Implementación Tenant O365 en Grupo Planeta De Agostini, S.L.

Nombre: Sánchez Navarro, José María

Área: Administración de redes y Sistemas Operativos

Tutor: López Sánchez-Montañés, Joaquin

14/06/2023

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implementación Tenant O365 en Grupo Planeta De Agostini, S.L.*
Nombre del autor:	*Sánchez Navarro, José María*
Nombre del consultor/a:	*López Sánchez-Montañés, Joaquin*
Nombre del PRA:	*Montse Serra Vizern*
Fecha de entrega (mm/aaaa):	06/2023
Titulación:	*Grado en Ingeniería Informática*
Área del Trabajo Final:	*Administración de redes y sistemas operativos*
Idioma del trabajo:	*Castellano*
Palabras clave	*Exchange, Microsoft, Tenant, On-Premises*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El proyecto consiste en un estudio de implementación de un Tenant O365 para la empresa *Grupo Planeta De Agostini, S.L. y de la migración de los buzones del entorno actual al nuevo entorno.*

Primero se ha realizado un análisis del sistema actual basado en el Exchange On-prem que tiene configurado donde se ha analizado con ellos las necesidades de negocio que tienen y que buscan/requisitos configurados en el tenant O365.

En segundo lugar, se llevó a cabo una consultoría para guiar a la empresa en todas las situaciones que se implementarán para garantizar la correcta ejecución del proyecto y para que conozcan la configuración del nuevo tenant y cómo se llevará a cabo.

Donde el punto central del proyecto es configurar el nuevo tenant O365 para satisfacer todas las necesidades empresariales y realizar la migración de los buzones de los usuarios del entorno anterior a este nuevo entorno con la menor interrupción posible.

Por último, se presentan los plazos de ejecución en caso de que se apruebe el estudio y se proporciona una estimación de costos.

Como conclusión, se arroja la necesidad de poner en marcha el proyecto para hacer que los empleados tengan as herramientas correctas, para tener una mejor producción en su día a día.

Abstract (in English, 250 words or less):

The project consists of a study of the implementation of a Tenant O365 for the company Grupo Planeta De Agostini, S.L. and the migration of the mailboxes from the current environment to the new environment.

First, an analysis of the current system has been carried out based on the Exchange On-prem that they have configured where they have analysed with them the business needs they have and what they are looking for/requirements configured in the O365 tenant.

Secondly, a consultancy was carried out to guide the company in all the situations that will be implemented to ensure the correct execution of the project and to make them aware of the configuration of the new tenant and how it will be carried out.

Where the central point of the project is to configure the new O365 tenant to meet all business needs and to migrate the users' mailboxes from the previous environment to this new environment with as little disruption as possible.

Finally, the timelines for implementation are presented in case the study is approved and a cost estimate is provided.

As a conclusion, it shows the need to implement the project in order to provide employees with the right tools to have a better production in their day-to-day work.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Este trabajo se enfoca en llevar a cabo un estudio completo para la implementación de un nuevo tenant O365, lo cual implica la configuración inicial del tenant, identidades, licencias, seguridad, diseño técnico y funcional. Asimismo, se planificará la ejecución del despliegue del nuevo tenant O365 y su posterior migración de las 7.818 identidades (nominales i departamentales) del entorno On-prem donde trabaja los usuarios a la nueva implementación desarrollada.

El objetivo de este proyecto es mejorar el proceso de trabajo mediante la implementación del proyecto, aumentando la eficiencia de los trabajadores y mejorando la calidad de los servicios. Se ha comprobado que, durante la crisis sanitaria, el trabajo colaborativo y la mejora de la productividad se han visto favorecidos con el uso de herramientas informáticas en la nube.

Por ello, se extenderá el uso de estas herramientas a todos los miembros de la empresa, lo que permitirá que cada usuario disponga de una cuenta de correo corporativo y acceso a otras herramientas de productividad. Sin embargo, para garantizar la seguridad de la información y de los usuarios en el uso de herramientas de productividad como Microsoft 365, es fundamental implementar un tenant propio, donde esto implica tener un entorno exclusivo y controlado para la organización, lo que brinda mayor autonomía y capacidad de gestión sobre los datos y las cuentas de usuario.

Al tener un tenant propio, la empresa puede establecer políticas de seguridad personalizadas y aplicar medidas adicionales para proteger la información confidencial y evitar accesos no autorizados a través de auditorías, litigation hold, etc.

Se definirá una propuesta de Plan de gestión del Cambio para acompañar a los usuarios de este nuevo Tenant y garantizar la máxima satisfacción, el mínimo impacto y la máxima productividad durante el proceso.

Se tomarán en cuenta todas las cuestiones necesarias para llevar a cabo un estudio y una futura implementación en una empresa, donde cabe mencionar que algunos aspectos podrán ser completados después de interactuar con el cliente y realizar pruebas con los usuarios. La experiencia de otras empresas que ya lo tienen implementado, como "La Caixa", confirma las ventajas del uso de herramientas informáticas en la nube para el trabajo colaborativo y el incremento de productividad.

1.2 Objetivos del Trabajo

Los principales objetivos de este proyecto son:

- Adquirir los conocimientos necesarios de cómo está montado el servicio de correo.
- Analizar el entorno actual de la empresa y visualizar las necesidades de

negocio.
- Definir la solución final del servicio de correo electrónico en O365.
- Definir la hoja de ruta para transformar el estado actual de la plataforma hacia la solución final.
- Definir el diseño de la solución y el nuevo modelo O365.

Los objetivos parciales para lograrlo son los siguientes:

- Tener el detalle de la definición del plan de adopción.
- Tener el detalle de la definición de los casos de uso.
- Definición detallada de la implantación.
- Definir la migración de datos.

1.3 Enfoque y método seguido

Primero se va a realizar un análisis de la situación actual que tiene la empresa. Es decir, se revisa la infraestructura montada, la cantidad de buzones que se tienen que mover ya sean nominales y departamentales hi se hablará con la empresa para que nos especifique sus necesidades de negocio para poder comenzar a pensar cómo se tendrá que hacer la configuración y la migración de datos.

En segundo lugar, se realizarán reuniones entre los distintos departamentos implicados para evaluar las necesidades. Los participantes han de ser a todos los niveles:

- Comité de dirección
- Responsables de los distintos departamentos implicados
- Personal de los departamentos implicados

En dichas reuniones, se recogera la información acerca del sistema actual y que se espera del nuevo tenant. Este segundo punto, es muy importante porque de aquí se van arroja datos que va a reflejar las deficiencias y los puntos a mejorar del sistema actual de correo; así como de las nuevas funcionalidades que se deberían implementar.

Sobre la configuración del tenant, aunque se tenga toda la información recopilada por las reuniones anteriormente comentadas, también se buscara tener reuniones semanales con el departamento de IT y el jefe de proyecto de la propia empresa, para que nos comenten si hay alguna modificación o hay que añadir/quitar alguna configuración de las que se había acordado en su momento, de esa manera se mantiene actualizado el proyecto en todo momento.

Seguidamente, se va a realizar un plan de migración de los buzones On-Premises al nuevo tenant a través de la aplicación de migración Quest On Demanad Migration. Donde dicha aplicación, será la encargada de pasar la información del sistema actual al nuevo sistema

De esa manera, lo que se busca es optimizar los procesos y mejorar la eficiencia de los trabajadores a la hora de hacer sus tareas en su día a día.

1.4 Planificación del Trabajo

Jose Maria Sanchez Navarro es el único recurso asignado para realizar el trabajo. La planificación consta de 4 fases, cada una correspondiente a una entrega, donde se proporcionará información detallada de cada fase más adelante.

El diagrama de Gantt incluye las tareas, fechas de inicio y finalización, así como la duración.

Las actividades para completar el TFG se llevarán a cabo en los siguientes días y horarios:

- Lunes a viernes: de 17:30 a 23:00

Los días de descanso, como los sábados, domingos o festividades nacionales o autonómicas, no se trabajarán en el TFG.

Debido a que solo hay un recurso disponible para realizar la consultoría, la planificación se ha creado utilizando la metodología tradicional de proyecto en cascada, ya que no es posible realizar tareas en paralelo. El plan de trabajo se divide en cuatro fases claramente definidas:

Fase 1 o PEC 1: Esta fase se centra en realizar un análisis detallado del sistema actual de la empresa. En este punto, se proporcionará una visión general de los sistemas de la compañía, su evolución reciente y se definirá un objetivo general con la proyección que con lleva a la aceptación del proyecto.

Fase 2 o PEC 2: En esta fase se definirán los objetivos específicos y detallados que se pretenden alcanzar, y en base a ellos se iniciará la implementación del tenant con los objetivos hablados. Se entregará una primera parte del desarrollo bastante avanzada, donde se podrá ver mucho de los puntos que se definieron en la fase 1 o Pec1.

Fase 3 o PEC 3: En esta fase se desarrollará el núcleo principal del proyecto y se extraerán las conclusiones relevantes. Se entregará una versión prácticamente completa del proyecto, que incluirá toda la información necesaria para la implementación exitosa del nuevo sistema.

Fase 4 o PEC 4: En esta última fase se realizarán los últimos ajustes finales, incluyendo la bibliografía y los anexos pertinentes, así como la cumplimentación de la presentación del proyecto.

Una vez se hayan cumplido todas las fases mencionadas anteriormente, se entregará el TFG estructurado con la plantilla proporcionada. Es importante tener en cuenta que cada fase se ha completada de manera rigurosa para garantizar la calidad y eficacia del proyecto.

Tarea	Fecha de inicio	Fecha de fin	Memoria
Entrega PEC1: Plan de Trabajo	**01/03/2023**	**13/03/2023**	
Aclarar Tema TFG	1/03/2023	02/03/2023	
Elaboración Tema TFG	03/03/2023	10/03/2023	Propuesta Plan de Trabajo
Entrega PEC 1	13/03/2023	13/03/2023	
Entrega PEC2: Herramientas Elegidas + diseño	**20/03/2023**	**21/04/2023**	
Evaluación de los resultados PEC1	20/03/2023	22/03/2023	
Introducción	20/03/2023	24/03/2023	Memoria Técnica
Análisis de situación actual	27/03/2023	31/03/2023	Consultoría y revisión de la estructura Origen
Solución Microsoft 365	03/04/2023	07/04/2023	Consultoría + Memoria
Configuración inicial 365	10/04/2023	14/04/2023	Consultoría + Memoria
Identidades	17/04/2023	19/04/2023	Consultoría + Memoria
Entrega PEC2	20/04/2023	21/04/2023	Memoria
Entrega PEC3: Resultados	**24/04/2023**	**25/05/2023**	
Evaluación de los resultados PEC 2	24/04/2023	26/04/2023	
Seguridad	24/04/2023	04/05/2023	Consultoría + Memoria
Herramientas de colaboración	05/05/2023	09/05/2023	Consultoría + Memoria
Flujo de Correo	10/05/2023	15/05/2023	Consultoría + Memoria
Plan de gestión del cambio	16/05/2023	18/05/2023	Consultoría + Memoria
Migración de Usuarios	19/05/2023	23/05/2023	Consultoría + Memoria
Entrega PEC 3	24/05/2023	25/05/2023	Memoria
Entrega TFG y Presentación	**29/05/2023**	**14/06/2023**	
Evaluación de los resultados PEC 3	29/05/2023	31/05/2023	
Valoración productiva y Presupuestaria	29/05/2023	31/05/2023	Consultoría + Memoria
Conclusiones	01/06/2023	02/06/2023	Memoria
Bibliografía	05/06/2023	06/06/2023	Memoria
Anexos	07/06/2023	08/06/2023	Memoria
Elaboración presentación TFG	09/06/2023	13/06/2023	Memoria
ENTREGA FINAL TFG	14/06/2023	14/06/2023	

Tabla 1: Temporización de las fases de implementación.

A continuación, se muestra un gráfico de Gantt por cada tarea, los tiempos asignados y las dependencias.

Diagrama de Gantt

Nombre	Fecha de inicio	Fecha de fin
ENTREGA PEC1: Plan de Trabajo	1/03/23	13/03/23
Aclarar Tema TFG	1/03/23	2/03/23
Elaboración del plan de trabajo	3/03/23	10/03/23
Entrega PEC 1	13/03/23	13/03/23
ENTREGA PEC2: Herramientas elegidas + diseño.	20/03/23	21/04/23
Evaluación de los resultados PEC1.	20/03/23	22/03/23
Introducción.	20/03/23	24/03/23
Análisis de situación actual.	27/03/23	31/03/23
Solución Microsoft 365.	3/04/23	7/04/23
Configuración inicial 365.	10/04/23	14/04/23
Identidades.	17/04/23	19/04/23
Entrega PEC 2	20/04/23	21/04/23
ENTREGA PEC3: Resultados	24/04/23	25/05/23
Evaluación de los resultados PEC 2.	24/04/23	26/04/23
Seguridad.	24/04/23	4/05/23
Herramientas de colaboración.	5/05/23	9/05/23
Flujo de Correos.	10/05/23	15/05/23
Plan de gestión del cambio.	16/05/23	18/05/23
Planificación.	19/05/23	23/05/23
Entrega PEC 3	24/05/23	25/05/23
ENTREGA TFG Y PRESENTACIÓN	29/05/23	14/06/23
Evaluación de los resultados PEC 3	29/05/23	31/05/23
Valoración Productiva y Presupuestaria.	29/05/23	31/05/23
Conclusiones.	1/06/23	2/06/23
Bibliografía.	5/06/23	6/06/23
Anexos.	7/06/23	8/06/23
Elaboración presentación TFG.	9/06/23	13/06/23
ENTREGA FINAL TFG	14/06/23	14/06/23

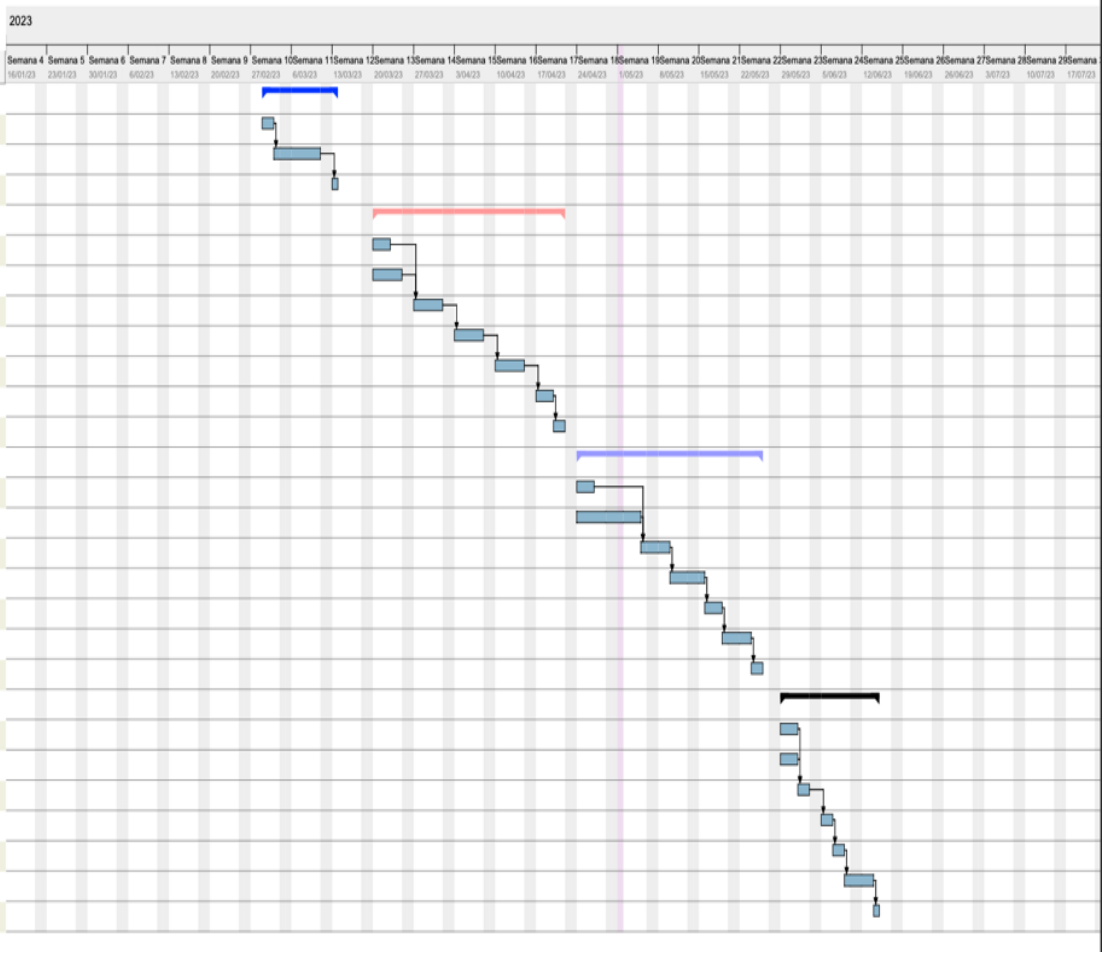

Figura 1: Planificación diagrama de Gant

1.5 Breve sumario de productos obtenidos

Se plantea una solución que tiene la empresa analizada *G*rupo Planeta De Agostini, S.l. con los sistemas actuales, donde se obtendrán los siguientes resultados:

Se creará una memoria que incluirá las actividades y prácticas recomendadas para un jefe de proyecto durante la fase de iniciación de un proyecto de migración a la nube. Además de analizar el área tecnológica, se tendrán en cuenta conceptos económicos y de recursos humanos que son importantes para asegurar el éxito de este tipo de proyecto. Se presentará un informe que incluirá:

- Un análisis del entorno actual
- La configuración que se llevará a cabo
- La migración y la gestión de cambios

Esta guía será útil para ayudar a las organizaciones en su proceso de transformación digital durante la migración de sus centros de datos tradicionales a la nube. También permitirá alinear las estrategias de negocio con las de tecnología de la información.

1.6 Breve descripción de los otros capítulos de la memoria

El presente trabajo consta de 15 capítulos donde lo que buscan, es presentar una propuesta de mejora en los sistemas de la empresa, con el objetivo de optimizar los procesos y mejorar la eficiencia de los trabajadores.

- En el primer capítulo, se centra en los antecedentes y la justificación del proyecto. Se incluye una breve descripción de la empresa y su estructura organizativa, así como los objetivos que se pretenden alcanzar con el proyecto.

- En el segundo capítulo, se realiza un análisis detallado de los requerimientos necesarios para iniciar el estudio. Se identifican los problemas y deficiencias en los sistemas actuales, lo que permitirá establecer las bases para el desarrollo del proyecto.

- En el tercer capítulo, se presenta la solución propuesta por Microsoft 365, incluyendo el licenciamiento y la lista de aplicaciones disponibles.

- En el cuarto capítulo se describe la configuración inicial de Microsoft 365.

- En el quinto capítulo, se aborda el tema de las identidades, incluyendo la infraestructura necesaria, la solución propuesta, la sincronización y el Single Sign-On.

- En el sexto capítulo, se trata el tema de la seguridad, incluyendo la implicación de la solución en la seguridad de la organización, Information Rights Management (IRM), Data Loss Prevention (DLP), Antiphising, Retención, Backup, MFA y Self Service Password Reset, así como la herramienta Intune.

- En el séptimo capítulo, se presentan las herramientas de colaboración disponibles en Microsoft 365, incluyendo Exchange Online, Teams y Power BI.

- En el octavo capítulo, se describe el flujo de correo dentro de la organización.

- En el noveno capítulo, se presenta un plan de gestión del cambio, incluyendo el alcance, la visión general y la descripción de actividades.

- En el décimo capítulo. se trata el tema de la migración de usuarios, incluyendo las herramientas de migración, el cronograma y la planificación.

- En el onceavo capítulo, se realiza una valoración productiva y presupuestaria de la solución propuesta.

Por último, en los últimos cuatro capítulos, se presentan las conclusiones obtenidas del trabajo, donde se resumen los principales resultados y se exponen las recomendaciones y sugerencias para la implementación del nuevo sistema, también se incluyen las referencias bibliográficas, los anexos correspondientes y el glosario.

2. Análisis de situación actual

2.1 Servicio de Correo

El servicio de correo actual está compuesto de una plataforma de Exchange 2016.

La totalidad de los buzones de correo de la empresa están alojados y gestionados por la granja de servidores de correo de Exchange 2016. Dicha plataforma ofrece una gran variedad de funcionalidades para el manejo de correos electrónicos, tales como la posibilidad de enviar correos con archivos adjuntos, calendarios compartidos, listas de contactos, tareas y notas, entre otros.

En resumen, el servicio de correo actual es una plataforma de Exchange 2016 que ofrece una gran variedad de funcionalidades para el manejo de correos electrónicos y cuenta con un total de 7.818 identidades, entre nominales y departamentales.

Según las extracciones que se ha podido realizar de los buzones alojados, tenemos lo siguientes datos sobres las diferentes identidades que tiene la empresa:

- Nominales: Identidades asociados a un usuario (7.002)
- Departamentales: Identidades asociados a buzones genéricos (816)

Dentro de las características principales del funcionamiento de la integración SMTP, se puede distinguir lo siguiente:

- El uso de Ironport de Cisco como herramienta de gestión de correo electrónico es muy beneficioso, ya que ayuda a gestionar el volumen de correos electrónicos entrantes y salientes, asegurando que los correos importantes lleguen a su destino y evitando que los correos no deseados (SPAM) o los correos infectados con virus dañinos lleguen a la bandeja de entrada de los usuarios pudiendo ser filtrado por la propia herramienta.

2.2 Plataforma Ofimática

En la siguiente tabla se muestra una relación entre Office 2010 y la Office 2016 que tiene implementado los usuarios en sus equipos corporativos:

Versión de Office	***Total***
Microsoft Office Professional Plus 2010	5.778
Microsoft Office Professional Plus 2016	616
Microsoft Office Standard 2016	1.424

Tabla 2: Relación entre Office 2010 y la Office 2016 que tiene implementado los usuarios.

Está previsto la migración a Office 2016. Esta actualización se comienza a realizar a principios de abril 2023 y que finalice a principios de agosto 2023.

2.3 Estructura Organizativa

Debido a la complejidad organizativa, existe una multitud de colectivos de usuarios que hay que identificar y analizar en profundidad en el momento de implementar la solución tecnología de la que es objecto este análisis.

De forma muy simplificada y genérica, se describen a continuación los principales colectivos de usuarios existentes

- Altos Cargos

  Usuarios que disponen de portátil personal, y en ocasiones de tablet i/o móvil para realizar sus tareas diarias. Entre sus tareas se encuentra la gestión de equipos i/o coordinación.

  La herramienta más utilizada para este tipo de perfil es el correo electrónico. Dicho correo, es su herramienta principal para la comunicación entre los interlocutores internos como externos.

- Personal de Oficina

  Son usuarios que no siempre tienen acceso a un ordenador portátil o de escritorio. Parte de sus tareas diarias incluyen la gestión de solicitudes de los altos cargos y la realización de tareas administrativas propias de la empresa.

  La herramienta más utilizada por este tipo de usuarios, al igual que los altos cargos, es el correo electrónico. El correo electrónico es utilizado diariamente para comunicarse tanto con interlocutores internos como externos, y también para enviar documentación.

- Personal de Almacén

  Este perfil se englobaría todos aquellos usuarios que no disponen de portátil u ordenador de mesa. Tienen que compartir el recurso con otros miembros del equipo. Se trata de un perfil en que el usuario de las herramientas ofimáticas es personal.

  La comunicación de estos usuarios con las persones internas como para las personas externos es a través del correo electrónico con el aplicativo pesado de Outlook, así como él envió de comunicación.

3. Solución Microsoft 365

Un Tenant de Microsoft es un entorno virtualizado en la nube que proporciona una plataforma centralizada para que las empresas y organizaciones administren y utilicen servicios de Microsoft como Microsoft 365 y Azure. Cada Tenant de Microsoft es único y aislado de otros tenants, lo que significa que los recursos, datos y configuraciones de una organización se mantienen separados y seguros.

Se han convertido, en una parte fundamental de la infraestructura empresarial moderna porque permiten a las organizaciones simplificar y centralizar la gestión de sus recursos de Microsoft. Con un Tenant de Microsoft, las empresas pueden administrar fácilmente sus cuentas de usuario, aplicaciones, datos y dispositivos en la nube de Microsoft desde una sola ubicación centralizada.

Además, los Tenants de Microsoft también proporcionan a las empresas una mayor seguridad y privacidad para sus datos, ya que se aíslan de otros tenants y solo los usuarios autorizados pueden acceder a ellos. Esto ayuda a proteger la información confidencial de la organización y a garantizar que se cumplan las regulaciones y normativas de privacidad de datos.

Su relevancia en el ámbito empresarial se debe a que facilitan la gestión de recursos de Microsoft y protegen la información confidencial de la organización.

También comentar, que todos los servicios de SaaS de Microsoft se ejecutan en un modelo de suscripción y un modelo de licenciamiento por usuario, por lo tanto, uno de los servicios más relevantes sobre el nuevo entorno será la gestión de identidades.

En el nuevo Tenant que se generara para dicha empresa, se consumirán principalmente los servicios de colaboración de Office 365, por ello se escogerá la licencia Microsoft 365 E3 ya que tiene integración con algunas aplicaciones empresariales. El objetivo de la empresa es centrar los esfuerzos en el servicio de correo y herramientas colaborativas como One Drive, Teams y Power Bi.

En los siguientes puntos de este documento, se describe la implementación de un nuevo tenant para la organización, y todas las características, funcionalidades y configuraciones definidas en él han sido cuidadosamente analizadas y validadas en un entorno de pruebas para garantizar la máxima eficacia.

Para llevar a cabo este proceso, se han tenido en cuenta las mejores prácticas recomendadas por Microsoft, así como una comprensión profunda del concepto de tenant. Además, se han examinado todas las características asociadas a MS365, como la gestión de dispositivos, la gestión de información y la gestión de seguridad, para asegurar que se han considerado todas las opciones y que se han seleccionado las soluciones más adecuadas para satisfacer las necesidades de la organización.

Es importante destacar que en este documento se especificarán detalladamente todas las características requeridas para la implementación del nuevo tenant en los bloques

correspondientes. De esta manera, se asegurará que se han cubierto todas las necesidades de la organización y que se han tomado en cuenta todas las consideraciones necesarias para garantizar una implementación eficaz y eficiente.

3.1 Licenciamiento

Dentro del entorno cloud de Microsoft todos los servicios se consumen por suscripción estas suscripciones se asignan a través de las diferentes licencias que asociadas al Tenant.

El planteamiento de licenciamiento que se tiene para este Tenant es la utilización mayoritariamente de licencias MS365 F3, MS365 F3+, MS365 F3++ y MS365 E3, en la siguiente captura se puede hacer una comparativa entre los diferentes niveles de licencias [1]:

	MS365 F3	MS365 F3+	MS365 F3++	MS365 E3
Aplicaciones de Office	Sí	Sí	Sí	Sí
Outlook Web App	Sí	Sí	Sí	Sí
OneDrive	Sí	Sí	Sí	Sí
SharePoint Online	Sí	Sí	Sí	Sí
Microsoft Teams	Sí	Sí	Sí	Sí
Skype Empresarial	No	Sí	Sí	Sí
Exchange Online	No	Sí	Sí	Sí
Power BI	No	No	Sí	Sí
Power Apps	No	No	Sí	Sí
Yammer	No	No	Sí	Sí
Microsoft Stream	No	No	Sí	Sí
Microsoft Planner	No	No	Sí	Sí
Microsoft Forms	No	No	Sí	Sí
Microsoft Whiteboard	No	No	Sí	Sí
Microsoft Lists	No	No	Sí	Sí
Microsoft Bookings	No	No	No	Sí
Microsoft StaffHub	No	No	No	Sí
Azure Active Directory	No	No	No	Sí
Intune	No	No	No	Sí
Windows Virtual Desktop	No	No	No	Sí
Almacenamiento OneDrive/Sharepoint	2 GB	2GB	1TB	1TB
Almacenamiento de Correo	2GB	50GB	50GB	50GB
Coste Mensual	9,23 €	11,07 €	19,37 €	29,52 €

Tabla 3: Planteamiento de licenciamiento que se tiene para este Tenant.

- MS365 F3 es la versión básica de Microsoft 365 diseñada para usuarios que no son de escritorio. Incluye las aplicaciones de Office y servicios en línea, como OneDrive, SharePoint Online y Microsoft Teams. Se destaca que en el nivel de F3 se disponen de licencia P1 de Azure Active Directory, que permite la utilización de Conditional Acces y Multifactor Autthetification dentro del Tenant, de esa manera únicamente tendrán acceso a las aplicaciones Online de la suite de Office.

- MS365 F3+ este tipo de licencia es la misma que la anterior, lo que se le agrega características adicionales, como Skype Empresarial y Exchange Online, lo que lo hace más adecuado para empresas que requieren una mayor integración de correo electrónico y comunicaciones unificadas.

- MS365 F3++ dicha licencia tiene todo lo comentado en los puntos anteriores, pero a la vez se enfoca en agregar herramientas de productividad, como Power BI, Power Apps y Yammer, para equipos que necesitan un mayor nivel de automatización y colaboración.

- MS365 E3 dicha licencias es la versión empresarial completa de Microsoft 365 y agrega características avanzadas, como Azure Active Directory, Intune y Windows Virtual Desktop, que son ideales para empresas más grandes que requieren una gestión centralizada y un mayor nivel de seguridad y control.

Remarcar también que en el caso de volver aplicar las soluciones de seguridad avanzadas que ofrece Microsoft dentro de su plataforma sería necesario adquirir licencias adicionales para ser utilizados.

3.2 Lista de aplicaciones

A continuación, se presenta un listado de las principales aplicaciones de la suite de Office 365, junto con una descripción más detallada de sus funcionalidades y capacidades de desarrollo:

- Microsoft Word: es una aplicación de procesamiento de texto que permite a los usuarios crear y editar documentos. Word también incluye herramientas de colaboración y coautoría, así como integración con otras aplicaciones de Office 365, como OneDrive y SharePoint [2]. Los desarrolladores pueden utilizar la API de Word para crear complementos y automatizar tareas específicas en documentos de Word [3].

- Microsoft Excel: es una aplicación de hoja de cálculo que permite a los usuarios realizar cálculos, análisis y visualizaciones de datos. Excel también incluye herramientas de colaboración y coautoría, así como integración con otras aplicaciones de Office 365, como Power BI y Power Automate. Los desarrolladores pueden utilizar la API de Excel para crear complementos y automatizar tareas específicas en hojas de cálculo de Excel [4].

- Microsoft PowerPoint: es una aplicación de presentación que permite a los usuarios crear y presentar diapositivas. PowerPoint también incluye herramientas de colaboración y coautoría, así como integración con otras aplicaciones de Office 365, como OneDrive y SharePoint. Los desarrolladores pueden utilizar la API de PowerPoint para crear complementos y automatizar tareas específicas en presentaciones de PowerPoint [5].

- Microsoft Outlook: es una aplicación de correo electrónico y calendario que permite a los usuarios enviar y recibir correos electrónicos, programar reuniones y eventos, y administrar tareas y contactos. Outlook también incluye herramientas de colaboración y coautoría, así como integración con otras aplicaciones de Office 365, como SharePoint y Microsoft Teams. Los desarrolladores pueden utilizar la API de Outlook para crear complementos y automatizar tareas específicas en correos electrónicos y calendarios de Outlook [6].

- Microsoft OneDrive: es una aplicación de almacenamiento en la nube que permite a los usuarios almacenar y compartir archivos. OneDrive también incluye herramientas de colaboración y coautoría, así como integración con otras aplicaciones de Office 365, como Word, Excel y PowerPoint. Los desarrolladores pueden utilizar la API de OneDrive para crear complementos y automatizar tareas específicas en archivos almacenados en OneDrive [7].

- Microsoft SharePoint: es una plataforma de colaboración y gestión de contenido que permite a los usuarios crear sitios web y aplicaciones empresariales personalizadas. SharePoint también incluye herramientas de colaboración y coautoría, así como integración con otras aplicaciones de Office 365, como Power Apps y Power Automate. Los desarrolladores pueden utilizar la API de SharePoint para crear soluciones personalizadas y hacer que estén disponibles para el personal en toda la organización [8].

- Microsoft Teams: es una plataforma de colaboración y comunicación que permite trabajar en equipo en tiempo real y compartir archivos, documentos y recursos. Teams también incluye herramientas de integración y personalización, así como integración con otras aplicaciones de Office 365, como Power Apps y Power Automate. Los desarrolladores pueden utilizar la API de Teams para crear aplicaciones personalizadas y ampliar la funcionalidad de Teams [9].

- Microsoft Power BI: es una herramienta de análisis y visualización de datos empresariales que permite a los usuarios crear paneles e informes personalizados para el análisis de datos empresariales. Con Power BI, los usuarios pueden conectarse a diferentes fuentes de datos y crear visualizaciones interactivas. Los desarrolladores pueden crear soluciones personalizadas para sus empresas y hacer que estén disponibles para el personal en toda la organización [10].

- Microsoft Power Automate: es una plataforma de automatización de flujos de trabajo que permite a los usuarios automatizar tareas y procesos empresariales

mediante la conexión de diferentes aplicaciones y servicios. Los usuarios pueden crear flujos de trabajo con una interfaz visual y sin necesidad de escribir código. Power Automate también incluye integración con otras herramientas de Office 365, como SharePoint y Microsoft Teams.

- **Microsoft Power Apps:** es una plataforma de desarrollo de aplicaciones empresariales que permite crear aplicaciones personalizadas sin necesidad de escribir código. Los usuarios pueden diseñar aplicaciones con una interfaz visual intuitiva que incluye elementos de diseño predefinidos. Power Apps también incluye integración con otras herramientas de Office 365, como SharePoint y Microsoft Teams, para que los usuarios puedan crear soluciones más completas [11].

La suite de Office 365 incluye una amplia variedad de aplicaciones que permiten a los usuarios crear, compartir y colaborar en documentos y archivos empresariales. Los desarrolladores tienen acceso a una variedad de herramientas y API para crear soluciones personalizadas y ampliar la funcionalidad de las aplicaciones.

4. Configuración inicial O365

Antes de la configuración inicial hace falta obtener el tenant propio, por lo que se adjunta los pasos a seguir:

1. **Acceder al sitio web de Microsoft 365:** Abre tu navegador web y visita el sitio web oficial de Microsoft 365 (https://www.microsoft.com/microsoft-365).

2. **Crear una cuenta de Microsoft:** Si aún no se tiene una cuenta de Microsoft, se debería crear una, los pasos seria:

   2.1 Haz clic en "Registrarse" o "Crear cuenta" y sigue las instrucciones para crear tu cuenta, se tiene asegurar de utilizar una dirección de correo electrónico válida y segura.

3. **Elegir un plan de Microsoft 365:** En este caso se ha de escoger el Plan E3 donde ofrece todas las necesidades que esta gran empresa necesita.

4. **Iniciar el proceso de compra:** Una vez que se haya seleccionado el plan adecuado, hacer clic en "Suscribirse" para comenzar el proceso de compra.

5. **Proporciona la información requerida:** Durante el proceso de compra, se te pedirá información de la empresa para que quede registrada con dicho tenant.

6. **Configura y personaliza tu tenant:** Una vez que se haya realizado la compra, se recibirá instrucciones sobre cómo configurar y personalizar el tenant de Microsoft 365 adquiridos.

7. **Configuraciones Iniciales:** Una vez tenido el tenant uno de los aspectos que se tiene que realizar es el acceso a los recursos del Tenant donde se encuentra restringido a los miembros de la organización principalmente. Por tal de cumplir los requerimientos, se proponen la siguiente configuración:

    - **Acceso de los usuarios invitados:** Se recomienda limitar el acceso a los propietarios y la pertenencia de los objetos de su propio directorio, de esa manera, los usuarios invitados no serán capaces de acceder a las propiedades de los objetos del directorio.

    - **Invitaciones:** Se recomienda limitar la posibilidad de invitar a usuario externos al Tenant, solo ciertos roles específicos.

    - **Restricciones de colaboración:** Se recomienda limitar los dominios en los cuáles se pueda enviar una limitación únicamente aquellos dominios en el que se confíen o que sean estrictamente necesarios.

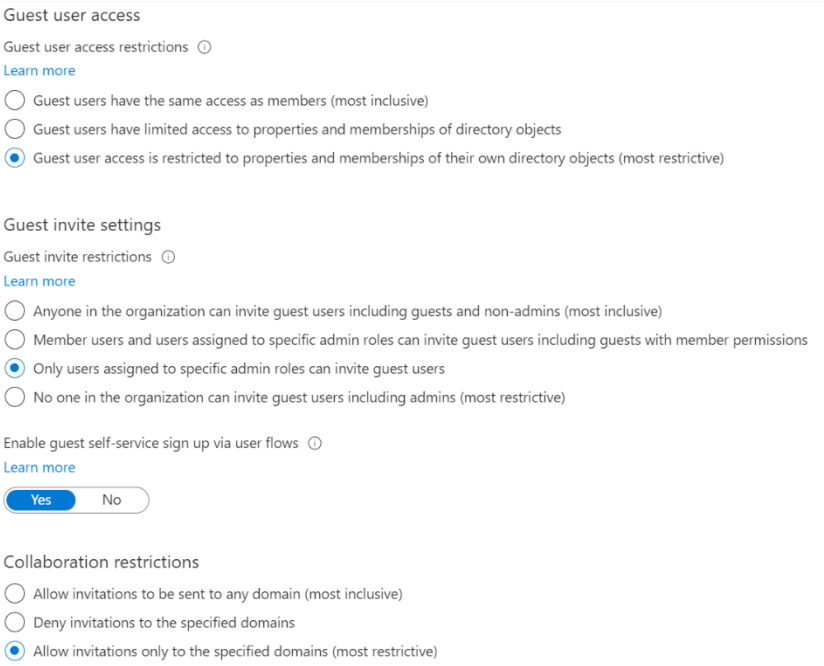

Figura 2: acceso a los recursos del Tenant.

Para diseñar en un Tenant el Azure Active Directory todos los usuarios de este Tenant deben tener permisos de lectura sobre el directorio, por tal de proteger los datos de los usuarios y limitar el acceso a la consola de Azure Active Directory se recomienda aplicar la siguiente configuración:

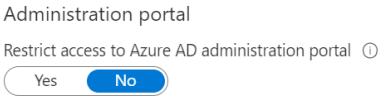

Figura 3: Administración del portal.

De esa manera limitas el acceso a la consola de Azure AD únicamente a los usuarios administradores.

Se recomienda, también limitar la capacidad de los usuarios para registrar aplicaciones en Azure AD utilizando la siguiente configuración

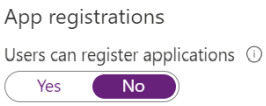

Figura 4: Registro de aplicaciones.

A la vez, se recomienda limitar la capacidad de los usuarios para enrolar dispositivos de Azure Active Directory. De esa manera, se da garantía que únicamente los usuarios específicos serán capaces de unir dispositivos al Tenant y verificar estas identidades con una autentificación de doble factor.

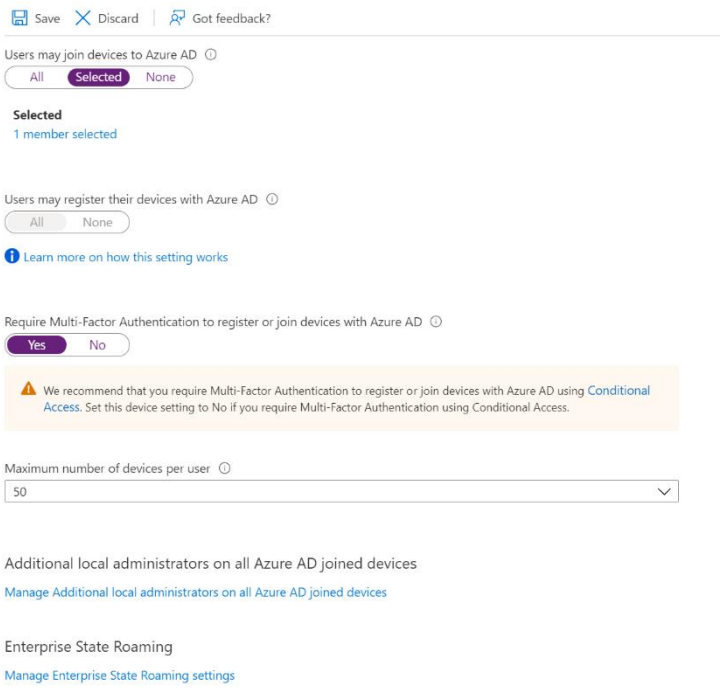

Figura 5: Limitar la capacidad de los usuarios.

5. Identidades

Uno de los elementos claves de los nuevos servicios de colaboración de Microsoft son las identidades. En este entorno es muy importante definir correctamente la gestión de las identidades para garantizar el correcto funcionamiento de la plataforma.

Para lograr una correcta gestión de identidades en los servicios de colaboración de Microsoft, es importante comprender el papel de Azure Active Directory (Azure AD) y Active Directory (AD) en el entorno de usuario.

Por la existencia de dos proveedores de identidades dentro del entorno del usuario puede generar complejidad en la gestión de las identidades. Para simplificar esta gestión y garantizar una experiencia de usuario homogénea, es necesario tener un servicio de sincronización entre los proveedores de identidades.

En este sentido, Microsoft ofrece Azure AD Connect es una herramienta que permite la sincronización de identidades entre AD y Azure AD. Con dicha herramienta, es posible sincronizar las identidades de los usuarios, grupos y dispositivos de AD con Azure AD, lo que permite a los usuarios acceder a los recursos de la nube de Microsoft utilizando las mismas credenciales que utilizan para acceder a los recursos On-Premises.

Además, con Azure AD Connect es posible habilitar la autenticación de paso a través (Passthrough Authentication) y la autenticación con hash de contraseñas (Password Hash Sync), lo que proporciona una experiencia de inicio de sesión sin fisuras para los usuarios y garantiza la seguridad de las credenciales [12].

Por lo que se puede garantizar una gestión de identidades adecuada a los servicios de colaboración de Microsoft, por lo que es necesario sincronizar las identidades entre AD y Azure AD utilizando Azure AD Connect, con lo que permite a los usuarios acceder a los recursos On-Premises y en la nube de Microsoft utilizando las mismas credenciales y proporciona una experiencia de usuario homogénea.

5.1 Infraestructura necesaria

Asociada al servicio de identidades se utilizará la siguiente infraestructura.

- Controladores de dominios existentes en el forest de la empresa
- Un servidor que ejecutara los servicios de sincronización AD connect.

Actualmente, se desconoce la estructura desplegada del directorio activo por el que se supondrá que es una infraestructura mínima para garantizar el servicio

Los requerimientos de red de la arquitectura son los siguientes [13]:

1. Connectividad entre Active Directory y Azure AD Connect

    - DNS (53 TCP/UDP)
    - Kerberos (88 TCP/UDP)
    - MS-RPC (135 TCP)
    - LDAP (389 TCP/UDP)
    - SMB (445 TCP)
    - LDAP SSL (636 TCP/UDP)
    - RPC (49152 – 65535 TCP)
    - WinRM (5985 TCP)
    - AD DS Web Services (9389 TCP)
    - Global Catalog (3268 TCP)

2. Connectividad entre Azure AD Connect y Azure AD

    - HTTP (80 TCP)
    - HTTPS (443 TCP)

5.2 Solución propuesta

Para cumplir con las recomendaciones explicadas anteriormente se ha pensado en realizar la configuración siguiente:

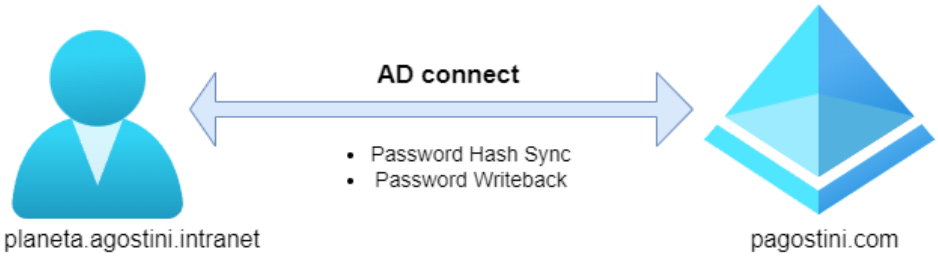

Figura 6: Solución propuesta.

Se utilizará el directorio actual asociado al lugar de trabajo como fuente de identidades. La utilización de este directorio permitirá una integración entre el lugar de trabajo y los nuevos servicios de colaboración

Por tal de mantener la sincronización entre los dos directorios se utilizará la solución de Microsoft AD Connect, que será el encargado de aprovisionar toda la información a las identidades existentes a Azure Active Directory.

Dentro de los servicios de sincronización se incluiría las siguientes features:

- **Password Hash:** Se sincronizará el hash del password de los usuarios hacia la nube, de esta manera se consigue acceso a Seamless SSO, que permite utilizar el proceso de autentificación al equipo para acceder a los servicios de colaboración sin introducir de nuevo el password. También se obtiene un entorno de contingencia en el caso de indisponibilidad de los servicios del directorio para que usuarios pueda seguir accediendo a las aplicaciones de colaboración [14].

- **Password WriteBack:** En un entorno hibrido existe la posibilidad de reiniciar la contraseña tanto en el entorno On-Premises como en el entorno nube, por tal de mantener la coherencia de los usuarios y aprovechar las herramientas de gestión de password en la nube se habilitará la propagación de password de nube a On-Premises [15].

5.3 Sincronización

Con el objetivo de mantener una experiencia homogénea al acceder a los diferentes recursos corporativos, es necesario implementar un servicio de sincronización entre las dos fuentes de identidad existentes.

Esta sincronización se llevará a cabo utilizando la herramienta propia de Microsoft Azure AD Connect. En este caso, la sincronización se realiza solo en uno de los servicios de identidad, específicamente en el servicio de Active Directory.
Por lo tanto, la gestión de las identidades se realizará de la misma manera que se hace actualmente, realizando cualquier modificación en los servicios locales del directorio (On-Premises). Bajo estas premisas, la gestión del ciclo de vida de las identidades se realizará en Active Directory, y los servicios de sincronización se encargarán de trasladar cualquier modificación (altas, bajas y modificaciones) a Azure Active Directory.

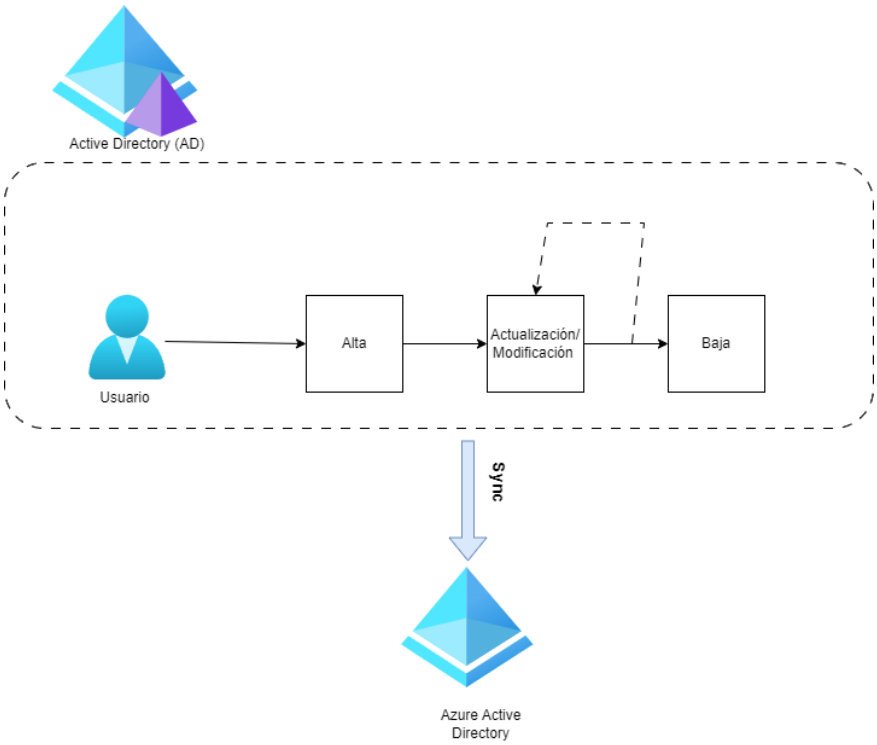

Figura 7: Sincronización de identidades.

El servicio de sincronización implica que todos los atributos informados a las identidades basadas en la nube tienen una dependencia directa de los atributos informados a las identidades On-Premises. Esta información es sincronizada utilizando la regla que se define dentro de la herramienta Azure AD Connect, estas reglas permiten definir que atributos sincronizan, que atributos son destino y si es necesario definir reglas para transformar ciertos atributos acordados [16].

5.4 Atributos y reglas de sincronización

Como se ha mencionado anteriormente, es fundamental que todos los atributos que se deseen informar en Azure Active Directory estén correctamente registrados en las identidades locales (On-Premises).

Los atributos mínimos de una identidad a Azure Active Directory son los siguientes:

- User Name
- Name

Por tanto, habrá que garantizar que los dos atributos se aprovisionan y se sincronizan correctamente, por lo que se ha definido a través de las necesidades de negocio que sería necesario sincronizar los siguientes atributos:

- Displayname
- Ubicación
- Cargo
- Departamento

Dentro de las reglas de sincronización es necesario tener en cuenta el ciclo de vida de las identidades y definir correctamente las reglas adecuadas para cada uno de los procesos asociados en este ciclo

- Altas:

  Entendemos como alta de usuario el proceso de generación de un nuevo usuario a la organización, durante este proceso se aprovisionará y se informará la identidad a Active Directory siguiendo los procesos existentes a la organización.

  Una vez aprovisionada la identidad los servicios de sincronización generarán un nuevo usuario a Azure Activo Directory y vincularán esta nueva identidad a la generada a Active Directory. Este proceso es importante, ja que se ha de definir correctamente la regla para la generación de este nuevo usuario a la nube, nos centraremos en este caso en el user name de este nuevo usuario, mientras que el resto de los atributos serán informados según las reglas de sincronización definidas.

  Se decide utilizar el UPN existente a Active Directory para generar el nuevo usuario a Azure Activo Directory.

- Actualizaciones:

  Entendemos como actualización cualquier modificación que se realice sobre una identidad existente, en este caso se realizarán las modificaciones sobre el usuario existente a Active Directory y serán las reglas de sincronización definidas a Azure

AD Connect las encargadas de trasladar estas modificaciones a la identidad ubicada a la nube.

- **Bajas:**

  Entendemos que las bajas es el proceso de eliminar un usuario del sistema. En este caso se tendría que cumplir los protocolos definidos tanto en On-Premises como en la nube, por lo que se tiene que garantizar que el usuario no tenga acceso a los recursos corporativos cuando se ejecute la baja.

  El proceso seria:

Figura 8: Proceso de Bajas.

Entendemos que el proceso asociado a las identidades On-Premises ya se encuentran consolidades dentro de la organización por lo que únicamente sería necesario definir las reglas de sincronización adecuados para eliminar los usuarios ubicados en la nube.

5.5 Single Sign-On

El Active Directory es un servicio de directorio desarrollado por Microsoft que se utiliza para almacenar información sobre los recursos de una red, incluyendo usuarios, grupos y dispositivos. Una de las ventajas clave del Active Directory es la posibilidad de habilitar el Single Sign-On (SSO), que permite a los usuarios acceder a múltiples recursos con una única autenticación [17].

El SSO es una funcionalidad que simplifica la experiencia de los usuarios al eliminar la necesidad de recordar múltiples nombres de usuario y contraseñas. Con el SSO, los usuarios solo necesitan autenticarse una vez para acceder a varios recursos, lo que aumenta la eficiencia y la productividad en el trabajo.

La utilización del Active Directory en la nube presenta un desafío adicional, ya que los recursos se encuentran distribuidos en diferentes ubicaciones y proveedores de servicios en la nube. Para abordar este problema, se puede utilizar Seamless SSO como solución.

Seamless SSO es una funcionalidad de Azure Active Directory (Azure AD) que permite a los usuarios autenticarse en la nube de forma transparente sin la necesidad de volver a introducir su contraseña. Seamless SSO utiliza la tecnología de Kerberos para autenticar automáticamente al usuario con su contraseña de Active Directory cuando accede a aplicaciones en la nube que están integradas con Azure AD.

La implementación de Seamless SSO simplifica el despliegue de la solución y reduce los requerimientos de infraestructura, así como la carga administrativa asociada. Al no requerir que los usuarios introduzcan sus credenciales de inicio de sesión, se elimina la necesidad de sincronizar las contraseñas entre Active Directory y Azure AD, lo que reduce la complejidad y los costos asociados.

Por lo que, la habilitación del SSO en el Active Directory y la utilización de Seamless SSO como solución en la nube mejora significativamente la experiencia de los usuarios al permitirles acceder a múltiples recursos con una única autenticación. Además, la implementación de Seamless SSO simplifica el despliegue de la solución y reduce la carga administrativa y los requerimientos de infraestructura asociados.

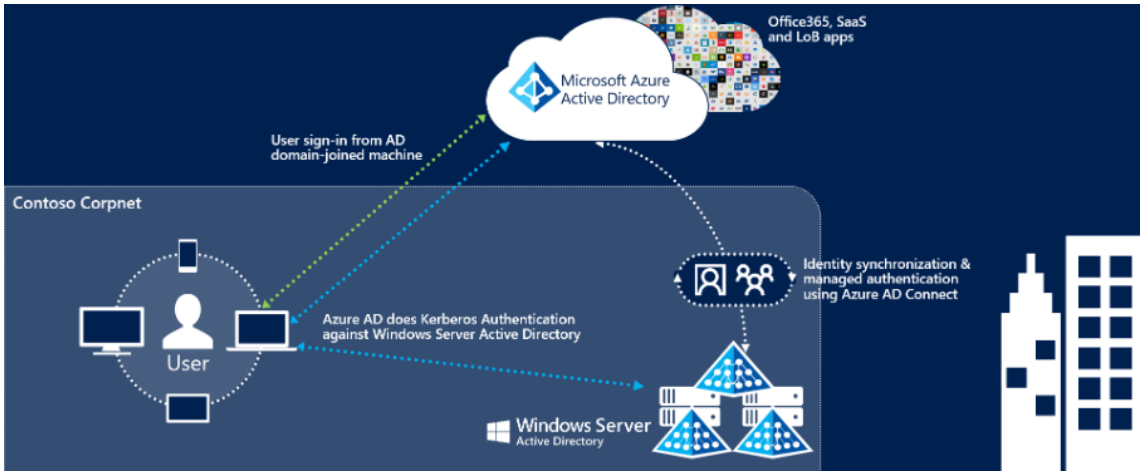

Figura 9: Cómo conectar SSO.

Para habilitar Seamless SSO, es necesario cumplir con los siguientes requisitos:

- Tener una cuenta de Azure Active Directory (Azure AD) habilitada.
- Tener una suscripción a Azure AD Premium P1 o superior para habilitar la funcionalidad de Seamless SSO.
- Tener un dominio personalizado en Azure AD.
- Configurar la sincronización de contraseñas de Active Directory a Azure AD utilizando Azure AD Connect.
- Configurar el inicio de sesión único de Azure AD para las aplicaciones y recursos en la nube que se deseen integrar con Seamless SSO.
- Configurar las reglas de acceso de usuario en Azure AD para que los usuarios puedan acceder a las aplicaciones y recursos en la nube que se han integrado con Seamless SSO.
- Tener acceso a los registros de eventos de Active Directory y Azure AD para solucionar problemas y depurar problemas de autenticación.
- El equipo tiene que estar en uno de los siguientes estados
    - Azure AD Joined
    - Azure AD Registered
    - Azure AD Hybrid Joined

Una vez que se cumplen estos requisitos, es posible habilitar Seamless SSO en la cuenta de Azure AD y configurarlo para las aplicaciones y recursos en la nube que se deseen integrar. Es importante tener en cuenta que la implementación exitosa de Seamless SSO requiere un conocimiento técnico sólido y experiencia en la administración de Azure AD y Active Directory, por lo que es recomendable buscar asistencia de un experto en caso de necesitar ayuda.

A continuación, se describe cada uno:

	Azure AD Joined	Azure AD Registered	Azure AD Hybrid Joined
Descripción	Dispositivos corporativos que acceden con una cuenta corporativa de Azure AD	Dispositivos que no requieren una cuenta corporativa por acceso	Dispositivos unidos a una Active Directory que requiere una cuenta corporativa
Sincronización de credenciales	Las credenciales de usuario se sincronizan con Azure AD mediante Azure AD Connect.	No se sincronizan las credenciales de usuario.	Las credenciales de usuario se sincronizan con Azure AD mediante Azure AD Connect.
Autenticación	Los usuarios pueden autenticarse en el dispositivo utilizando sus credenciales de Azure AD.	Los usuarios pueden autenticarse en el dispositivo utilizando sus credenciales de Azure AD o de otro proveedor de identidad compatible.	Los usuarios pueden autenticarse en el dispositivo utilizando sus credenciales de Active Directory local y de Azure AD.
Administración de dispositivos	Los dispositivos se administran a través de Azure AD.	Los dispositivos se administran a través de MDM (Mobile Device Management).	Los dispositivos se administran a través de Active Directory local y de Azure AD.
Audiencia	• Todos los usuarios • Escenarios Híbridos y nube	• Dispositivos BYOD • Dispositivos móviles	• Todos los usuarios • Entornos que mantienen infraestructura basada en AD
Propiedad del equipo	Organización	Organización y Usuario	Organización
Sistemas Operativos	Windows 10	• Windows 10 • IOS • Android • Mac Os	Windows 10,8.1,7
Métodos de autentificación	• Password • Windows Hello for Business	• Credenciales locales • Password • Windows Hello	• Password • Windows Hello for Business (W10)

	• FIDO2.0 security Keys	• PIN • Biometria	
Capacidades clave	• SSO a recursos cloud y On-Prem • Self Service Password Reset y Windows Hello PIN reset des de la pantalla de bloqueo • Políticas de acceso condicionales basados en MDM • Roaming de la configuración corporativa entre dispositivos	• SSO a recursos cloud Conditional Acces basados en MDM • Conditional Acces basado en políticas de APP Protection • Autentificación basada en políticas de APP Protection • Autenticación basada a través del móvil usando MS autenticator	• SSO a recursos cloud y On-Prem • Self Service Password Reset y Windows Hello PIN des de la pantalla de bloqueo • Politicas de acceso condicionals basado en MDM • Roaming de la configuración corporativa entre dispositivos

Tabla 3: Estado de los dispositivos de Azure AD.

Hoy en día, la autenticación es un aspecto crítico en cualquier entorno de red, ya que garantiza que solo los usuarios autorizados puedan acceder a los recursos protegidos. A medida que la tecnología ha evolucionado, ha habido un cambio hacia entornos de red híbridos, en los que se combinan recursos en la nube y en las instalaciones locales.

Dentro de estos entornos híbridos, existen diferentes estrategias de autenticación que pueden utilizarse para garantizar la seguridad de los recursos protegidos. Una de estas estrategias es el Hybrid Joined, que se ha convertido en una opción popular debido a su eficacia en la autenticación de dispositivos.

En esencia, es una estrategia que permite a los dispositivos unirse a un dominio local mientras mantienen la capacidad de autenticarse en la nube. Esto se logra mediante la creación de una relación de confianza entre el dispositivo y el servicio de autenticación de la nube.

La carga administrativa es reducida en comparación con un entorno registrado porque el proceso de registro es menos complejo y más eficiente. Por lo que los dispositivos simplemente se unen al dominio local como lo harían normalmente y luego utilizan las credenciales de autenticación de la nube para acceder a los recursos protegidos en línea. Esto reduce el tiempo y el costo de administración de la infraestructura.

Además, el uso también ofrece capacidades interesantes en la autenticación de dispositivos. Por ejemplo, permite a los administradores controlar y auditar los dispositivos que se unen a la red, lo que ayuda a reducir el riesgo de ataques cibernéticos y a garantizar la seguridad de la red. También permite la autenticación multifactorial, lo

que significa que se pueden utilizar varias capas de autenticación para aumentar la seguridad y proteger aún más los recursos.

En conclusión, como estrategia de autenticación en entornos híbridos es una opción atractiva debido a su eficacia en la autenticación de dispositivos, a la reducción de la carga administrativa y a la vez se obtiene capacidades interesantes en la autentificación en los dispositivos.

6. Seguridad

La seguridad es uno de los aspectos más importantes a considerar en cualquier solución de nube, y la solución de Microsoft no es una excepción. Microsoft cuenta con un conjunto de medidas de seguridad y protección de datos para proteger los recursos en la nube y garantizar la privacidad y confidencialidad de los datos de los usuarios.

Entre los elementos de seguridad más relevantes en la solución de nube de Microsoft se encuentran [18]:

- **Autenticación y autorización:** La autenticación y la autorización son esenciales para la seguridad en cualquier sistema. Microsoft proporciona Azure Active Directory (Azure AD), un servicio de identidades basado en la nube que permite autenticar y autorizar a los usuarios para acceder a los recursos de la nube. Azure AD es compatible con diversos protocolos de autenticación, incluyendo OpenID Connect, OAuth 2.0, SAML, WS-Federation, entre otros.

- **Encriptación de datos:** La encriptación de datos es otra medida esencial para garantizar la seguridad en la nube, donde se ofrece opciones de encriptación para los datos en tránsito y en reposo. Los datos en tránsito se protegen mediante el cifrado SSL/TLS, mientras que los datos en reposo se pueden encriptar mediante el cifrado AES-256. Además, se permite a los usuarios administrar sus propias claves de encriptación para tener un mayor control sobre la protección de sus datos.

- **Protección contra amenazas y vulnerabilidades:** Microsoft cuenta con medidas de seguridad avanzadas para proteger los recursos en la nube contra amenazas y vulnerabilidades. Esto incluye la detección y prevención de ataques de denegación de servicio (DDoS), la protección contra ataques de phishing y la identificación de vulnerabilidades de seguridad en tiempo real.

- **Cumplimiento normativo:** La solución de nube de Microsoft cumple con una amplia variedad de normativas y regulaciones de seguridad, incluyendo ISO 27001, HIPAA, GDPR, entre otras. También, ofrece herramientas de cumplimiento y auditoría para ayudar a los usuarios a cumplir con sus propios requisitos de seguridad.

La solución de Microsoft cuenta con un conjunto de medidas de seguridad y protección de datos para garantizar la seguridad, privacidad y confidencialidad de los datos de los

usuarios. Esto incluye medidas de autenticación y autorización, encriptación de datos, protección contra amenazas y vulnerabilidades y cumplimiento normativo, donde los usuarios pueden confiar en la solución de nube de Microsoft para mantener un nivel de seguridad que cumpla los estándares definidos.

Por lo que, uno de los aspectos con más importancia de la nueva solución a la nube se mantener un nivel de seguridad que cumpla los estándares definidos, en el siguiente apartado se tratan algunos de los elementos de seguridad más relevantes dentro de la solución.

6.1 Implicación de la solución

Dentro de la plataforma cloud de Microsoft existen ciertas funcionalidades que se ven introducidas por el propio diseño de la plataforma y por el funcionamiento de las diferentes herramientas que Microsoft pose a disposición de la organización.

La plataforma cloud de Microsoft es una de las más utilizadas a nivel mundial para alojar diferentes tipos de aplicaciones y servicios. Entre las funcionalidades que se pueden encontrar dentro de esta plataforma, se destacan aquellas que se ven introducidas por el propio diseño de la plataforma y por el funcionamiento de las diferentes herramientas que Microsoft posee a disposición de la organización.

Una de las principales funcionalidades que se pueden encontrar en la plataforma cloud de Microsoft es la integración con otras herramientas y servicios de la compañía, como por ejemplo Office 365, Dynamics 365, SharePoint, OneDrive, Teams, entre otros. Esto permite a las organizaciones utilizar estas herramientas de manera conjunta y de forma más eficiente, así como también compartir información de manera segura y controlada.

Sin embargo, esta integración también puede generar riesgos de seguridad, como el acceso no autorizado a la información, la pérdida de datos, la exposición de información confidencial, entre otros. Por esta razón, es importante aplicar recomendaciones de seguridad definidas por el CCN (Centro Criptológico Nacional) para mitigar estos riesgos y garantizar la seguridad de la información, se exponen todas las medidas en el apartado de anexos [19].

6.2 Information Rights Management (IRM)

Teniendo en cuenta que la información esta accesible a trabas de internet y que se posible enviar esta información a trabas de las diferentes herramientas de colaboración, necesitamos una herramienta que permita garantizar que un fichero únicamente puede ser consumido por un usuario o grupo de usuarios autorizados.

En este caso existe una solución dentro de la organización que se encarga de gestionar estos accesos SealPath, integrado con la suite de Office y con soluciones de Office 365 como Sharepoint nos permitirá proteger toda la información de la organización.

Será necesario validar el correcto funcionamiento de la solución en función de los casos de se defina para garantizar el cumplimiento de las directivas de protección vigentes.

Como alternativa a la solución de SealPath encontramos Azure Information Protection P1 que incluido dentro de la suite de seguridad de Office 365 con la licencia F3 no supondría un coste adicional en la hora de proteger la información, en el caso de necesitar opciones avanzadas de protección se podría adquirir Azure Information Protection P2 para los usuarios que lo requieran [20].

A la siguiente tabla se describen las capacidades de securizacion de Azure Information Protection en todos los tiers disponibles [21]:

Comparing Azure Information Protection plans

FEATURES	Azure Information Protection for Office 365	Azure Information Protection Premium P1	Azure Information Protection Premium P2
Azure Information Protection content consumption by using work or school accounts from AIP policy-aware apps and services	✔	✔	✔
Protection for Exchange Online, SharePoint Online and OneDrive for Business content	✔	✔	✔
Bring Your Own Key (BYOK) for customer-managed provisioning life cycle[2]	✔	✔	✔
Custom templates, including departmental templates	✔	✔	✔
Protection for on-premises Exchange and SharePoint content via Rights Management connector	✔	✔	✔
AIP content creation by using work or school accounts	✔	✔	✔
Office 365 Message Encryption	✔	✔	✔
Administrative control[3]	✔	✔	✔
AIP SDK for protection for all platforms (Windows, Windows Mobile, iOS, macOS, Android)		✔	✔
Protection for non-Microsoft Office file formats, including PTXT, PJPG and PFILE (generic protection)		✔	✔
Manual, default and mandatory document classification		✔	✔
AIP scanner for content discovery of on-premises files matching any of the sensitive information types		✔	✔
AIP scanner to apply a label to all files in an on-premises file server or repository		✔	✔
Rights Management connector with on-premises Windows Server file shares by using the File Classification Infrastructure connector		✔	✔
Document tracking and revocation		✔	✔
Microsoft Information Protection SDK to apply labels/protection to emails and files for all platforms (Windows, iOS, macOS, Android, Linux)		✔	✔
Configure conditions for automatic and recommended classification			✔
Set labels to automatically apply preconfigured S/MIME protection in Outlook			✔
Control oversharing of information when using Outlook (warn, justify or block emails)			✔
Hold Your Own Key (HYOK) that spans AIP and Active Directory Rights Management for regulated scenarios			✔
AIP scanner for automated classification, labeling and protection of supported on-premises files			✔

Figura 10: Comparación de los planes de protección de la información de Azure.

6.3 Data Loss Prevention (DLP)

La seguridad de la información es un aspecto crítico para cualquier organización, especialmente cuando se trata de información sensible o confidencial. Garantizar la seguridad de los datos es esencial para proteger a la organización de las amenazas internas y externas que pueden poner en peligro la confidencialidad, integridad y disponibilidad de los datos.

La solución MVision de McAfee es una solución que puede ayudar a las organizaciones a proteger la información sensible y confidencial. Esta solución ofrece una serie de características y funcionalidades que pueden ayudar a garantizar la seguridad de los datos, como el control de accesos, el control de impresión, el control de copia y la prevención de fugas de información. MVision permite a los administradores de la organización establecer políticas de seguridad que ayudan a garantizar que la información sensible y confidencial se proteja adecuadamente.

Además de MVision, Microsoft también ofrece su propia solución DLP (Prevención de Pérdida de Datos) incluida dentro de la licencia F3 para Exchange Online. Esta solución ofrece capacidades básicas de DLP, pero para funcionalidades más avanzadas, como la protección a nivel de cliente o a nivel de Teams, es necesario hacer un upgrade a las licencias F5.

Para garantizar el cumplimiento de las directivas de protección vigentes, es necesario validar el correcto funcionamiento de la solución seleccionada. Esto implica llevar a cabo pruebas de seguridad, pruebas de penetración y revisiones regulares para asegurarse de que la solución está funcionando correctamente y se está protegiendo adecuadamente la información sensible y confidencial [22].

En resumen, es fundamental que las organizaciones establezcan medidas de seguridad y protección de datos para proteger la información sensible y confidencial de la organización. La solución MVision de McAfee y la solución DLP de Microsoft son dos soluciones que pueden ayudar a las organizaciones a cumplir con estas medidas de seguridad y protección de datos. Es importante realizar pruebas y revisiones regulares para garantizar que estas soluciones funcionen correctamente y protejan adecuadamente la información sensible y confidencial de la organización.

6.4 Antiphising

El phishing es una técnica de ingeniería social que se utiliza para engañar a los usuarios y obtener información personal y confidencial. Este tipo de ataque se lleva a cabo mediante el envío de correos electrónicos falsos que parecen provenir de fuentes legítimas, como bancos o empresas reconocidas. El objetivo es que los usuarios introduzcan sus datos personales o descarguen archivos maliciosos que permitan a los atacantes obtener información crítica o dañar los sistemas.

Para evitar casos de phishing, se crearán los registros correspondientes en los servidores DNS, para habilitar las funcionalidades:

Para combatir los ataques de phishing a todos los dominios federados al Tenant de Office 365, es necesario implementar medidas de seguridad adecuadas. Una de estas medidas es la implementación de registros MX, SPF, DKIM y DMARC en los servidores DNS.

MX

El registro MX (Mail Exchange) es un tipo de registro DNS que se utiliza para especificar los servidores de correo electrónico que están autorizados para recibir correos electrónicos enviados a un dominio específico.

En nuestro caso apuntaremos nuestros MX hacia los servidores de correo de entrada de CISCO CES.

SPF

El registro SPF (Sender Policy Framework) se utiliza para determinar qué servidores están autorizados para enviar correos electrónicos en nombre de un dominio. En el caso de Office 365, el registro SPF debe incluir el dominio de protección de Outlook para garantizar que solo se permita el envío de correos electrónicos desde Exchange Online.

v=spf1 “IP’s CISCO CES” mx exists ”Nombre del host” -all

Con esta configuración conseguimos que los servidores destinatarios de correos rechacen el correo, si no procede Exchange en línea.

DKIM

El registro DKIM (DomainKeys Identified Mail) se utiliza para asegurar que los correos electrónicos no sean falsificados durante el envío. Esta técnica utiliza una clave privada para cifrar la cabecera del correo electrónico en el servidor de correo saliente y la clave pública se publica como un registro DNS para que el destinatario pueda verificar la autenticidad del correo electrónico.

DMARC

El registro DMARC (Domain-based Message Authentication, Reporting and Conformance) se utiliza para validar que los correos electrónicos cumplan con los registros SPF y DKIM. DMARC permite que los destinatarios de los correos electrónicos identifiquen los correos electrónicos legítimos y los correos electrónicos falsificados que provienen de un dominio específico.

6.5 Retención

La retención de datos es un aspecto crítico en cualquier entorno de Office 365. La capacidad de retener y recuperar datos es esencial para garantizar el cumplimiento de las regulaciones y para proteger a la organización de posibles litigios y amenazas.

Cuando se trata de seleccionar la mejor opción de retención en un nuevo tenant de Office 365, existen varias opciones disponibles.

- La primera opción es la **Retención de Litigios**, que es una funcionalidad incorporada en Office 365. Esta funcionalidad permite a las organizaciones retener los datos electrónicos que son relevantes para un caso legal específico durante un período de tiempo determinado.

- La segunda opción es la **Retención de Datos**, que permite a las organizaciones retener los datos en Office 365 durante un período de tiempo determinado, independientemente de si se relacionan o no con un caso legal específico. La Retención de Datos se puede aplicar a todo el tenant o a grupos específicos de usuarios o ubicaciones.

- La tercera opción es la **Retención de eDiscovery**, que es una combinación de la Retención de Litigios y la Retención de Datos. Esta opción permite a las organizaciones retener los datos relevantes para un caso legal específico, así como los datos que deben ser retenidos por razones de cumplimiento o retención de información.

La selección de la mejor opción de retención en un nuevo tenant de Office 365 dependerá de las necesidades y regulaciones de la organización. Si la organización tiene requisitos específicos de cumplimiento o litigios, la Retención de Litigios puede ser la mejor opción.

Si la organización necesita retener los datos durante un período de tiempo determinado, independientemente de si se relacionan o no con un caso legal específico, la Retención de Datos puede ser la mejor opción. Si la organización necesita una combinación de ambas opciones, la Retención de eDiscovery puede ser la mejor opción.

Es importante tener en cuenta que la selección de la mejor opción de retención es solo el primer paso. Una vez que se ha seleccionado la opción de retención adecuada, es importante establecer políticas y procedimientos claros para garantizar que los datos se retengan adecuadamente y se recuperen cuando sea necesario. Además, se deben llevar a cabo pruebas y revisiones regulares para garantizar que la opción de retención seleccionada está funcionando correctamente y cumpliendo con los requisitos de la organización [23].

6.6 Backup

La necesidad de implementar una solución de backup efectiva en un entorno de Office 365 es crítica, ya que la copia de seguridad es una parte esencial de cualquier estrategia de recuperación de desastres y de protección de datos. Es importante tener en cuenta que, aunque Office 365 dispone de algunas funcionalidades de retención y gestión de versiones de archivos, estas no son suficientes para garantizar una protección completa de los datos.

En este caso, se menciona que no se han definido requerimientos de Backup específicos por parte de la empresa y que la plataforma de Office 365 no dispone de herramientas nativas de Backup. Por lo tanto, se hace necesario considerar soluciones de terceros para garantizar una protección adecuada de los datos.

Es importante tener en cuenta que la selección de una solución de backup adecuada dependerá de las necesidades específicas del Tenant. Las soluciones de backup varían en términos de características, funcionalidades, costos y complejidad. Por lo tanto, se debe llevar a cabo una evaluación cuidadosa de las diferentes soluciones disponibles en el mercado para seleccionar la que mejor se adapte a las necesidades del Tenant.

Una solución de respaldo efectiva es inadecuada por sí misma y debe complementarse con pruebas y revisiones periódicas para cumplir con los requisitos de protección de datos de la organización. Además de eso, los procedimientos y políticas para la recuperación de datos deben incorporarse en una estrategia integral de recuperación ante desastres para recuperar datos en caso de una interrupción o pérdida de datos.

Existen varias herramientas de terceros que ofrecen soluciones de backup para un tenant de Office 365. A continuación, se presentan tres herramientas que pueden ser consideradas:

- Veeam Backup: Esta herramienta ofrece una solución de backup y recuperación completa para los datos de Office 365, incluyendo Exchange Online, SharePoint Online y OneDrive for Business. Permite realizar copias de seguridad tanto en la nube como localmente, y ofrece funciones avanzadas como recuperación granular, búsqueda de correo electrónico y retención de datos a largo plazo [24].

- Acronis Backup: Esta herramienta proporciona una solución de backup y recuperación automatizada para los datos de Office 365, incluyendo Exchange Online, SharePoint Online y OneDrive for Business. Permite realizar copias de seguridad en la nube o localmente, y ofrece opciones de restauración flexibles, incluyendo restauración a nivel de archivo y de correo electrónico [25].

- AvePoint Cloud Backup: Esta herramienta ofrece una solución de backup y recuperación automatizada para los datos de Office 365, incluyendo Exchange Online, SharePoint Online y OneDrive for Business. Permite realizar copias de seguridad en la nube o localmente, y ofrece funciones avanzadas de recuperación

granular y de búsqueda de correo electrónico. También cuenta con herramientas de monitoreo y alerta para la gestión proactiva de la protección de datos [26].

Cabe destacar que estas son solo algunas opciones de herramientas de backup para Office 365, y se debe realizar una evaluación cuidadosa para seleccionar la que mejor se adapte a las necesidades específicas del tenant y a nivel económico cual la va mejor a la empresa.

6.7 MFA

La autenticación de doble factor (MFA) es una técnica de seguridad que proporciona una capa adicional de protección para los accesos a la plataforma de Office 365. En términos simples, significa que un usuario no solo necesitará su contraseña para iniciar sesión, sino también otro factor de autenticación, como una huella digital o un código de acceso enviado a su teléfono móvil.

La implementación de MFA es un paso importante para aumentar la seguridad de la plataforma y proteger la información confidencial de la empresa. Además, la combinación de MFA y políticas de acceso condicional permite una gestión más fina y segura de los accesos, ya que se pueden establecer criterios específicos para permitir o denegar el acceso a determinados recursos en función de diversos factores, como la ubicación, el dispositivo utilizado o la hora del día.

Es importante tener en cuenta que la solución de MFA de Microsoft solo se aplica a los recursos en la nube que utilizan Azure AD para la autenticación, como Office 365 y otros servicios en la nube de Microsoft. Si la empresa utiliza servicios On-Premises, como Exchange Server o SharePoint Server, será necesario utilizar otras soluciones de MFA específicas para estos servicios [27].

Por tanto, se recomienda que se establezca una política clara de registro de usuarios para el servicio de MFA y se generen tantas políticas de acceso condicionales como sea necesario para garantizar la seguridad y el cumplimiento de las políticas de la empresa. Además, se debe tener en cuenta que la implementación de MFA puede ser un proceso complejo y que es importante realizar una planificación adecuada y una formación a los usuarios para garantizar una implementación exitosa.

6.8 Self Service Password Reset

El servicio **Self Service Password Reset (SSPR)** es una herramienta muy útil para las empresas, ya que permite que los usuarios puedan reiniciar sus contraseñas de forma autónoma sin tener que recurrir al departamento de soporte técnico. Esto no solo reduce la carga de trabajo del personal de soporte, sino que también mejora la experiencia de usuario al hacer que el proceso de recuperación de contraseña sea más sencillo y rápido [28].

El SSPR de Azure AD ofrece la posibilidad de que los usuarios gestionen sus contraseñas tanto para los recursos en la nube como los recursos On-Premises. Además, con la integración con las políticas de acceso condicional, se pueden establecer requisitos adicionales de seguridad para restablecer la contraseña, como verificar la identidad del usuario mediante un mensaje de texto o una llamada telefónica.

Otra característica importante del SSPR es la opción de configurar una notificación de cambio de contraseña, que puede ser enviada al administrador del Tenant o a cualquier otra persona designada, para que esté al tanto de los cambios en las credenciales de los usuarios.

En cuanto a los costos, el servicio SSPR está incluido en la licencia E3 de Microsoft, por lo que no representa ningún costo adicional para la empresa. Sin embargo, es importante tener en cuenta que algunos servicios adicionales como el writeback de contraseñas sí pueden tener costos asociados, dependiendo de la licencia utilizada.

Es una herramienta muy útil y práctica para la gestión de contraseñas en una empresa, y su integración con las políticas de acceso condicional y otras funcionalidades de seguridad de Azure AD la convierten en una herramienta de gran valor para garantizar la seguridad de la plataforma de Office 365, por lo que se recomienda implementar dicha herramienta en este nuevo tenant.

6.9 Intune

Intune es una plataforma de gestión de dispositivos y aplicaciones móviles en la nube de Microsoft. Implementar Intune en un tenant puede tener varias ventajas, entre ellas [29]:

- **Gestión centralizada de dispositivos:** Al implementar Intune en un tenant, se puede centralizar la gestión de dispositivos móviles, lo que permite administrarlos de manera eficiente y segura. Esto incluye la posibilidad de aplicar políticas de seguridad, actualizar aplicaciones y sistemas operativos, y controlar el acceso a datos corporativos.

- **Integración con otras herramientas de Microsoft:** Intune se integra con otras herramientas de Microsoft, como Azure Active Directory, Office 365 y Power BI, lo que permite una gestión más eficiente y un flujo de trabajo más fluido. Esto puede mejorar la eficiencia y productividad de los equipos.

- **Seguridad mejorada:** Intune proporciona funciones de seguridad avanzadas, como la encriptación de datos y la protección contra amenazas móviles, lo que ayuda a garantizar la seguridad de los dispositivos móviles de la organización y los datos corporativos que contienen.

- **Configuración personalizada:** Intune permite configurar de manera personalizada las políticas y la gestión de dispositivos para adaptarse a las necesidades específicas de la organización.

La configuración de Intune puede incluir la creación de perfiles de configuración que permiten establecer políticas y configuraciones específicas para los dispositivos móviles, como la configuración de Wi-Fi y VPN, las restricciones de uso, la configuración de correos electrónicos y calendarios, entre otras. Además, se pueden definir políticas de cumplimiento que permiten asegurar que los dispositivos cumplan con los requisitos de seguridad y cumplimiento de la organización.

Implementar Intune en el tenant puede mejorar la eficiencia, seguridad y gestión de dispositivos móviles de la organización, y la configuración puede adaptarse para cumplir con las necesidades específicas de la organización.

7. Herramientas de colaboración

Dentro del licenciamiento de la solución encontraremos diferentes herramientas de colaboración que serán adoptadas por la organización, dentro de la organización se plantea en un principio la utilización de las siguientes herramientas dentro de la suite:

- Exchangue Online
- Teams
- Power BI

A continuación, se describe las características y configuraciones de este servicio según los requerimientos traslados por la empresa cuando se hablaron con ellos para que se nos presentara las necesidades de negocio.

7.1 Exchange Online

Uno de los motivos por los que se ha escogido el directorio de puesto de trabajo como fuente de identidades sé que no se encuentra vinculado con un Exchange, de este modo se posible construir un modelo de correo totalmente basado en la nube.

Con este planteamiento no se generan dependencias con el esquema de Exchange ni será necesario mantener una consola de Exchange On-Premises para gestionar los atributos específicos de Exchange sobre el Active Directory. De este modo se reduce la necesidad de infraestructura, así como la carga administrativa asociada a la gestión de la propia infraestructura como la gestión de los atributos adicionales.

El servicio de Exchange ofrece una capa de seguridad llamada Exchange en línea Protection (EOP), un servicio que se encuentra disponible con independencia del licenciamiento utilizado que permite filtrar:

- SPAM
- Malware
- Pishing
- Otras amenazas a trabas de correo electrónico

Adicionalmente, se plantea mantener la solución corporativa ya implementada anteriormente en Exchange 2016, por lo tanto, se utilizará la herramienta Cisco IronPorts como analizador del flujo de correo.

7.1.1 Buzones

- **Buzones Principales:** Se utilizará el UPN del AD. Actualmente se utiliza un formato que se basara con la primera letra del nombre y seguidamente el apellido ejemplo: (jsanchez@pagostini.com)

  Existe una dependencia directa entre el UserName y el buzón que se genera por el que la creación de los usuarios a la nube tendrá que cumplir la regla que se defina para el buzón. Este buzón se la que tendrá la licencia asignada y será la cuenta con el que se colaborará.

- **Buzones Departamentales:** Buzones compartidos, dirigidos a uso de grupos o buzones genéricos se dejará que el manager que solicite la alta de dicho buzón compartido pueda elegir el formato.

  El buzón principal tendrá acceso completo sobre el buzón secundaría (Departamental) pudiendo haceros indiferente de los dos buzones, según sea necesario, pudiendo pasar de buzón compartido (SharedMailbox) a buzón genérico que se tendrá que acceder con dirección de correo y contraseña asociado a ese buzón

7.2 Teams

Se contempla también la utilización de Teams como herramienta de colaboración [30].

Teams es una poderosa herramienta de colaboración y comunicación dentro de Microsoft 365. Aquí adjunto una explicación más detallada de algunos aspectos relevantes de Teams:

- **Creación de equipos y canales:** En Teams, se puede crear equipos para organizar y agrupar a los miembros de la empresa. Dentro de cada equipo, se puede crear canales temáticos para organizar las conversaciones y los archivos relacionados con aspectos específicos de cada área o zona de la empresa.

- **Conversaciones y chat**: Se permite tener conversaciones tanto a nivel de equipo como a nivel de canal, donde se puede iniciar conversaciones en un canal específico para discutir temas relacionados con ese canal en particular. Además, puedes chatear de forma individual o en grupos con otros miembros del equipo.

- **Compartir archivos**: Se puede compartir archivos de manera rápida y sencilla. Se puede cargar documentos, presentaciones, hojas de cálculo u otros archivos relevantes en los canales correspondientes para que los miembros del equipo

puedan acceder, colaborar y revisarlos hi a la vez se guarda en el Sharepoint una copia de dichos documentos.

- Reuniones y videoconferencias: Ofrece una función de videoconferencia que permite llevar a cabo reuniones virtuales con los compañeros de equipo, supervisores o incluso realizar presentaciones. Puedes programar reuniones, invitar a participantes externos y compartir pantallas para realizar presentaciones.

- Colaboración en tiempo real: Teams permite la colaboración en tiempo real en documentos compartidos, donde se puede crear y editar documentos de Word, Excel y PowerPoint directamente en Teams, lo que facilita el trabajo colaborativo y la sincronización de cambios entre los miembros del equipo.

- Integraciones y aplicaciones: Se ofrece una amplia gama de integraciones y aplicaciones de terceros que puedes utilizar para mejorar la productividad y personalizar tu experiencia. Por ejemplo, se puede integrar herramientas de gestión de proyectos, servicios de almacenamiento en la nube, o incluso bots de productividad que automatizan tareas repetitivas.

- Notificaciones y actualizaciones: Se puede recibir notificaciones sobre nuevos mensajes, menciones en conversaciones, cambios en archivos compartidos, etc. Lo que permite estar al tanto de las últimas novedades y participar de manera activa en el proyecto.

- Acceso desde múltiples dispositivos: Se puede acceder a dicha herramienta desde tu ordenador, tablet o teléfono móvil, lo que te brinda flexibilidad para trabajar cualquier lugar. La sincronización entre dispositivos asegura que siempre tengas acceso a la información y conversaciones más recientes.

7.3 Power BI

Power BI es una plataforma de análisis y visualización de datos que permite a las organizaciones transformar sus datos en información útil para la toma de decisiones. Implementar Power BI en un tenant, es decir, en un entorno de trabajo compartido en la nube de Microsoft, puede tener varias ventajas [31]:

- Centralización de datos: Al implementar Power BI en un tenant, se puede centralizar el acceso y la gestión de los datos de la organización, lo que facilita la colaboración y reduce la duplicación de esfuerzos. Además, esto permite mantener un control más riguroso sobre la seguridad de los datos, ya que se pueden establecer permisos y restricciones de acceso a nivel de usuario.

- Integración con otras herramientas de Microsoft: Power BI se integra con otras herramientas de Microsoft, como Excel, SharePoint, Teams, Dynamics 365, entre otras, lo que permite un flujo de trabajo más fluido y sin interrupciones. Esto también puede mejorar la eficiencia y productividad de los equipos.

- Visualización de datos en tiempo real: Power BI permite conectar con una amplia variedad de fuentes de datos, incluyendo bases de datos en la nube y on-premise, archivos locales, servicios web, entre otros. Esto permite visualizar los datos en tiempo real y tomar decisiones más rápidas y precisas.

- Personalización y automatización: Power BI permite la personalización de los informes y paneles de control, así como la automatización de tareas repetitivas a través de la creación de flujos de trabajo. Esto puede mejorar la eficiencia y la calidad de los análisis realizados.

Implementar Power BI en el tenant puede mejorar la colaboración, la eficiencia, la seguridad y la calidad de los análisis realizados por la organización.

8. Flujo de correo

La incorporación del producto CES de Cisco como la primera capa de seguridad en la red de Planeta de Agostini, brindará una protección adicional contra las amenazas cibernéticas. Esta herramienta de seguridad avanzada funciona mediante el análisis de los correos electrónicos entrantes y salientes para detectar posibles amenazas y proteger la red de la organización.

Al agregar esta capa de seguridad donde se establecerá una barrera más sólida contra las amenazas cibernéticas, se podrá llegar a detectar y bloquear automáticamente los correos electrónicos maliciosos, los ataques de phishing y los virus, lo que permitirá a los empleados de la propia empresa trabajar sin preocupaciones y mantener sus datos seguros.

Además, al elegir utilizar CES, se agregaría una segunda capa de seguridad en la que se pueden establecer políticas personalizadas de seguridad para adaptarse a las necesidades específicas de la organización, donde permitiría a la organización tener un mayor control sobre la seguridad de su red y asegurar que se cumplan los requisitos regulatorios.

Permitiría a la organización, detectar rápidamente y resolver problemas de seguridad en tiempo real. El producto cuenta con herramientas de monitoreo y alertas que permiten a los administradores de la red detectando y respondiendo a las amenazas de manera oportuna.

Finalmente, al configurar EOP para que solamente acepte correos electrónicos de CES, se reducirá significativamente el riesgo de que se entreguen correos electrónicos maliciosos o no deseados a la red de la organización. Esto es porque se restringe el acceso a la red solo a los correos electrónicos que se han verificado previamente a través de la propia herramienta de CISCO, lo que reduce el riesgo de que se entreguen correos electrónicos no deseados o maliciosos a la red.

La adopción de dicha herramienta como la primera capa de seguridad y la configuración adecuada de EOP permitirán tener una estrategia sólida y efectiva de seguridad cibernética, lo que les permitirá centrarse en su trabajo sin tener que preocuparse constantemente por las amenazas de seguridad.

El flujo sería el siguiente:

Figura 11: Flujo de correo

9. Plan de gestión del cambio

9.1 Alcance

El alcance general del proyecto en cuanto a la Gestión del Cambio consistirá en ajustar la estrategia, planificar y ejecutar todas las acciones de acompañamiento al usuario relacionadas con la migración al nuevo Tenant, así como la adopción de las nuevas herramientas colaborativas de Microsoft 365.

- Alcance temporal: se prevé la realización de tareas de Gestión del Cambio a lo largo de 6 meses.

- Alcance organizativo: toda la organización. El número estimado de usuarios impactados es de aproximadamente 7.818.

- Alcance funcional: se trabajará sobre las afectaciones funcionales al usuario derivadas de la migración de datos a la plataforma Microsoft 365, y la adopción de las nuevas herramientas de la plataforma.

9.2 Visión general

Para llevar a cabo una gestión del cambio exitosa, es necesario contar con un plan adecuado que contemple todas las actividades necesarias para lograr el objetivo final. En el caso de Planeta de Agostini, se ha identificado que el nivel de complejidad del cambio puede ser medio o alto, lo que implica la necesidad de un enfoque integral y coordinado para abordar todos los aspectos relevantes.

En este contexto, se ha elaborado una propuesta de Plan de Gestión del Cambio de nivel medio-alto, que se compone de 5 bloques de actividades interconectadas y

complementarias entre sí. Cada uno de estos bloques se enfoca en una etapa específica del proceso de cambio, desde la evaluación inicial hasta la consolidación del cambio.

Figura 12: Plan de gestión del cambio.

9.3 Descripción de actividades

A continuación, se muestra un resumen general de las principales actividades que se llevarían a cabo en cada uno de los bloques (descritas en el siguiente apartado):

Evaluación inicial y definición de	Planificación del cambio	Implementación del cambio	Comunicación y formación	Consolidación del cambio
•Análisis de los procesos actuales y evaluación de su eficacia. •Identificación de las necesidades de cambio. •Definición de los objetivos a alcanzar.	•Definición de estrategias y tácticas para lograr los objetivos definidos en el bloque anterior. •Diseño de un plan detallado para implementar el cambio. •Establecimiento de un calendario de implementación del cambio.	•Ejecución del plan de implementación del cambio. •Supervisión del progreso y evaluación del impacto del cambio. •Identificación y resolución de problemas o desviaciones.	•Comunicación interna y externa sobre el proceso de cambio. •Definición de planes de formación y capacitación para el personal afectado. •Implementación de actividades de formación y capacitación.	•Supervisión y evaluación del impacto del cambio a largo plazo. •Identificación de posibles mejoras y ajustes. •Integración del cambio en la cultura organizacional de la empresa.

Tabla 5: Descripción de actividades.

El proceso de cambio en cualquier organización es una tarea compleja que requiere una planificación cuidadosa y una estrategia adecuada para garantizar que se lleve a cabo de manera efectiva. En el caso de Planeta de Agostini, se espera que la implementación del nuevo servicio de correo requiera un Plan de Gestión del Cambio de nivel medio-alto, por lo que significa que se necesitará una estrategia integral y estructurada para abordar el proceso de cambio de manera eficiente.

Para asegurar que la implementación del nuevo servicio de correo se lleve a cabo sin problemas, se han propuesto diferentes bloques de actividades que se trabajarán de manera conjunta para aportar a la empresa la facilitación del cambio deseado, por lo que cada uno de estos bloques de actividades tiene un propósito específico y están diseñados para abordar diferentes aspectos del cambio.

Por lo que la implementación del nuevo servicio de correo requerirá una adaptación significativa de los procesos y las prácticas actuales, por lo que es crucial tener un enfoque integral y estructurado para abordar el proceso de cambio. La gestión adecuada del cambio garantizará que el proceso de implementación sea lo más fluido posible y que el nuevo servicio de correo se integre adecuadamente en la organización.

10. Migración de usuarios

10.1 Herramientas de migración

La herramienta de migración que se utilizará en dicha migración será Quest On Demanad Migration es una opción valiosa para proyectos de implementación de tenant debido a varias razones:

- Capacidad de migrar datos: Una de las principales ventajas de la herramienta de migración es su capacidad para migrar grandes cantidades de datos de manera rápida y eficiente. Esto es particularmente útil en proyectos de implementación de tenant, donde se necesita transferir grandes cantidades de datos de un sistema a otro.

- Flexibilidad: La herramienta de migración es muy flexible y puede utilizarse para migrar datos entre diferentes plataformas y sistemas, lo que la hace ideal para proyectos de implementación de tenant que implican la transferencia de datos entre sistemas heterogéneos.

- Automatización: Es capaz de automatizar muchas tareas relacionadas con la migración de datos, lo que reduce significativamente el tiempo y el costo involucrado en el proceso de migración.

- Pruebas y validación: Incluye funciones de prueba y validación que permiten verificar la integridad y precisión de los datos migrados, lo que ayuda a reducir el riesgo de errores y problemas en la implementación del tenant.

- Soporte y documentación: Cuenta con un equipo de soporte dedicado y una amplia documentación disponible en línea, lo que facilita la resolución de problemas y la comprensión de su uso.

Dicha herramienta, es una excelente opción para realizar este proyecto de implementación del tenant debido a su capacidad para migrar grandes cantidades de datos de manera rápida y eficiente, su flexibilidad para trabajar con diferentes sistemas

y plataformas, su capacidad de automatización, sus funciones de prueba y validación, y el soporte y documentación disponibles.

10.2 Cronograma

En el contexto del proyecto de implementación, se ha incluido una propuesta de cronograma de alto nivel con el objetivo de estimar la duración del mismo. Esta planificación ha sido expresada en meses, con el propósito de facilitar una visión clara y general del tiempo que se espera que lleve cada fase del proyecto.

Es importante destacar que esta propuesta de cronograma de alto nivel es solo una estimación preliminar y, por lo tanto, debe ser refinada y ajustada a medida que avanza el proyecto.

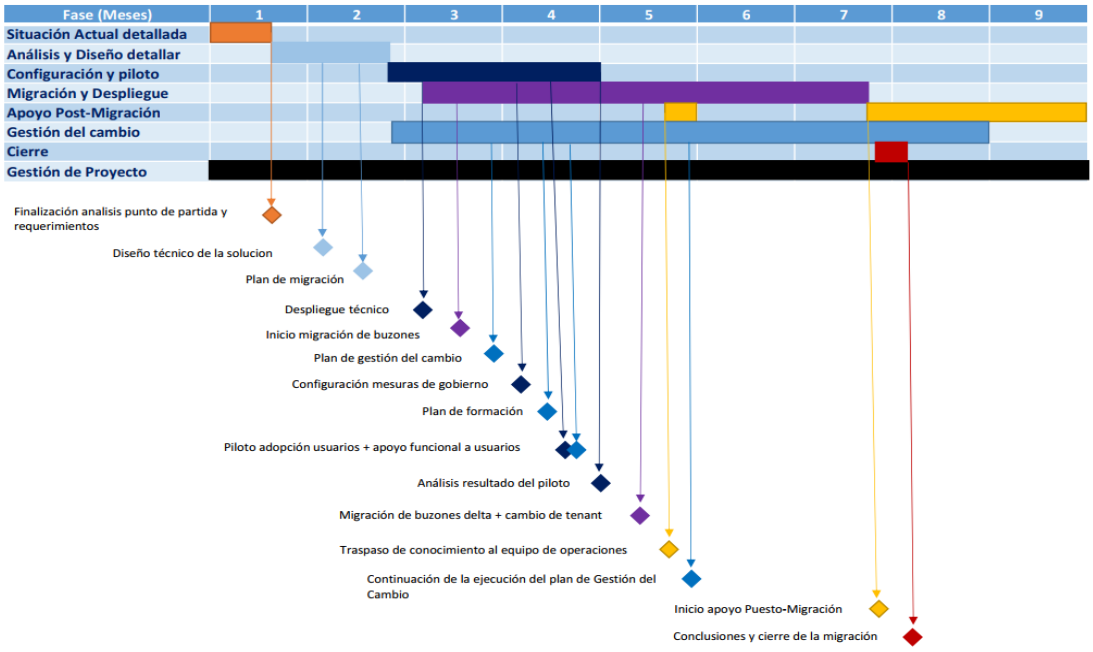

Figura 13: Cronograma proyecto de implementación

10.3 Planificación

La migración de los usuarios a una nueva plataforma puede ser una tarea crítica y compleja en cualquier proyecto de tecnología de la información. En el caso de la implementación del nuevo servicio de correo en Planeta de Agostini, la migración de los usuarios es una de las tareas más importantes y críticas en el proyecto. Cualquier interrupción en los servicios podría generar inconvenientes significativos para los usuarios, lo que podría afectar la satisfacción del cliente y la imagen de la organización.

Por esta razón, se ha tomado en cuenta cuidadosamente la migración de los usuarios en la planificación del proyecto, donde se ha desarrollado un esquema detallado de las actividades necesarias para completar con éxito el proceso de migración. Este esquema incluye los pasos necesarios para transferir los datos y sincronizar la información,

configurar los usuarios en la nueva plataforma, realizar pruebas y llevar a cabo la implementación final del proceso de migración.

La planificación cuidadosa de la migración de los usuarios ayudará a minimizar el tiempo de inactividad y a garantizar la continuidad de los servicios para los usuarios durante el proceso de migración. Además, se ha diseñado un plan de contingencia para hacer frente a cualquier problema o interrupción que pueda ocurrir durante la migración.

La implementación de este esquema será supervisada y monitoreada cuidadosamente para garantizar que el proceso de migración se lleve a cabo de manera efectiva y eficiente.

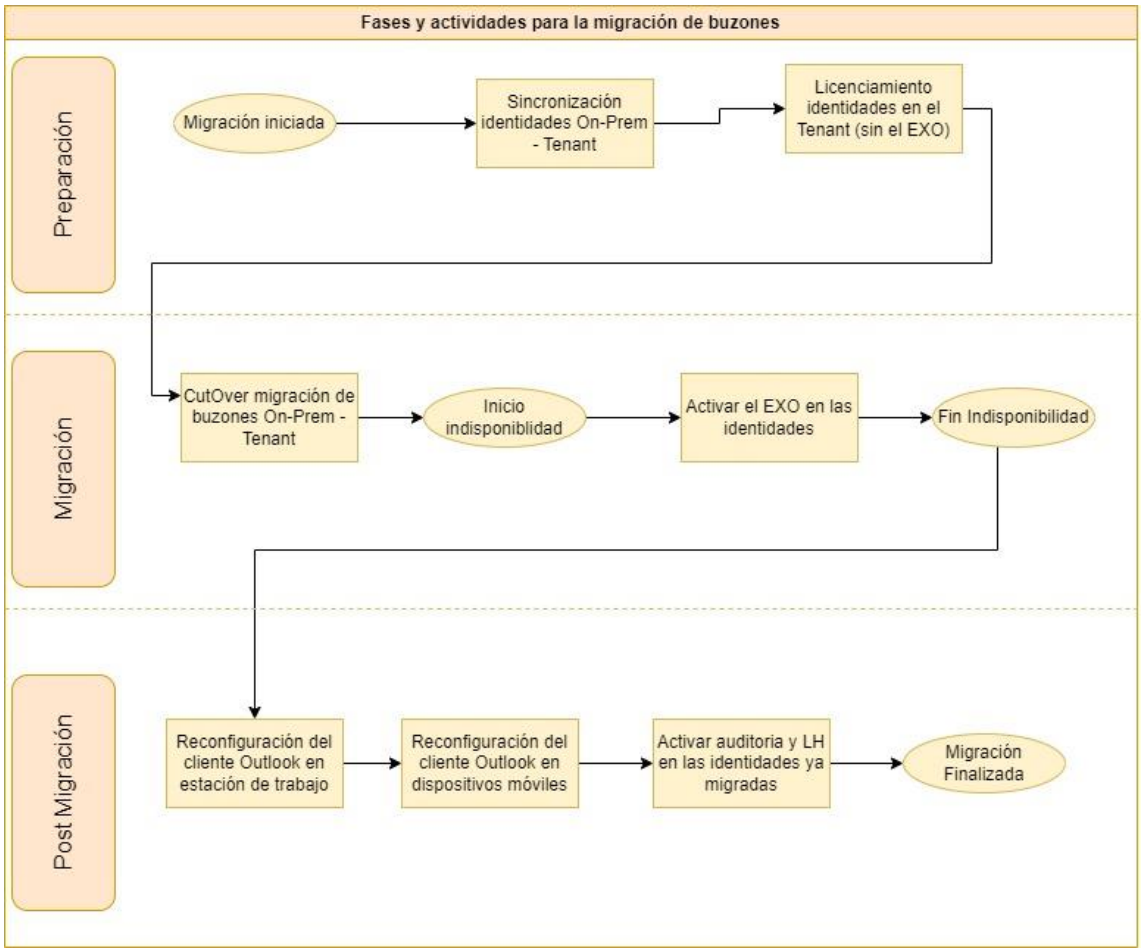

Figura 14: Planificación migración

11. Valoración productiva y presupuestaria

Para lograr los objetivos relacionados con el futuro proyecto de implementación del nuevo Tenant, estimamos que será necesaria la participación de los siguientes perfiles técnicos dentro de la empresa externa que se contratará para realizar la implementación/migración/gestión del cambio:

- Jefe de proyecto Externo: responsable de coordinar las acciones técnicas que se llevarán a cabo, así como de proporcionar los medios necesarios para la realización de las tareas requeridas. Participaría en el proyecto al 50%.

- Consultor Senior M365: especializado en MS365 y Azure. Responsable de las tareas de análisis, diseño y planificación de piloto y despliegue. También supervisaría y coordinaría los trabajos técnicos del despliegue. Participaría en el proyecto al 70%.

- Arquitecto M365: especializado en MS365 y Azure. Responsable de los trabajos de despliegue técnico y migración. También daría soporte técnico durante las fases de piloto y despliegue. Participaría en el proyecto al 80%.

- Técnico M365: especializado en MS365 y Azure. Encargado de la ejecución de los trabajos de despliegue técnico y migración. También daría soporte técnico durante las fases de piloto y despliegue.

- Consultor Senior de Gestión del cambio: será el encargado de la definición del plan de comunicación, estrategia de uso de las nuevas herramientas de trabajo y la documentación formativa a elaborar y diseñar el plan de formación. También (informes de seguimiento y cualquier otro requerimiento que surja a lo largo del proyecto).

- Consultor de Gestión del cambio: será el encargado de ejecutar el Plan de Comunicación y el Plan de Formación, así como colaborar en la definición de la estrategia de uso de las nuevas herramientas de trabajo y en elaborar la documentación formativa a elaborar.

- Consultor de Gestión del cambio especialista en Soporte al usuario – Global Assistant: encargado de resolver las dudas funcionales que surjan durante el despliegue dando soporte, tanto a los usuarios finales.

- Técnico de soporte O365: será el encargado de la resolución de incidencias técnicas post migración durante el período de tiempo que se establezca. Participará en el proyecto con una dedicación del 100% a partir del inicio de la primera Ola de migración (Ola Piloto), por lo que si hiciéramos el porcentaje global que tendría en el proyecto des del inicio hasta el fin seria de un 25%.

Por la parte interna se buscará involucrar los siguientes perfiles:

- Jefe de proyecto Interno: responsable de coordinar las acciones técnicas que se llevarán a cabo, así como de proporcionar los medios necesarios para la realización de las tareas requeridas.

- Técnico de sistemas: será por parte de la empresa el encargado de estar con el técnico de soporte y técnico M365 para poder ir aprendiendo y realizado el apoyo para ir asumiendo el mantenimiento completo del servicio de este nuevo tenant. Participará en el proyecto con una dedicación del 100% a partir del inicio de la primera Ola de migración (Ola Piloto), por lo que si hiciéramos el porcentaje global que tendría en el proyecto des del inicio hasta el fin seria de un 25%.

- Analista de Sistema: será por parte de la empresa el encargado de estar con el arquitecto O365 para poder ir aprendiendo y realizado el apoyo para ir asumiendo el mantenimiento completo del servicio de este nuevo tenant con la infraestructura generado de ADCONECT y todos sus servicios que involucran fuera de gestionar buzones, listas de distribución, salas, etc.

La siguiente tabla muestra los costes de los recursos internos:

Rol	Participa-ción	Horas	€/Hora	Coste Total
Jefe de Proyecto Interno	50%	720h	60€	43.200€
Técnico de sistemas	25%	360h	15€	5.400€
Analista de Sistema	80%	1152h	50€	57.600€

Tabla 6: Recursos Internos

La siguiente tabla muestra los costes de los recursos externos:

Rol	Participa-ción	Horas	€/Hora	Coste Total
Jefe de Proyecto Externo	50%	720h	60€	43.200€
Consultor Senior M365	70%	1008h	80€	80.640€
Arquitecto M365	80%	1152h	60€	69.120€
Técnico M365	65%	936h	30€	28.080€
Consultor Senior Gestión del cam-bio	50%	720h	50€	36.000€
Global Assistant	35%	504h	30€	15.120€
Técnico de soporte O365	25%	360h	15€	5.400€

Tabla 7: Recursos Externos

En la siguiente imagen, se podrá visualizar el coste total que tendría cada uno de los empleados que participarían en el proyecto, contando la participación que tendrá en el proyecto y el coste/hora que se tiene para cada uno de los roles definidos.

Como se puede observar en la gráfica se ha dividido en color azul el personal interno y en color rojo el personal externo para que se puede diferencia correctamente.

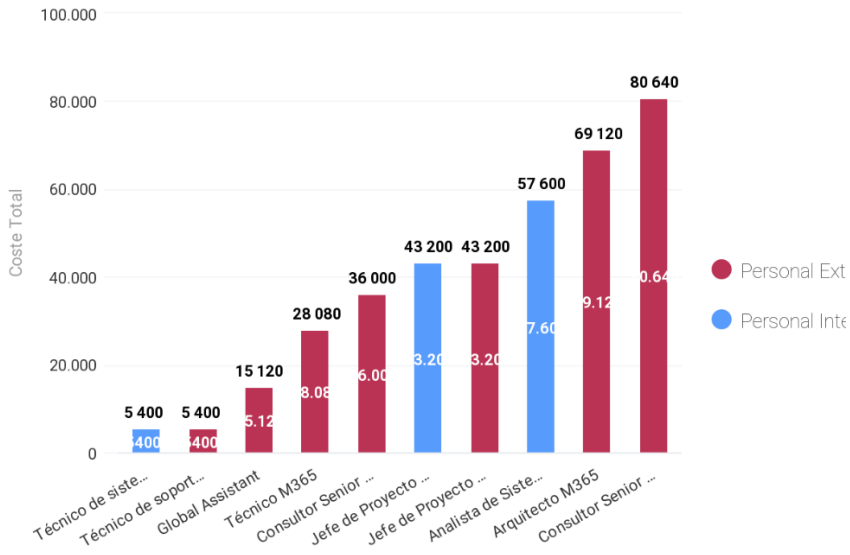

Figura 15: Coste total personal

Por lo tanto, el coste total del personal que trabajará dentro de este proyecto de implementación de tenant será el total de 383.760€ y luego a dicho coste se tendría que sumar el coste que tendría las licencias de Quest que en este caso no se puede calcular, ya que el precio de cada licencia se tiene que negociar con la propia compañía que lo suministra.

Seguidamente la parte de La infraestructura/Microsoft/CISCO lo hemos calculado a través de 3 tablas que se muestra a continuación, pero es el coste anual que tendría mantener dicho tenant:

Infraestructura, son todos aquellos servidores necesarios para poder implementar el tenant ya sea para el tema de Directorio Activo, ADCONECT, etc.

	Cantidad	Precio	Coste Total
Servidores Windows Server	3	600€	1.800€

Tabla 8: Infraestructura – Servidores

Por la parte de Microsoft:

	Cantidad	Precio	Coste Total
Licencias	7818	15€	117.720€
Licencia Tenant - Microsoft 365 E3	7818	25€	2.345.400€

Tabla 9: Infraestructura – Microsoft

**Quiero comentar que las licencias se la ha puesto un coste de 15€ ya que es el precio promedio, luego ese dato variaría según las licencias que se necesiten para cada usuario como se ha visto en la tabla del apartado 3.1 licenciamiento.*

*También remarcar que los 2.345.400€ salen de calcular 7818*25= 195.450€ y como este tipo de licencia se cobra por usuario/mes, por lo que hay que multiplicar ese resultado que hemos obtenido por los 12 meses del año y de ahí te sale el coste total de la tabla*

Y por último la parte de la infraestructura CES

	Cantidad	Precio	Coste Total
Licencias CES	1	100.000€	100.000€
Hardware CES	1	50.000€	50.000€
Mantenimiento y Soporte Anuales CES	1	25.000€	25.000€

Tabla 10: Infraestructura – CISCO CES

Por lo que el coste total anual de mantener dicha implementación es de 2.639.920€

12. Conclusión

Este trabajo de fin de grado presenta una guía para identificar y definir los conceptos más relevantes en un proyecto de migración a la nube, basándose en la consulta de información de Microsoft y la experiencia profesional del autor. Una de las conclusiones aprendidas es que la implantación de un tenant de 0 no solo implica su generación, sino también su configuración según las necesidades del cliente y las normativas de seguridad definidas por el CCN para garantizar la seguridad de la información.

La investigación realizada ha permitido adquirir conocimientos sobre la nube, sus servicios y su funcionamiento básico, accesibles a través de la documentación publicada en internet por el proveedor y los cursos gratuitos en línea.

El trabajo se ha divido en 4 fases, las 3 primeras corresponde a la entrega de PEC y la 4 es la Entrega final de dicho proyecto. Se creo una planificación bastante detallada y no se ha producido desviaciones significativas, donde el plan se creo tiene en cuenta la disponibilidad real para poder afrontar el trabajo y se ha podido seguir sin grandes dificultades.

La metodología de mejora continua es la que se ha seguido durante la realización del trabajo. Se ha utilizado la retroalimentación del profesor para modificar y actualizar las secciones del trabajo, por lo que el contenido de las primeras secciones no estaba del todo correcto y se tuvo que ir adaptando según las correcciones que se iban viendo. En general, se ha seguido la estructura de secciones descrita al principio del trabajo.

Se han identificado posibles líneas de trabajo futuro que podrían ser consideradas para mejorar el proceso de migración a la nube.

- En primer lugar, se propone incluir un nuevo caso de negocio en la fase de preparación con costes más detallados para confirmar la viabilidad del proyecto.

Esto permitiría tener una visión más precisa de los recursos y presupuesto necesarios para llevar a cabo el proyecto.

- Otra línea de trabajo clave sería definir un plan de formación para los equipos de operaciones en tecnología cloud. Se deben identificar los cursos necesarios y comenzar con la formación de los equipos internos, ya que esto es un proceso que requiere tiempo y preparación adecuada. De esta forma, los equipos estarán mejor preparados para afrontar los nuevos desafíos y tomar las decisiones adecuadas.

- Finalmente, se sugiere revisar y actualizar el organigrama de TI de la empresa para para adaptarlo a los nuevos modelos de operaciones en la nube. Esto podría implicar cambios en la estructura y roles de los departamentos de la organización para garantizar una gestión eficiente y alineada con las nuevas tecnologías y modelos de operaciones.

A pesar de haber alcanzado el objetivo inicial del proyecto, se reconoce que esto es solo el punto de partida para un camino de migración a la nube y que es necesario seguir trabajando y mejorando en estas áreas clave para garantizar el éxito en el proceso de migración.

En conclusión, este trabajo es un documento de referencia para la preparación de un proyecto de implementación de un nuevo tenant, con las configuraciones más importantes que interesan al cliente, incluyendo un plan de gestión del cambio y migración de usuarios.

13. Glosario

- Ironport: Es una marca de productos de seguridad informática, principalmente en el área de correo electrónico. Los productos IronPort son utilizados para proteger a las empresas y organizaciones contra amenazas como spam, virus y phishing en sus sistemas de correo electrónico.
- Tenant: Se refiere a un inquilino de Microsoft 365, es decir, una entidad que ha adquirido una suscripción a Microsoft 365 y ha creado un espacio de trabajo en la nube para sus usuarios y recursos.
- Saas: Se refiere a un modelo de entrega de software en el que el proveedor de servicios aloja la aplicación en la nube y la distribuye a través de internet a los usuarios que pagan una suscripción periódica.
- Cloud: Se refiere a la nube informática, que es un modelo de entrega de servicios y recursos informáticos a través de internet
- Conditional Acces: Se refiere a una función de seguridad en los sistemas informáticos que permite restringir el acceso a recursos o datos según ciertos criterios o condiciones predefinidas
- Azure Active Directory: Es un servicio de gestión de identidades y accesos en la nube ofrecido por Microsoft.
- Multifactor Authetificator: Es un método de seguridad que requiere que el usuario proporcione más de un factor de autenticación para verificar su identidad antes de acceder a un recurso protegido
- API: Se trata de un conjunto de protocolos, herramientas y estándares que permiten a los desarrolladores de software construir y comunicarse con otras aplicaciones y servicios de software.
- Microsoft: Microsoft es una empresa multinacional de tecnología fundada en 1975 por Bill Gates y Paul Allen. Con sede en Redmond, Washington, Microsoft es conocida por sus productos de software, incluyendo el sistema operativo Windows, la suite de productividad Microsoft Office, el navegador web Microsoft Edge y la plataforma de juegos Xbox.
- Active Directory: Es un servicio de directorio de servicios de Microsoft que se utiliza para almacenar información de identidad y acceso de los usuarios y recursos de una organización
- Azure AD Connect: Es una herramienta de sincronización de identidades que permite a las organizaciones integrar sus entornos de Active Directory local con Azure Active Directory (AD) en la nube de Microsoft.
- Pasthorugh Authetifcation: Es un método de autenticación que permite a los usuarios acceder a recursos de red y servicios en línea utilizando las credenciales de inicio de sesión de su entorno local sin tener que introducir sus credenciales nuevamente
- Password Hash Sync: Es un método de sincronización de contraseñas que se utiliza con Azure Active Directory (AD). Con Password Hash Sync, las contraseñas de los usuarios se sincronizan de forma segura desde el entorno local de Active Directory a Azure AD, lo que permite a los usuarios utilizar sus credenciales de inicio de sesión locales para acceder a servicios y recursos en línea.

- Forest: Es una estructura lógica que representa una colección de dominios de Active Directory que comparten una relación de confianza común
- DNS: Se refiere a un sistema utilizado para traducir nombres de dominio en direcciones IP numéricas que se utilizan para identificar dispositivos y servicios en Internet
- Kerberos: Es un protocolo de autenticación de red utilizado para verificar la identidad de los usuarios y garantizar la seguridad de la comunicación en entornos de red
- MS-RPC: Es un protocolo de comunicación utilizado por sistemas operativos Windows para permitir que los procesos en diferentes sistemas se comuniquen entre sí a través de una red.
- LDAP: Es un protocolo de acceso a directorios utilizado para acceder y gestionar información de directorios en una red
- SMB: Es un protocolo de red utilizado por sistemas operativos Windows para compartir archivos, impresoras y otros recursos en una red.
- LDAPSSL: También conocido como LDAPS, es una variante del protocolo LDAP que utiliza SSL/TLS para cifrar y asegurar las comunicaciones entre clientes y servidores LDAP
- RPC: Es un protocolo de comunicación utilizado por los sistemas operativos y aplicaciones para permitir que los procesos en diferentes sistemas se comuniquen entre sí a través de una red
- WinRM: Es un protocolo de administración remota utilizado por los sistemas operativos Windows para permitir la administración remota de servidores y estaciones de trabajo.
- AD DS Web Services: Es un componente de Active Directory que permite la interoperabilidad de servicios de directorio a través de protocolos web estándar, como Simple Object Access Protocol (SOAP) y Web Services Description Language (WSDL)
- Global Catalog: Es un componente de Active Directory que contiene una copia parcial de los atributos de todos los objetos de directorio en un bosque de Active Directory.
- HTTP: Es un protocolo de comunicación utilizado para la transferencia de datos en la World Wide Web.
- HTTPS: Es una variante segura del protocolo HTTP utilizado para la transmisión segura de datos en la World Wide Web
- TCP: Es un protocolo de comunicación utilizado para la transmisión confiable de datos a través de redes de computadoras.
- UDP: Es un protocolo de comunicación utilizado para la transmisión confiable de datos a través de redes de computadoras.
- Seamless SSO: Es una característica de Azure Active Directory (AAD) que permite a los usuarios autenticarse automáticamente en aplicaciones y servicios en línea de Microsoft sin tener que ingresar manualmente sus credenciales.
- On-Premises: Se refiere a la infraestructura tecnológica y los servicios que se ejecutan en el sitio en una organización, en lugar de ser alojados y gestionados en la nube o por un proveedor de servicios externo.

- UPN: Significa User Principal Name (Nombre Principal del Usuario) y se utiliza en los sistemas de identidad y autenticación, como Active Directory, para identificar de forma única a un usuario.
- SAML: Es un estándar abierto para el intercambio de información de autenticación y autorización entre diferentes sistemas y aplicaciones.
- SSL: Es un protocolo de seguridad que proporciona una conexión segura y cifrada entre un servidor y un cliente
- TLS: Es un protocolo de seguridad que se utiliza para proporcionar una conexión segura y cifrada entre dos aplicaciones de red.
- GPDR: Es una ley de privacidad de datos de la Unión Europea que entró en vigor el 25 de mayo de 2018. El objetivo principal del GDPR es proteger los datos personales de los ciudadanos de la UE y regular la forma en que las organizaciones tratan, almacenan y protegen esos datos.
- SealPath: Es una plataforma de seguridad de datos que proporciona soluciones de protección de información para empresas y organizaciones de diversos sectores. Permite a los usuarios controlar y proteger el flujo de información confidencial dentro y fuera de la empresa.
- Azure Information Protection: Es una solución de clasificación y protección de datos de Microsoft que ayuda a las empresas a proteger su información confidencial y cumplir con los requisitos de cumplimiento normativo.
- Upgrade: Se refiere al proceso de actualizar o mejorar un sistema, aplicación o hardware a una versión más reciente o avanzada. La actualización puede incluir nuevas funciones, correcciones de errores, mejoras de seguridad y mejoras de rendimiento.
- eDiscovery: Es el proceso de descubrir, identificar y recuperar información electrónica relevante para una investigación legal, un litigio o una auditoría
- DMARC: Es una tecnología de autenticación de correo electrónico que ayuda a reducir el riesgo de fraude por correo electrónico, como el phishing y el spoofing
- DKIM: Es un protocolo de autenticación de correo electrónico que ayuda a verificar la autenticidad del remitente y la integridad del mensaje.
- SPF: Es un protocolo de autenticación de correo electrónico que ayuda a verificar la autenticidad del remitente de un mensaje de correo electrónico
- EOP: Es un servicio de protección de correo electrónico basado en la nube que se utiliza para proteger los buzones de correo electrónico de los usuarios de Microsoft Exchange Online y otros servicios de correo electrónico en la nube de Microsoft, como Microsoft 365 y Office 365.
- SPAM: Se refiere a mensajes de correo electrónico no solicitados y no deseados, que a menudo contienen publicidad, estafas, malware o phishing.
- Pishing: Es una técnica utilizada por los ciberdelincuentes para engañar a los usuarios y obtener información confidencial, como contraseñas, información financiera o datos personales.
- Quest On Demand Migration: es una herramienta de migración en línea de la empresa Quest Software que permite a las organizaciones migrar sus datos de correo electrónico y colaboración de un entorno local a la nube de manera segura y eficiente.

14. Bibliografía

1. Compare Microsoft 365 Enterprise Plans [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/compare-microsoft-365-enterprise-plans
2. Microsoft 365 Word [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/word?activetab=tabs%3afaqheaderregion3
3. ¿Qué es digitar en Word? [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://leydeteletrabajo.cl/que-es-digitar-en-word
4. Microsoft 365 Excel [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/excel
5. Microsoft 365 Powerpoint [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/powerpoint
6. Microsoft 365 Outlook [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/outlook/email-and-calendar-software-microsoft-outlook
7. Microsoft 365 OneDrive [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/onedrive/onedrive-for-business
8. Microsoft 365 Sharepoint [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/sharepoint/collaboration
9. Microsoft 365 Teams [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-teams/group-chat-software
10. Microsoft 365 PowerBI [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://powerbi.microsoft.com/es-es/
11. Microsoft 365 PowerApps [en línea] [consulta: 28 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/microsoft-365/business/microsoft-powerapps
12. Administración de la gobernanza de identidades de Microsoft 365 [en línea] [consulta: 01 de abril de 2023]. Disponible en: https://learn.microsoft.com/es-es/microsoft-365/enterprise/manage-microsoft-365-identity-governance?view=o365-worldwide
13. La identidad híbrida requería puertos y protocolos [en línea] [consulta: 03 de abril de 2023]. Disponible en: https://learn.microsoft.com/es-es/azure/active-directory/hybrid/reference-connect-ports
14. What is password hash synchronization with Azure AD? [en línea] [consulta: 05 de abril de 2023]. Disponible en: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs

15. How does self-service password reset writeback work in Azure Active Directory? [en línea] [consulta: 10 de abril de 2023]. Disponible en: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback
16. Set up directory synchronization for Microsoft 365 [en línea] [consulta: 10 de abril de 2023]. Disponible en: https://learn.microsoft.com/es-es/microsoft-365/enterprise/set-up-directory-synchronization?view=o365-worldwide
17. Inicio de sesión único de conexión directa de Azure Active Directory [en línea] [consulta: 15 de abril de 2023]. Disponible en: https://learn.microsoft.com/es-es/azure/active-directory/hybrid/how-to-connect-sso
18. Seguridad de Microsoft 365 [en línea] [consulta: 24 de abril de 2023]. Disponible en: https://learn.microsoft.com/es-es/microsoft-365/security/?view=o365-worldwide
19. ESCENARIO DE NUBE PARA EL MANEJO DE INFORMACIÓN SENSIBLE EN MICROSOFT OFFICE 365 [en línea] [consulta: 26 de abril de 2023]. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/6224-ccn-stic-885es-escenario-de-nube-para-el-manejo-de-informacion-sensible-en-microsoft-office-365/file.html
20. Configurar Information Rights Management (IRM) en el Centro de administración de SharePoint [en línea] [consulta: 02 de mayo de 2023]. Disponible en: https://learn.microsoft.com/es-es/microsoft-365/compliance/set-up-irm-in-sp-admin-center?view=o365-worldwide
21. Azure Information Protection P1 vs. P2: What's the difference? [en línea] [consulta: 02 de mayo de 2023]. Disponible en: https://www.techtarget.com/searchwindowsserver/tip/Azure-Information-Protection-P1-vs-P2-Whats-the-difference
22. Obtenga más información acerca de la prevención contra la pérdida de datos [en línea] [consulta: 05 de mayo de 2023]. Disponible en: https://learn.microsoft.com/es-es/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide
23. Más información sobre directivas y etiquetas de retención [en línea] [consulta: 05 de mayo de 2023]. Disponible en: https://learn.microsoft.com/es-es/microsoft-365/compliance/retention?view=o365-worldwide
24. Veeam Data Platform [en línea] [consulta: 08 de mayo de 2023]. Disponible en: https://www.veeam.com/es/data-protection-platform.html?ad=homepage-hero-banner
25. Acronis Cyber Protect [en línea] [consulta: 08 de mayo de 2023]. Disponible en: https://www.acronis.com/es-es/products/cyber-protect/backup/
26. AvePoint Cloud Backup [en línea] [consulta: 08 de mayo de 2023]. Disponible en: https://www.avepoint.com/products/cloud/backup

27. How it works: Azure AD Multi-Factor Authentication [en línea] [consulta: 11 de mayo de 2023]. Disponible en: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks
28. Self-service password reset frequently asked questions [en línea] [consulta: 15 de mayo de 2023]. Disponible en: https://learn.microsoft.com/en-us/azure/active-directory/authentication/active-directory-passwords-faq#self-service-password-reset
29. Microsoft Intune administra identidades, administra aplicaciones y administra dispositivos de forma segura [en línea] [consulta: 18 de mayo de 2023]. Disponible en: https://learn.microsoft.com/es-es/mem/intune/fundamentals/what-is-intune
30. Descripción del servicio Microsoft Teams [en línea] [consulta: 08 de junio de 2023]. Disponible en: https://powerbi.microsoft.com/es-es/why-power-bi/
31. Por qué Microsoft Power BI [en línea] [consulta: 23 de mayo de 2023]. Disponible en: https://powerbi.microsoft.com/es-es/why-power-bi/

15. Anexos

Annexo 1: Medidas de aplicación sobre el tenant

TIPO DE CONFIGURACIÓN AZURE AD	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	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 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	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	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
Contraseñas	Definiciones políticas de contraseñas	No expirarán nunca.	El valor recomendado no interfiere con ningún caso de uso.

Contraseñas	Definiciones 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 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.
Protocolos	Protocolos básicos de autenticación	Habilitar protocolos modernos, deshabilitando los básicos.	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.
Configuración del tenant	Configurar idioma y zona horaria	UTC + 01:00	El valor recomendado no interfiere con ningún caso 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	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.

TIPO DE CONFIGURACIÓN EXCHANGUE	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	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.
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.

TIPO DE CONFIGURACIÓN SHAREPOINT	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.
Autenticación	Bloquear autenticación legacy para SharePoint	Bloquear	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	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	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.
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.
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

TIPO DE CONFIGURACIÓN TEAMS	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
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	Chat	Activado	El valor recomendado no interfiere con ningún caso de uso.
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	Etiquetas sugeridas	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	Las cuentas de Surface Hub pueden enviar correos electrónicos	Desactivado	Desactivado salvo que se utilicen estos dispositivos
Modo de coexistencia	Modo de coexistencia	Teams solo	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.
Propiedades de mensaje	Propietarios pueden eliminar mensajes enviados	Activado	El valor recomendado no interfiere con ningún caso 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	Crear mensajes de voz	Desactivado	El valor recomendado no interfiere con ningún caso 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	Rol de permisos de chat	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.
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.
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.