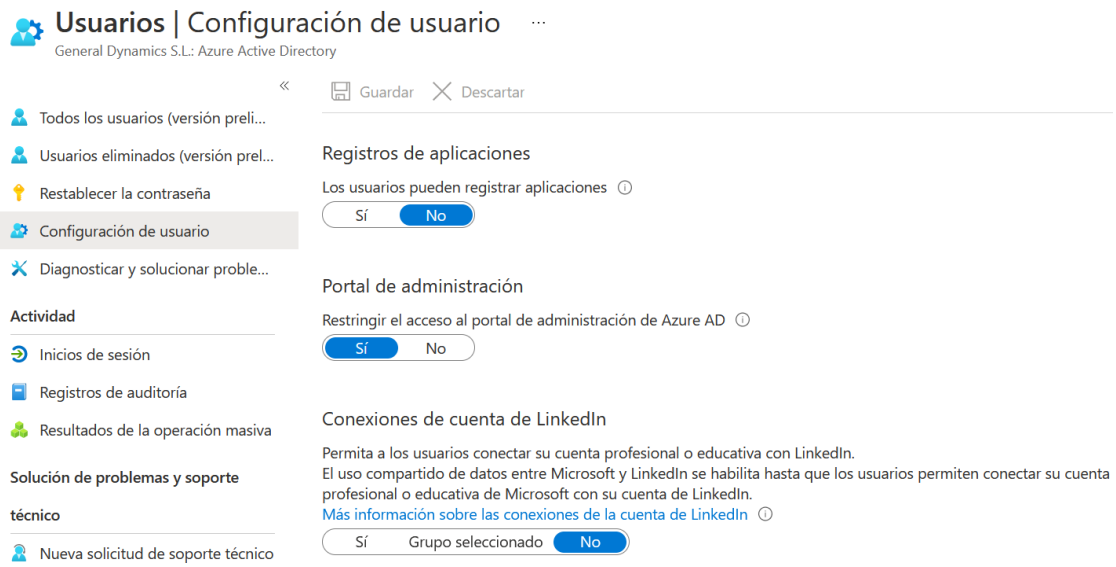
En los apartados posteriores se definirán las medidas manuales aplicadas por cada uno de los servicios afectados, tal y como se expone en el punto "4 CONFIGURACIONES DE SEGURIDAD DE MICROSOFT 365".

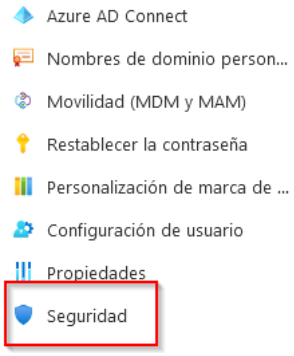
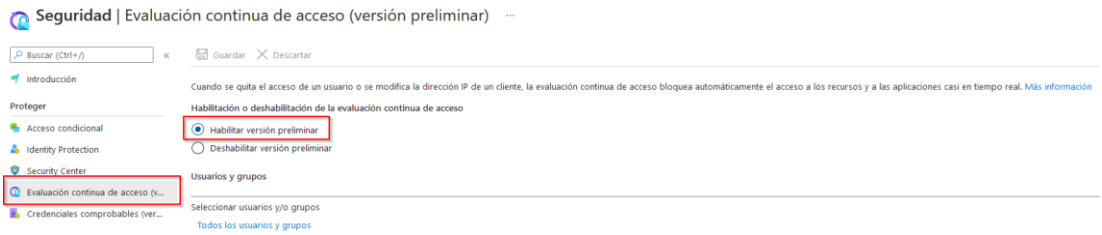
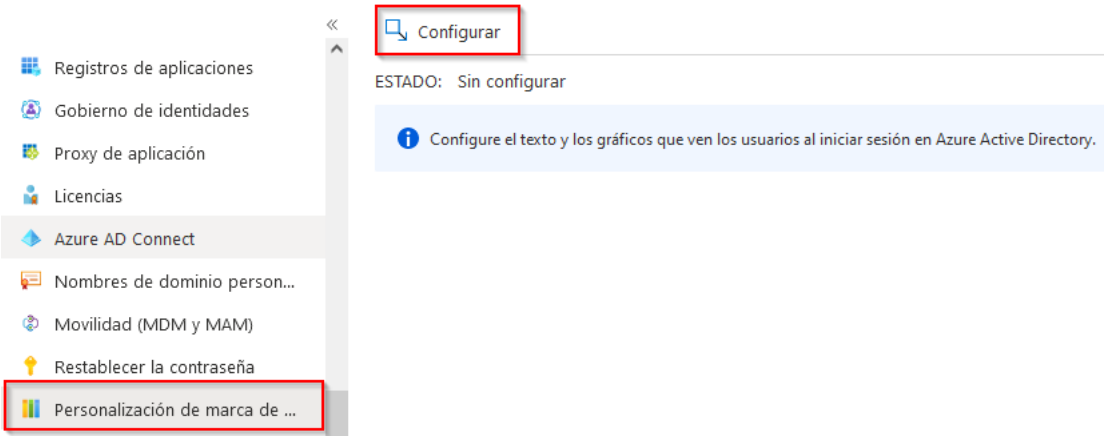
7.1 TENANT

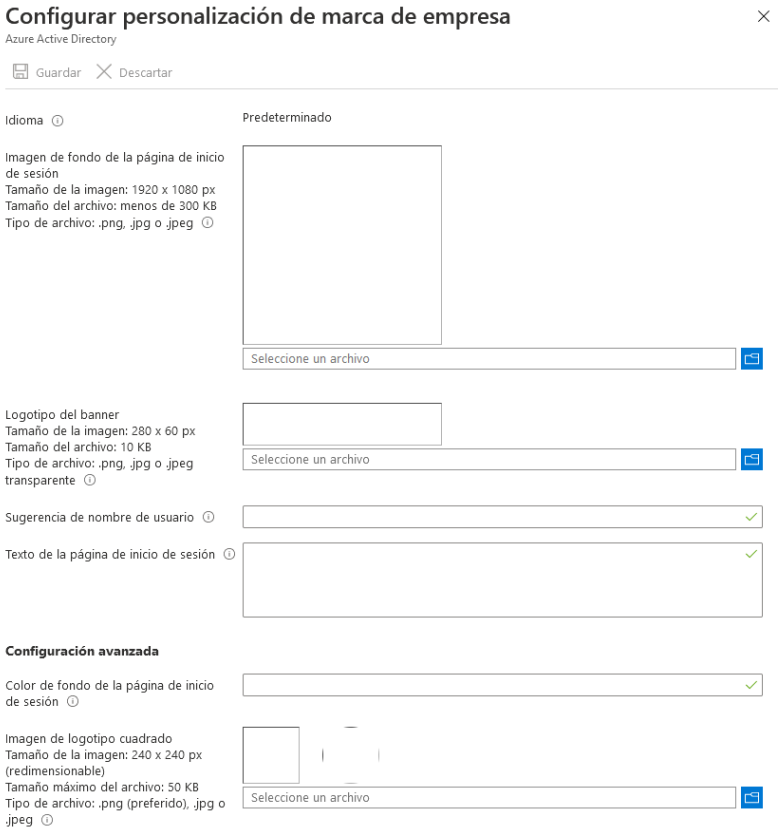
A continuación, se indican los pasos para aplicar las configuraciones manuales sobre el Tenant.

Paso	Descripción
1.	Acceda al portal de administración de Microsoft 365 por medio del siguiente enlace: – https://www.microsoft.com/es-es/microsoft-365/business/office-365-administration
2.	En la esquina superior derecha pulse sobre "Iniciar sesión". 

Paso	Descripción
3.	A continuación, deberá introducir las credenciales con privilegios de administración sobre Microsoft 365. Pulse “Siguiente” para continuar.  **Nota:** Es posible que se le solicite información adicional en caso de tener ya habilitado un sistema de autenticación multifactor (MFA).
4.	En el menú lateral izquierdo pulse sobre el icono de administración. 
5.	En la nueva pestaña emergente, de nuevo sobre el menú lateral izquierdo pulse sobre “Azure Active Directory”. 

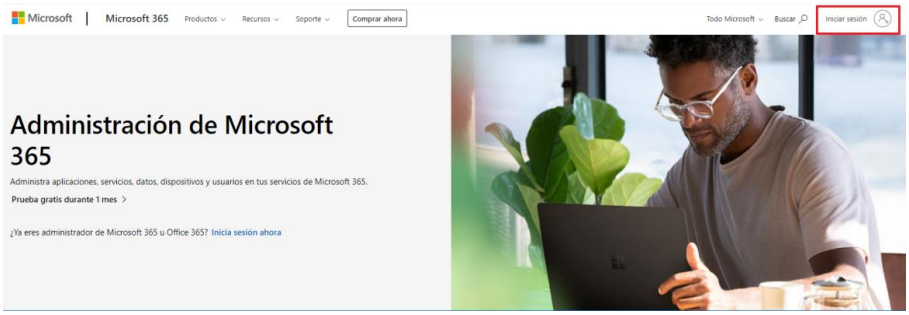
Paso	Descripción
6.	En la nueva pestaña emergente que se abrirá seleccione “Usuarios” en el menú lateral izquierdo. 
7.	Seleccione a continuación en el panel central, “Configuración del usuario”. Establezca la configuración según se indica a continuación: – Registros de aplicaciones → “No” – Portal de administración → “Sí”. – Conexiones de cuenta de Linkedin → “No” 
8.	A continuación, realice las siguientes configuraciones en el apartado de seguridad del panel de Azure Active directory. Para ello siga los pasos 1 a 5.

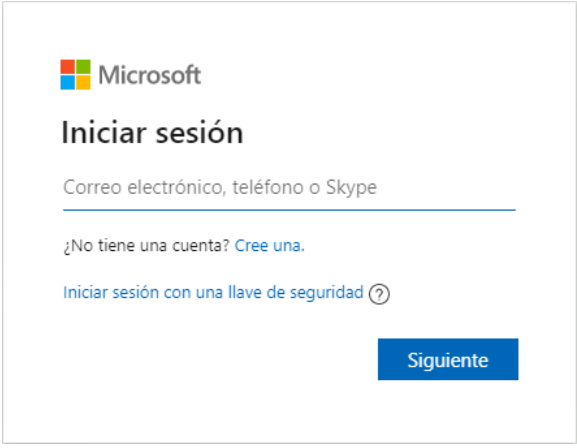
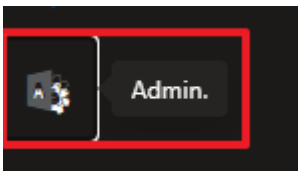
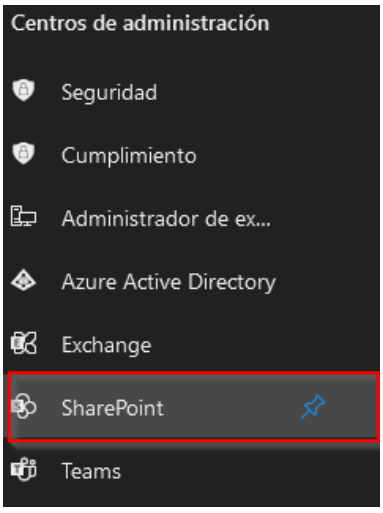
Paso	Descripción
9.	Posteriormente sobre el panel lateral izquierdo seleccione “Seguridad”. 
10.	Seleccione evaluación continua de acceso en el panel lateral izquierdo y a continuación, marque la opción de “Habilitar versión preliminar” como muestra la siguiente imagen: 
11.	A continuación, realice las siguientes configuraciones en el apartado de Personalización de marca de empresa del panel de Azure Active directory. Para ello siga los pasos 1 a 5.
12.	Seleccione la opción “Personalización de marca de empresa en el panel lateral izquierdo y a continuación, pulse el botón configurar, tal y como muestra la siguiente imagen: 

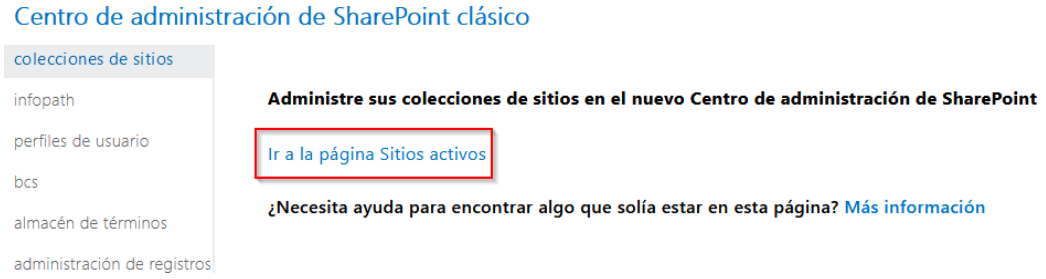
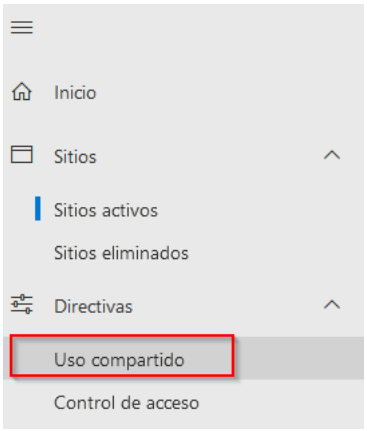
Paso	Descripción
13.	Finalmente, configure el fondo de página, el logo y el texto de su portal: 

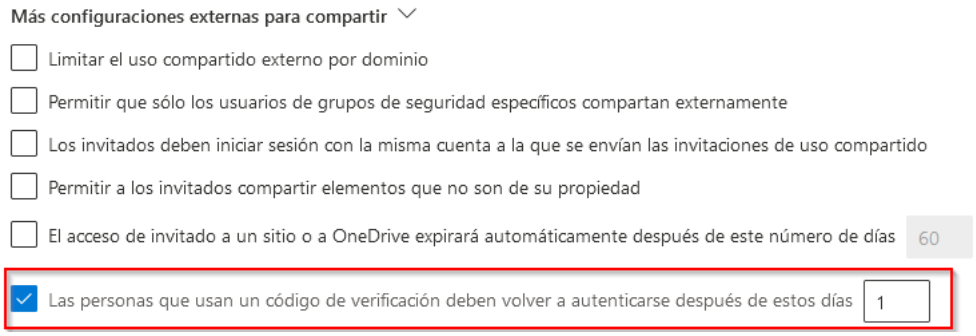
7.2 SHAREPOINT ONLINE

A continuación, se indican los pasos para aplicar las configuraciones manuales sobre SharePoint.

Paso	Descripción
1.	Acceda al portal de administración de Microsoft 365 por medio del siguiente enlace: https://www.microsoft.com/es-es/microsoft-365/business/office-365-administration
2.	En la esquina superior derecha pulse sobre “Iniciar sesión”. 

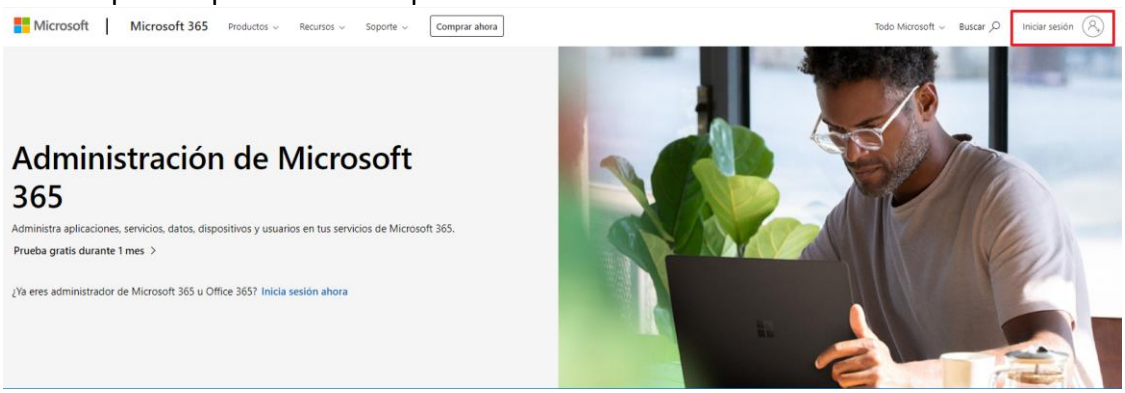
Paso	Descripción
3.	A continuación, deberá introducir las credenciales con privilegios de administración sobre Microsoft 365. Pulse “Siguiente” para continuar.  **Nota:** Es posible que se le solicite información adicional en caso de tener ya habilitado un sistema de autenticación multifactor (MFA).
4.	En el menú lateral izquierdo pulse sobre el icono de administración. 
5.	En la nueva pestaña emergente, de nuevo sobre el menú lateral izquierdo pulse sobre “SharePoint”. 

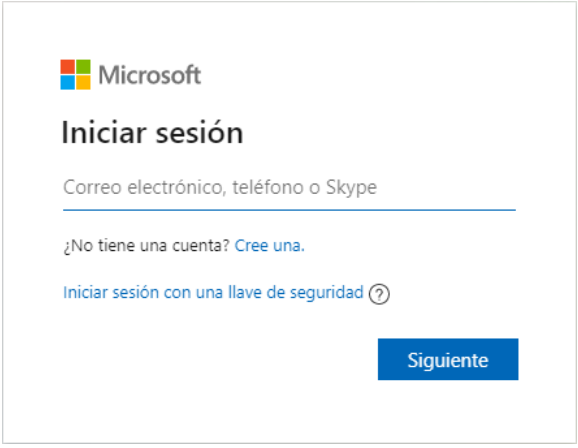
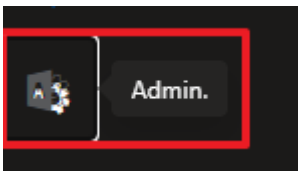
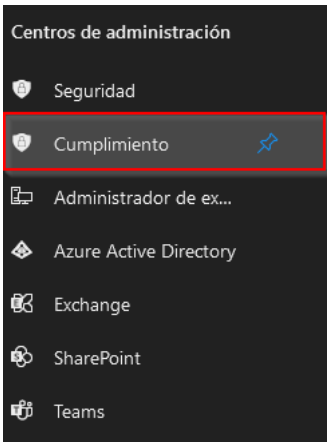
Paso	Descripción
6.	En la nueva ventana, pulse en “Ir a la página Sitios activos”. 
7.	En el menú lateral derecho, pulse sobre “Uso compartido”. 
8.	A continuación, despliegue el resto de opciones haciendo clic sobre “Más configuraciones para compartir”. 

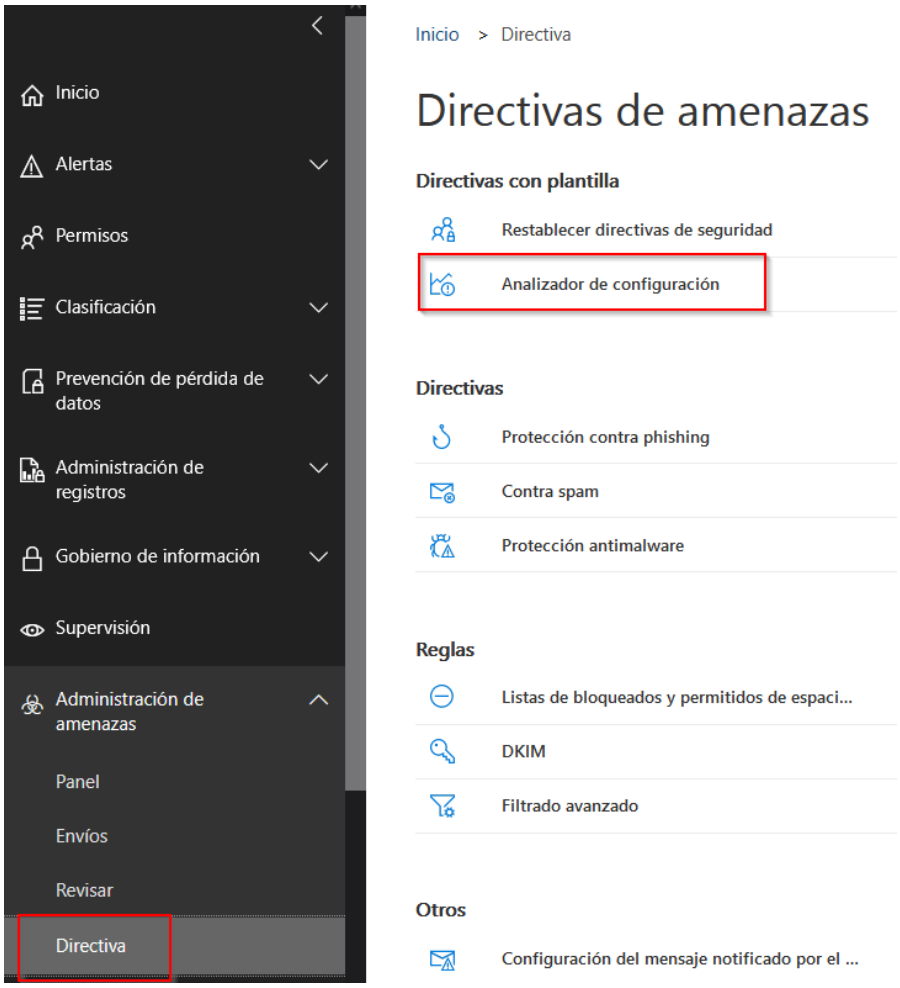
Paso	Descripción
9.	En las opciones adicionales que se muestran, marque la casilla “Las personas que usan un código de verificación deben volver a autenticarse después de estos días” y, adicionalmente, introduzca el valor “1” en el cuadro de la derecha, tal y como muestra la siguiente imagen: 

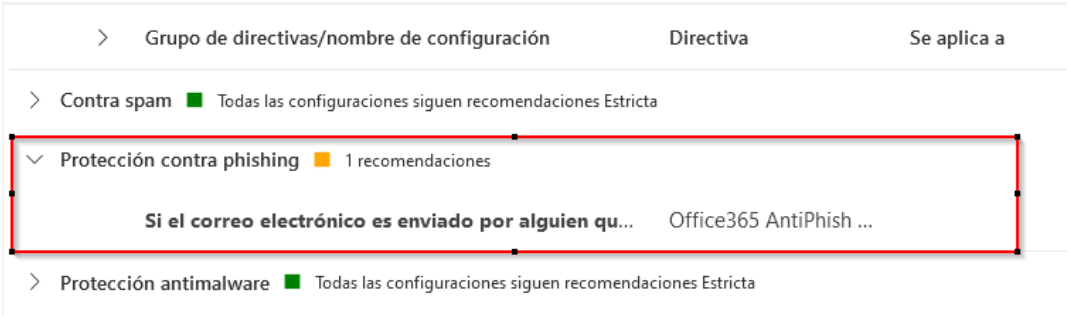
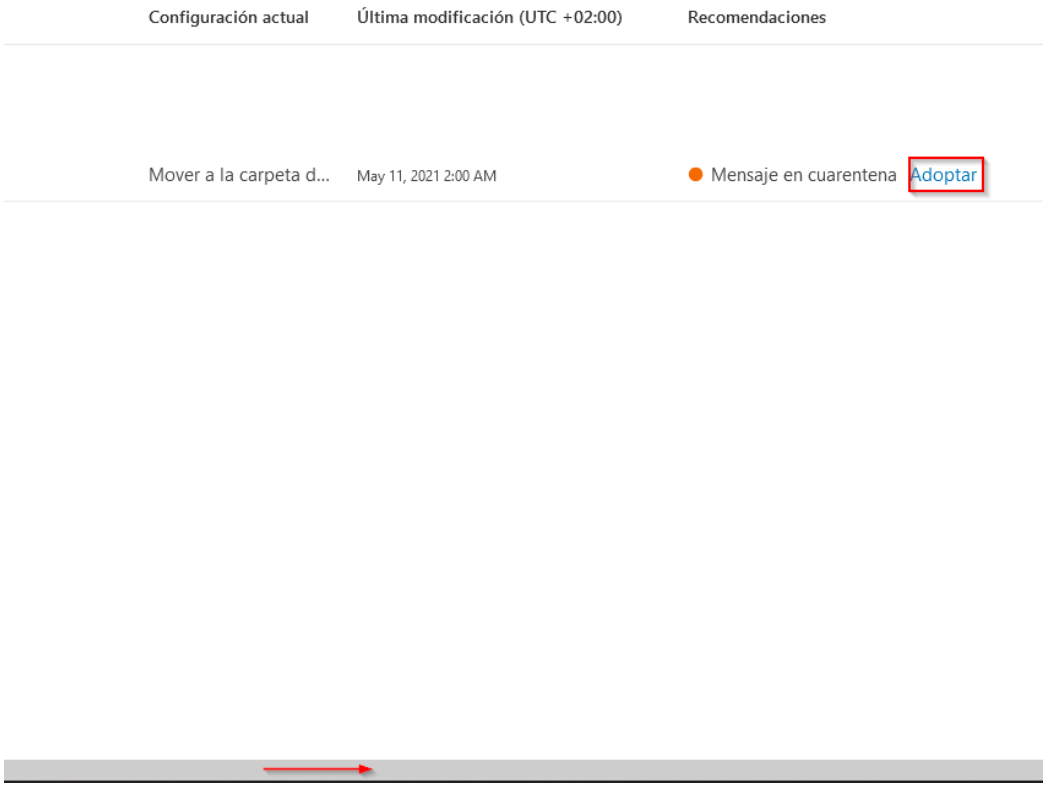
7.3 EXCHANGE ONLINE

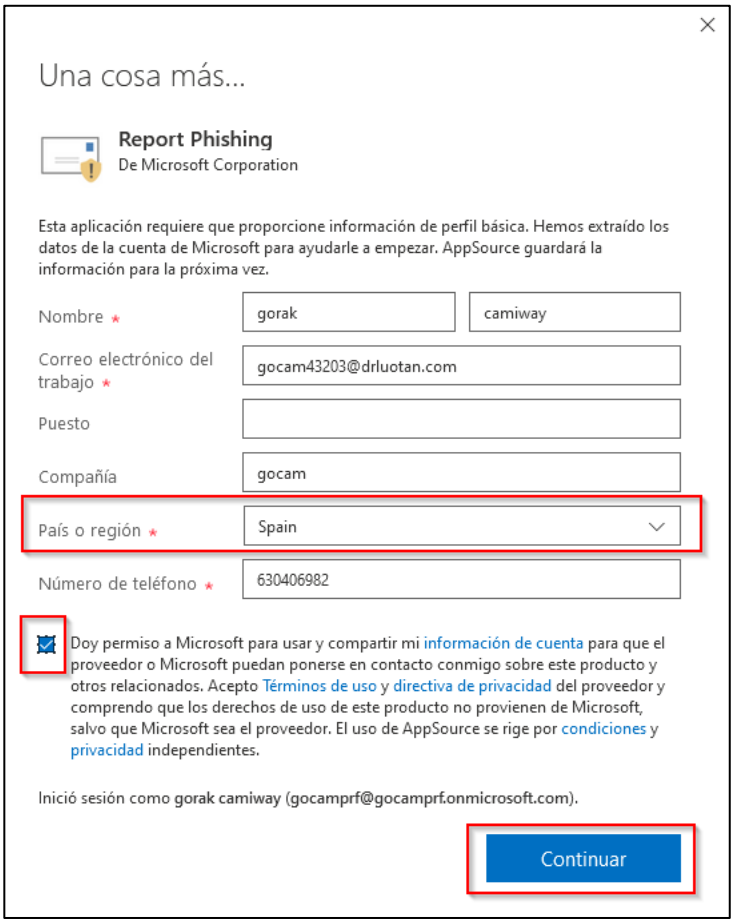
A continuación, se indican los pasos para aplicar las configuraciones manuales sobre Exchange.

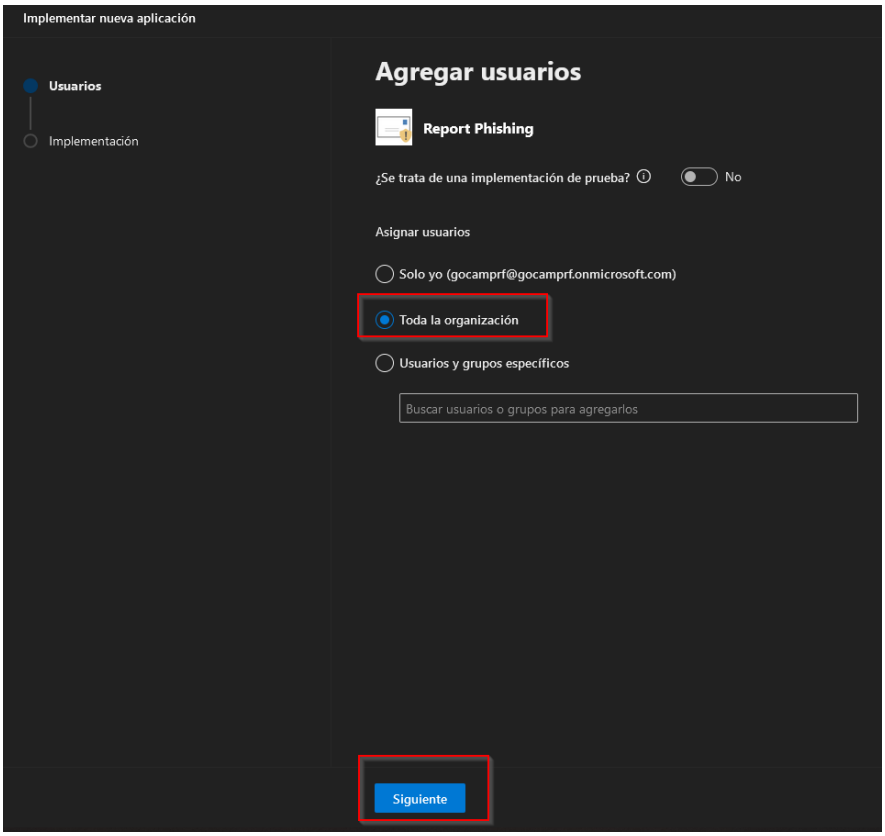
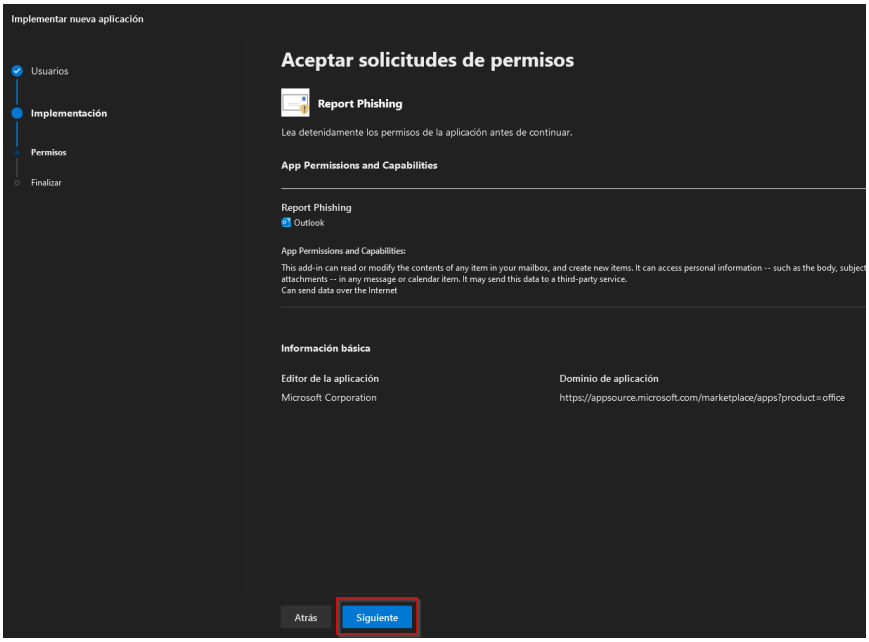
Paso	Descripción
1.	Acceda al portal de administración de Microsoft 365 por medio del siguiente enlace: https://www.microsoft.com/es-es/microsoft-365/business/office-365-administration
2.	En la esquina superior derecha pulse sobre “Iniciar sesión”. 

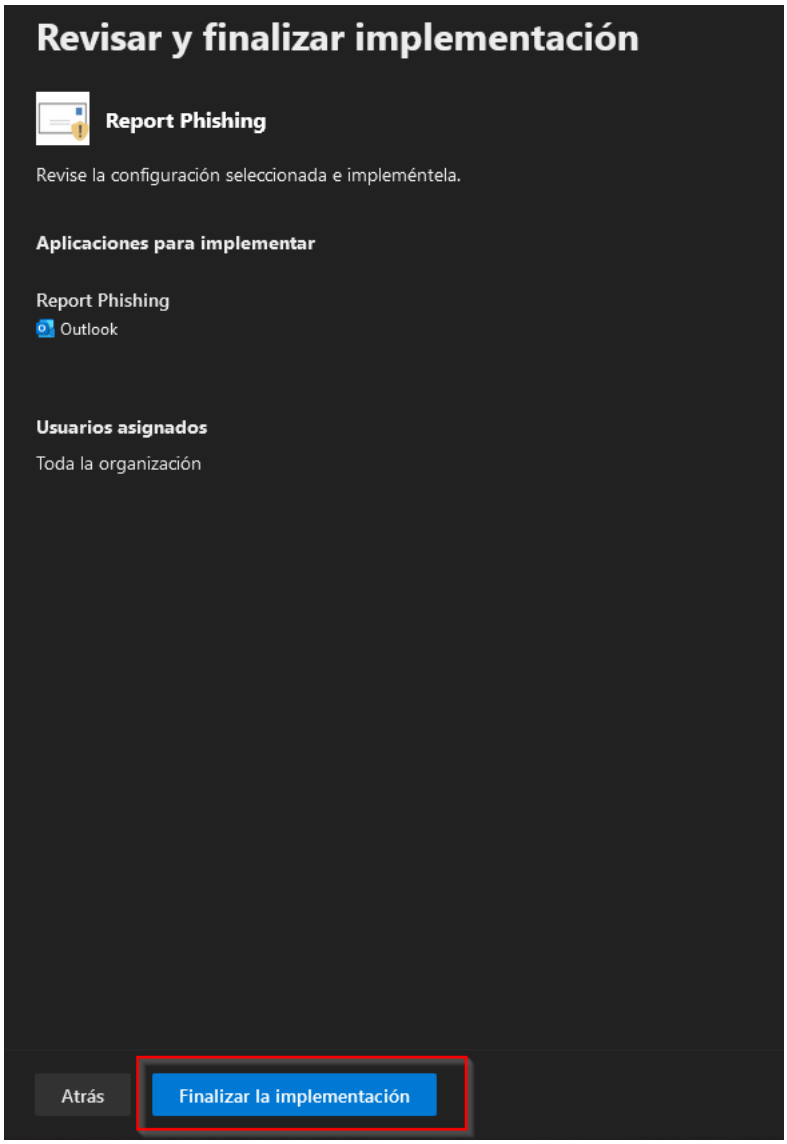
Paso	Descripción
3.	A continuación, deberá introducir las credenciales con privilegios de administración sobre Microsoft 365. Pulse “Siguiente” para continuar.  **Nota:** Es posible que se le solicite información adicional en caso de tener ya habilitado un sistema de autenticación multifactor (MFA).
4.	En el menú lateral izquierdo pulse sobre el icono de administración. 
5.	En la nueva pestaña emergente, de nuevo sobre el menú lateral izquierdo pulse sobre “Cumplimiento”. 

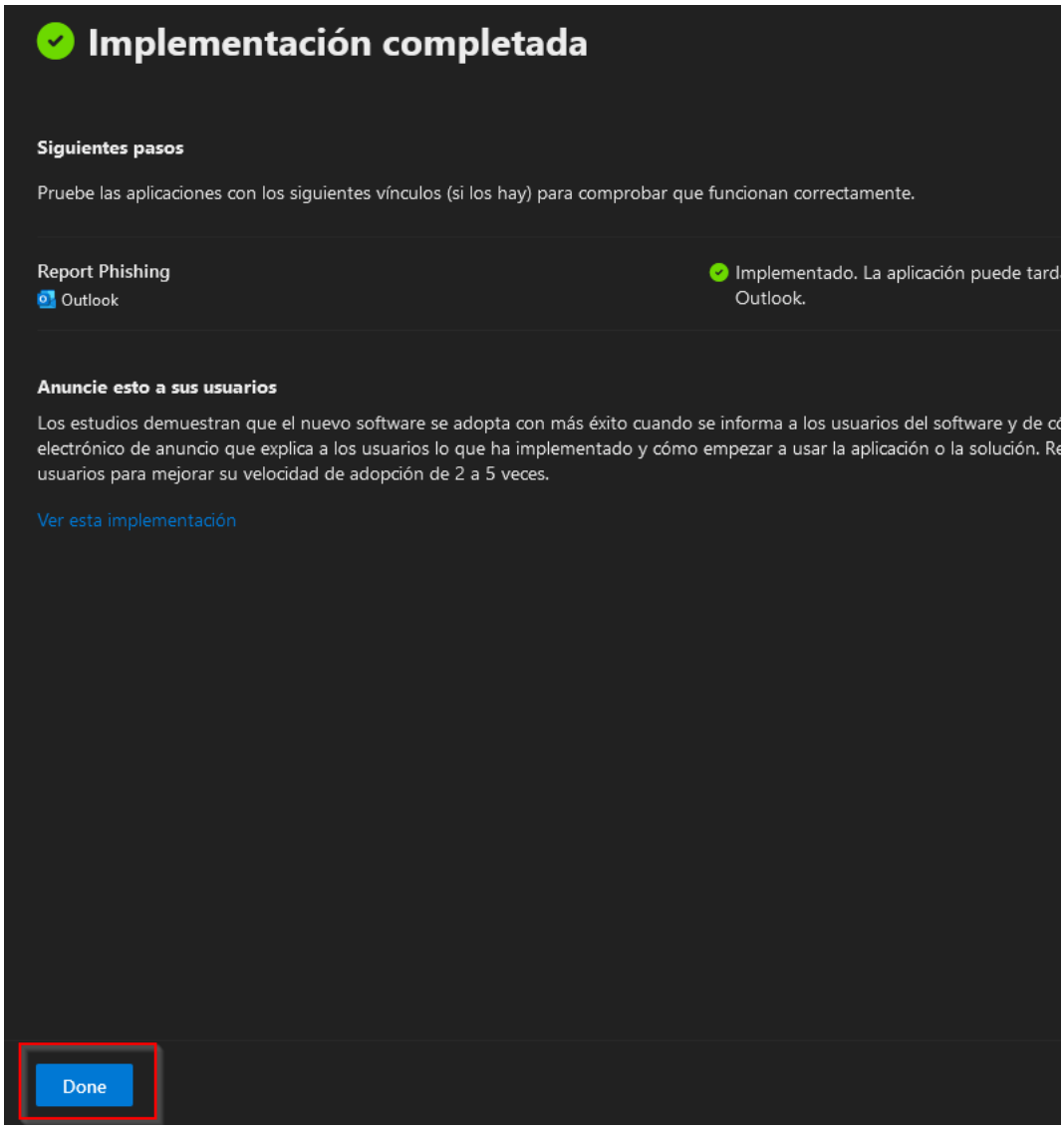
Paso	Descripción
6.	En el panel lateral izquierdo, pulse la opción “Directiva” y a continuación, pulse en “Analizador de configuración” como muestra la siguiente imagen: 
7.	En la nueva ventana, pulsa sobre “Ver recomendaciones Estricta”. 

Paso	Descripción
8.	A continuación, será necesario desplegar aquellas configuraciones donde existan recomendaciones sin aplicar, como muestra la siguiente imagen: 
9.	Desplace la ventana hacia la derecha para poder acceder al botón de “Adoptar” y posteriormente, pulse el botón “Adoptar”.  **Nota:** Será necesario repetir este procedimiento para todas las recomendaciones que estén pendientes de habilitar.
10.	Por último, diríjase al portal de aplicaciones de Microsoft para descargar el complemento “Report Phising”, puede hacerlo a través de este enlace: – https://appsource.microsoft.com/es-es/product/office/WA200002469

Paso	Descripción
11.	En la nueva ventana, pulse el botón “Obtener ahora”. 
12.	A continuación, será necesario rellenar el formulario para poder instalar la aplicación correctamente. 

Paso	Descripción
13.	Marque las opciones “Toda la organización” y pulse el botón siguiente. 
14.	De nuevo, pulse el botón siguiente en la nueva ventana. 

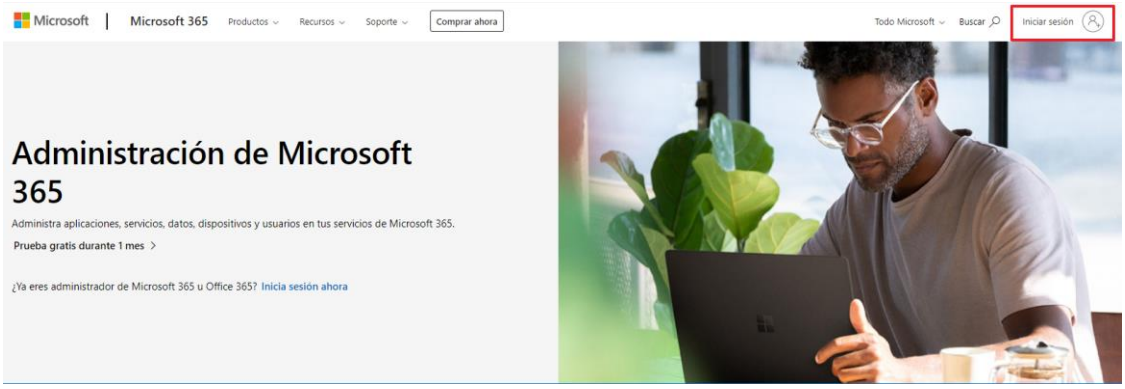
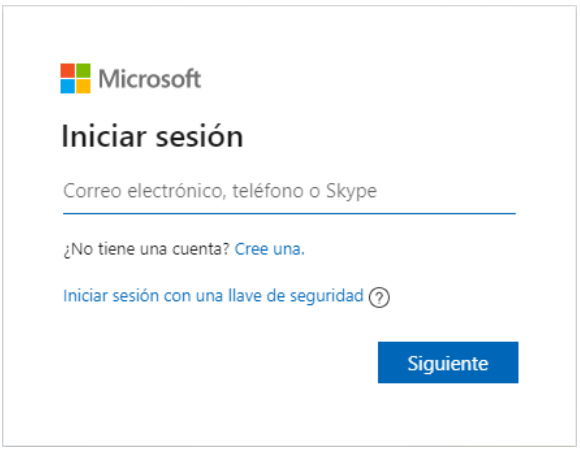
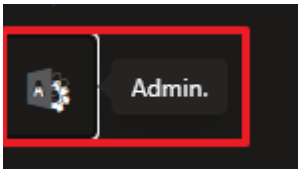
Paso	Descripción
15.	En la siguiente ventana, pulse el botón “Finalizar la implementación” 

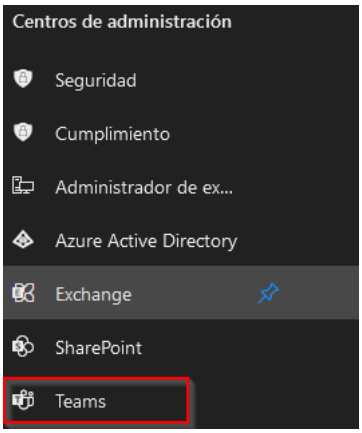
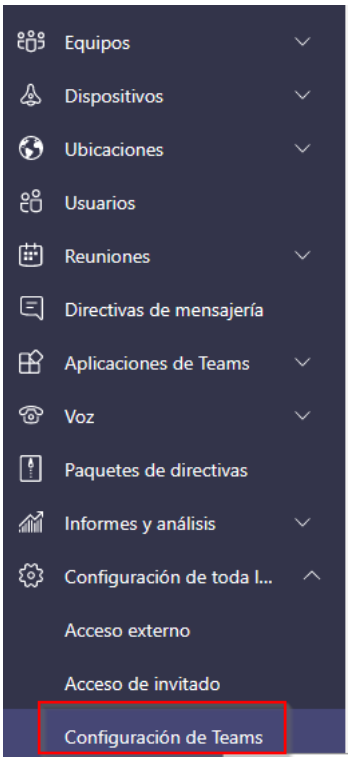
Paso	Descripción
16.	Finalmente, pulse el botón “Done” para finalizar el proceso de instalación. 

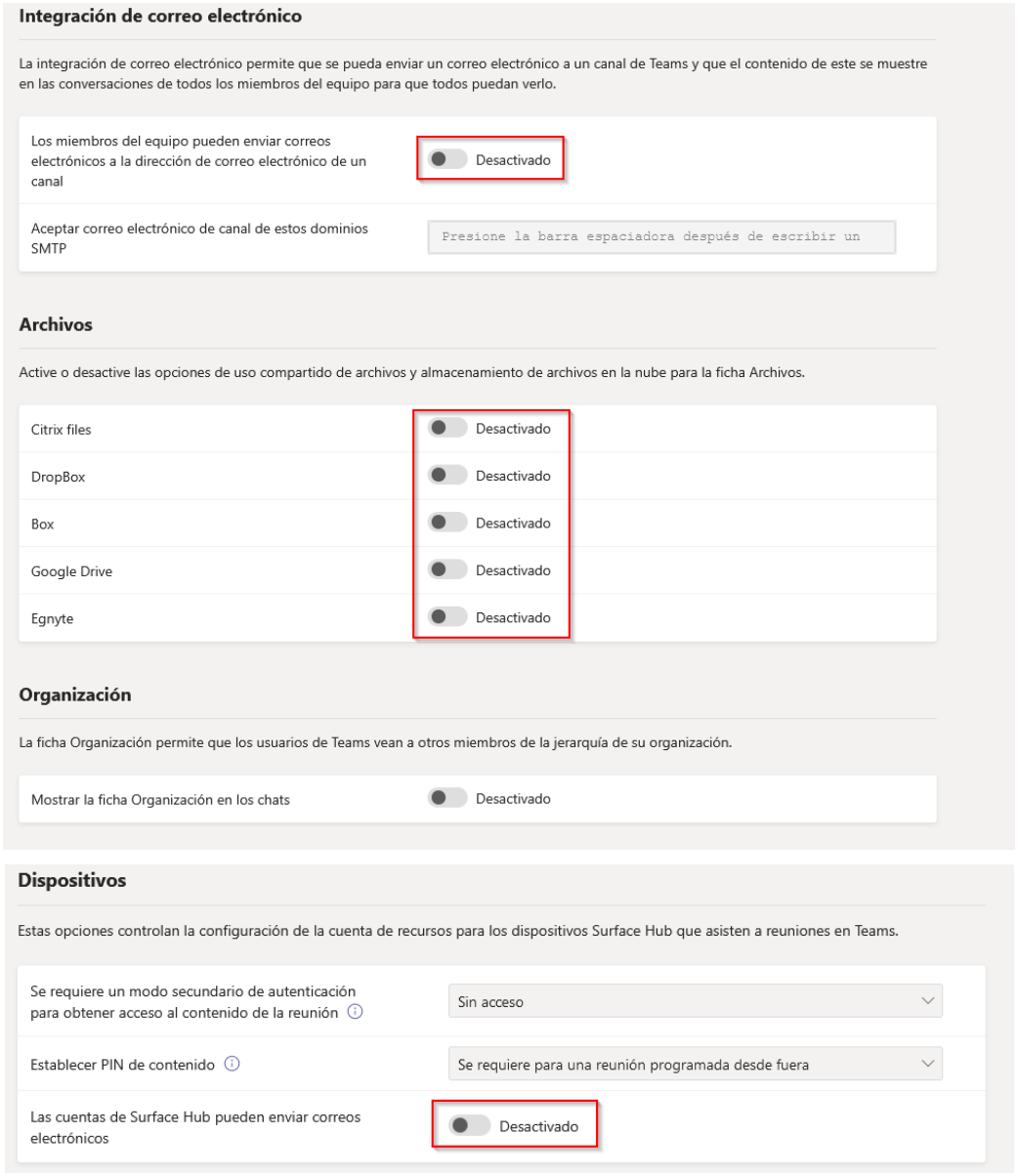
7.4 TEAMS

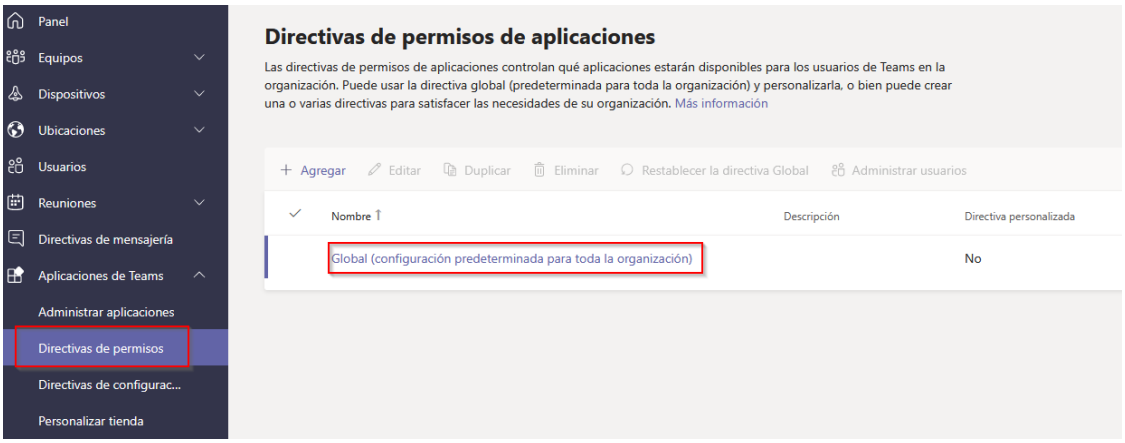
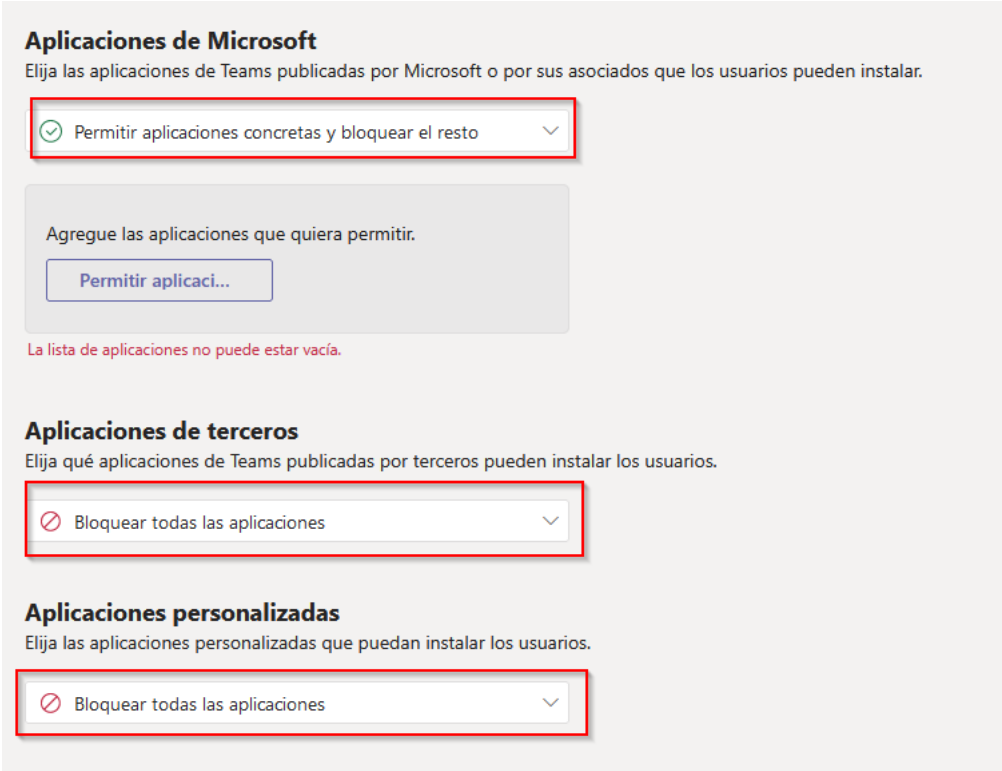
A continuación, se indican los pasos para aplicar las configuraciones manuales sobre Teams.

Paso	Descripción
1.	Acceda al portal de administración de Microsoft 365 por medio del siguiente enlace: https://www.microsoft.com/es-es/microsoft-365/business/office-365-administration

Paso	Descripción
2.	En la esquina superior derecha pulse sobre “Iniciar sesión”. 
3.	A continuación, deberá introducir las credenciales con privilegios de administración sobre Microsoft 365. Pulse “Siguiente” para continuar.  **Nota:** Es posible que se le solicite información adicional en caso de tener ya habilitado un sistema de autenticación multifactor (MFA).
4.	En el menú lateral izquierdo pulse sobre el icono de administración. 

Paso	Descripción
5.	En el menú lateral izquierdo, seleccione “Teams”. 
6.	En la nueva ventana, seleccione “Configuración de Teams” en el panel lateral izquierdo 

Paso	Descripción
7.	Establezca la configuración central según se indica a continuación: – Los miembros del equipo pueden enviar correos electrónicos a la dirección de correo electrónico de un canal→ "Desactivado". – Active o desactive las opciones de uso compartido de archivos y almacenamiento de archivos en la nube para la ficha Archivos.→ **TODOS** los métodos (Citrix, Dropbox, etc.) deben estar como "Desactivado". – Las cuentas de Surface Hub pueden enviar correos electrónicos→ "Desactivado".  **Nota:** Para el resto de configuraciones existentes en esta ventana y definidas bajo el documento "CCN- Nube Sensible - Despliegue - Tareas v1.0" deberán ser revisadas acorde al valor que más se adecue a la organización.
8.	A continuación, realice las siguientes configuraciones en el apartado de seguridad del panel de Teams. Para ello siga los pasos 1 a 5.

Paso	Descripción
9.	En el panel lateral izquierdo, seleccione “Directivas de permisos” y haga clic sobre “Global” 
10.	A continuación, configure las opciones para que se establezcan de la siguiente forma: – Aplicaciones de Microsoft→ “Permitir aplicaciones concretas y bloquear el resto”. – Aplicaciones de terceros→ “Bloquear todas las aplicaciones”. – Aplicaciones personalizadas→ “Bloquear todas las aplicaciones”. 

8. CONFIGURACIÓN DE SEGURIDAD ADICIONAL

Puede obtener más información sobre las configuraciones de seguridad de los servicios de Microsoft Azure y Office 365 consultando la serie de guías y Perfiles de Cumplimiento Específicos CCN-STIC 884 y CCN-STIC 885.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL