MICROSOFT 365

GUÍA ESENCIAL

HORNETSECURITY

INTRODUCCIÓN

TE DAMOS LA BIENVENIDA A ESTE E-BOOK SOBRE MICROSOFT 365 DE HORNETSECURITY. TE ENSEÑAREMOS A UTILIZAR ESTOS SERVICIOS EN LA NUBE PARA MEJORAR TU NEGOCIO Y SACAR EL MÁXIMO PARTIDO A MICROSOFT 365. ESTA ES LA TERCERA VERSIÓN DE ESTE LIBRO ELECTRÓNICO Y SE HA ACTUALIZADO EN JULIO DE 2023.

MICROSOFT 365
GUÍA ESENCIAL

PARA QUIÉN ES ESTA GUÍA

Los destinatarios de este libro son los administradores y el personal de IT que gestionan un entorno de Microsoft 365. Trata de las prácticas recomendadas y las configuraciones óptimas para las aplicaciones y características más importantes. También ofrece una visión general de la suite, que resulta especialmente útil para quienes se disponen a migrar a Microsoft 365 o para quienes ya han migrado y necesitan hacerse una idea general. Si eres un desarrollador que quiere crear aplicaciones y servicios sobre la plataforma Microsoft 365, este libro no es para ti. Si te encargas más de tomar decisiones empresariales que de implementar cuestiones técnicas, este libro será una buena introducción a lo que puedes esperar cuando tu organización haya migrado a la nube y las formas en que puedes adoptar varios servicios de Microsoft 365 para mejorar la eficiencia de tu negocio. Si eres un Partner Microsoft que gestiona implementaciones de otras empresas y utilizas Microsoft 365 Lighthouse como forma de gestionar varios tenants en una sola consola, el contenido de este libro es completamente válido para ti.

ESTRUCTURA DEL LIBRO

El libro consta de tres partes. La Parte 1 (capítulos 1-6) es una introducción a Microsoft 365. Si ya estás familiarizado con los conceptos básicos, puedes pasar a la Parte 2 (capítulos 7-13) para aprender sobre la administración y gestión cotidianas, las prácticas recomendadas y el mantenimiento. La Parte 3 (capítulos 14-16) se centra en tres temas esenciales de M365 que todos los entornos de Microsoft 365 deben abordar, como son la seguridad, las copias de seguridad y el cumplimiento normativo.

Más adelante en el libro trataremos las diferencias con mayor profundidad, pero este es un buen momento para aclarar que **Office 365** (en adelante, O365) es una herramienta de colaboración por correo electrónico y una serie de otros servicios proporcionados en forma de Software como servicio (SaaS), mientras que **Microsoft 365** (en adelante, M365) es Office 365 más Azure Active Directory Premium, Endpoint Manager (Intune) – gestión de dispositivos y seguridad basada en la nube más Windows 11 Enterprise. Ambos son servicios de suscripción basados en el usuario que no requieren (o requieren muy poco) despliegue de infraestructura en las instalaciones. Para los planes de pequeñas empresas (hasta 300 usuarios) solo está disponible Microsoft 365 y, aunque ambos tienen planes Enterprise disponibles, las enormes ventajas de los servicios adicionales de Microsoft 365 hacen que no sea frecuente tener únicamente planes de Office 365. Por ello, a partir de ahora nos referiremos principalmente a Microsoft 365.

Esta es la tercera versión de este libro electrónico y se ha actualizado en julio de 2023.

ÍNDICE

PARTE 1

CONCEPTOS BÁSICOS DE OFFICE Y MICROSOFT 365

MICROSOFT 365
GUÍA ESENCIAL

Esta sección presenta M365, cómo realizar la gestión básica, la migración a M365, las opciones de asistencia, qué aplicaciones cliente es probable que admita y gestione y Windows 10/11. Si ya estás familiarizado con M365 y buscas información más avanzada sobre la administración de M365, ve directamente a la **Parte 2**.

¡OLVIDA LO QUE SABES!

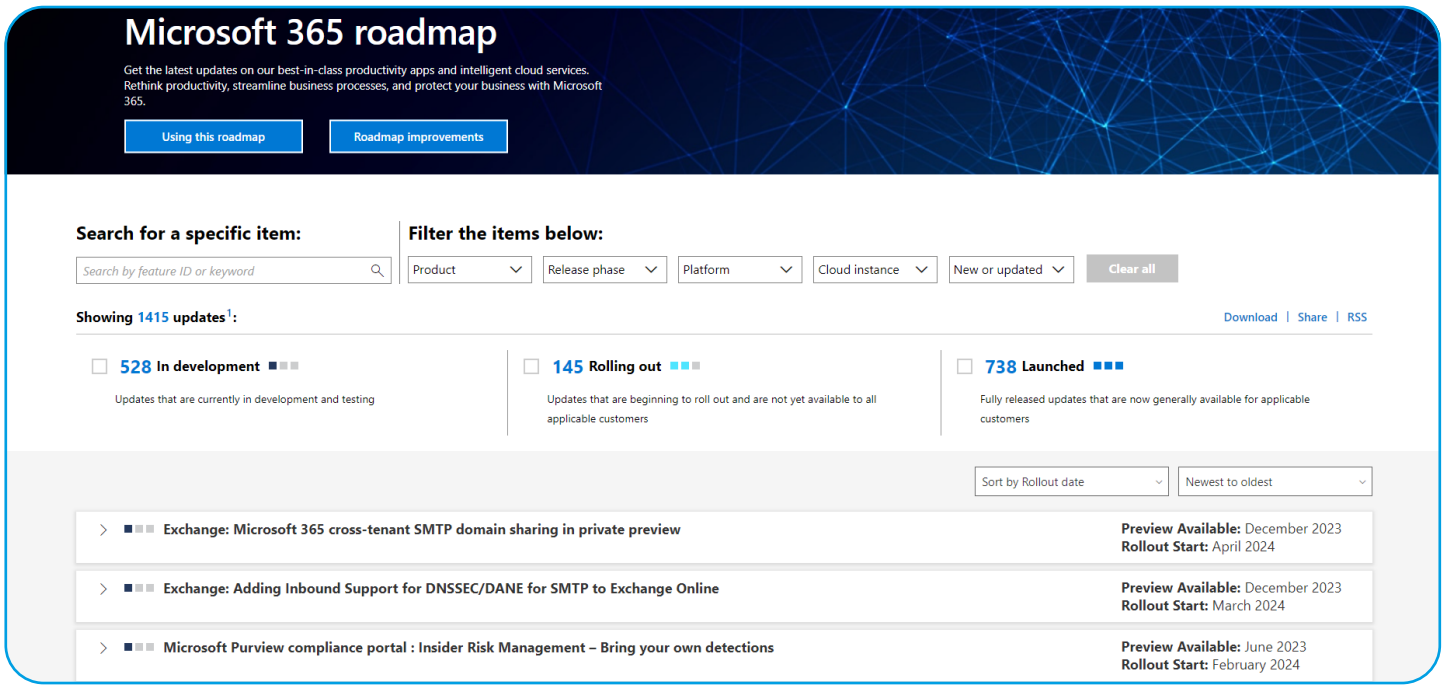
Una de las cosas más importantes que debes hacer si tienes experiencia con Exchange Server o SharePoint Server local es descartar la idea de que M365 es solo un alojamiento para Exchange o SharePoint. Hace algunos años, esto era cierto y O365 era simplemente Microsoft en su tarea de alojar servidores de Exchange, SharePoint y Lync en sus centros de datos, pero ya no es así. Ahora M365 es una plataforma integrada en la que Exchange Online y SharePoint Online constituyen algunos de los pilares básicos, pero sobre la que se asientan muchos otros servicios que te perderás (o malinterpretarás) si sigues pensando en términos de alojamiento de servidores de correo. Un ejemplo de ello es Microsoft Teams, un servicio de colaboración que utiliza Exchange Online para almacenar los datos y los chats conservados, SharePoint para almacenar documentos, Planner para la gestión ligera de proyectos y Azure AD para la identidad. Toda esa complejidad la gestiona Microsoft, y tú te limitas a administrar Teams como un servicio más. Esto también significa que nunca habrá un «servidor de Teams» con instalación local, ya que los componentes necesarios son demasiado complejos para que la mayoría de las empresas los implanten.

La otra cosa que hay que dejar de lado si vienes de un entorno local es la planificación de actualizaciones de software cada pocos años. Actualizar Exchange Server, por ejemplo, puede ser un proyecto de gran envergadura (dependiendo del tamaño de tu entorno), cuya planificación y ejecución puede llevar meses. M365 es algo totalmente distinto, ya que funciona a base de pequeñas actualizaciones que llegan cada día o cada semana, por lo que tu trabajo se transforma en evaluar estos cambios, cómo afectarán a los usuarios y gestionar el cambio en la organización.

CÓMO ESTAR AL DÍA

He trabajado con Exchange Server desde la versión 5.5 (1997) y me acostumbré al ritmo de una nueva versión cada 2-3 años. Compraba libros y me informaba sobre todas las novedades y cambios para prepararme para la siguiente iteración. Ese enfoque del desarrollo de software es historia.

Casi todos los proyectos de software (lo que incluye, sin duda, los de M365) pretenden ahora introducir cambios frecuentes e incrementales. Esto aporta varias ventajas: en primer lugar, las actualizaciones son más reducidas y no se requiere un gran plan de proyecto para la «actualización». En segundo lugar, los desarrolladores pueden ajustar el rumbo y añadir continuamente nuevas características en función de los comentarios de los usuarios con mucha más rapidez.



El plan de desarrollo de Microsoft 365

Sin embargo, esto implica un gran reto para los administradores de M365. En lugar de tener que planificar y familiarizarse con una gran cantidad de nuevas características que vayan a incorporarse en la próxima gran versión, las nuevas características se publican a diario y es necesario comprenderlas para que tu organización las aproveche. En función de tu estilo de aprendizaje, hay varias formas de conseguirlo. Algunas personas aprenden leyendo, otras escuchando, otras mirando vídeos y otras solo haciendo tareas por sí mismas (y como mejor aprendemos la mayoría es con una mezcla de todo esto). Aquí tienes algunos recursos que puedes añadir a tu caja de herramientas para estar al día de los cambios en M365:

El plan de desarrollo oficial de **Microsoft 365** (microsoft.com) te permite filtrar muchos componentes diferentes de M365.

Staying on top of Office 365 Updates (techcommunity.microsoft.com) es una excelente entrada de blog con enlaces a diversos recursos para gestionar la avalancha de actualizaciones y está pensada para diferentes tipos de público.

Novedades **de Microsoft Intune** ofrece detalles sobre las actualizaciones semanales de Microsoft Intune.

¿Cuáles **son las novedades de Azure Active Directory?** trata de las actualizaciones mensuales de Entra ID (anteriormente, Azure AD) (consulta el capítulo 7).

Azure AD Connect: Historial de lanzamiento de versiones trata de las actualizaciones de AAD Connect (consulta el capítulo 7).

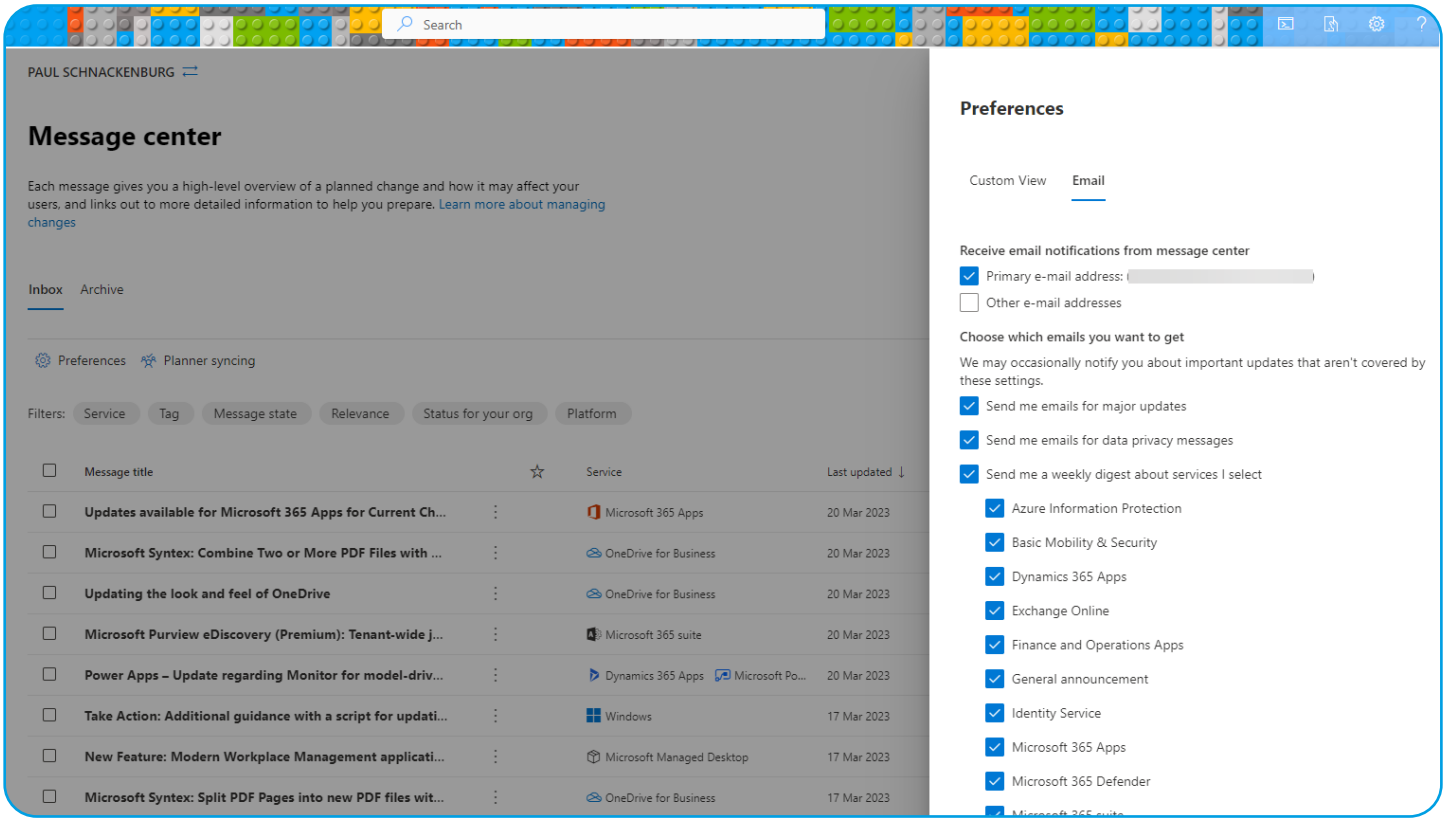
Microsoft Mechanics es un canal de YouTube con entrevistas y demostraciones sobre las próximas características, junto con listas de reproducción de Office y Azure.

Y, por último, el **Centro de mensajes** del portal (capítulo 2) muestra un flujo de los cambios y las novedades. Haz clic en el enlace Preferencias para personalizar los servicios que se deben actualizar y para decidir quién quieres que reciba el resumen semanal por correo electrónico. Una práctica recomendada es crear una lista de distribución de correo electrónico para que el personal que no tenga acceso al Centro de mensajes pueda recibir actualizaciones semanales por correo electrónico.

SÉ TU PROPIO CONEJILLO DE INDIAS

Es importante que, como administrador, pruebes las nuevas características cuando salgan o, a poder ser, cuando estén en fase de vista previa. Existen dos vías para las actualizaciones publicadas en O365: **Versión estándar y Versión dirigida**. La primera es la cadencia normal de despliegue, mientras que la segunda garantiza que recibas las nuevas características en cuanto estén listas.

Anteriormente se recomendaba tener un pequeño tenant de prueba aislado con este propósito y todo el tenant estaba en **Versión dirigida**. Si dispones del presupuesto, esta opción puede ser útil.



Control de las notificaciones del Centro de mensajes

Hoy en día es más frecuente definir los miembros del equipo de IT y los usuarios avanzados de tu empresa con la **Versión dirigida para usuarios seleccionados.** También existe una **opción** para garantizar que la instalación local de Aplicaciones de Office para empresas reciba las actualizaciones antes que el resto de los usuarios.

ADOPCIÓN

Si tu reto es ayudar a otras personas de tu empresa a subirse al tren de M365, Microsoft tiene una **comunidad excelente** y muchos **recursos** para ayudarte. Además, si necesitas ayuda para seguir impulsando la adopción de volúmenes de trabajo en M365, apúntate gratis al **Champions Program**.

Otro gran recurso es **Fasttrack**, que proporciona ayuda sobre la migración de cada tenant de M365 (y Dynamics 365 y Azure). Si usas M365 y tienes más de 150 usuarios puedes hablar con un experto en migración en línea, y si tienes más de 500 usuarios, **un ingeniero te puede ayudar con la migración** (de forma remota) y los proyectos de adopción posteriores.

CAPÍTULO 1:

LA BIENVENIDA A MICROSOFT (Y OFFICE) 365

EN ESTE CAPÍTULO VAMOS A VER LAS DISTINTAS VERSIONES DE M365, CÓMO ESCOGER UNA Y QUÉ VALOR APORTAN A TU EMPRESA. COMO SE HA INDICADO ANTERIORMENTE, SI YA HAS CONFIGURADO TU ENTORNO M365 O BUSCAS INFORMACIÓN MÁS AVANZADA, PASA DIRECTAMENTE A LA PARTE 2.

UN SERVICIO DE MICROSOFT 365 CORRECTAMENTE IMPLEMENTADO ES UN HABILITADOR PARA TU EMPRESA QUE FACILITA EL TRABAJO EN EQUIPO DE TU PERSONAL Y LA COLABORACIÓN TANTO INTERNA COMO CON PERSONAS EXTERNAS DE FORMA SEGURA. TAMBIÉN PERMITE A TUS EMPLEADOS TRABAJAR DESDE CASA O DESDE CUALQUIER LUGAR DE FORMA SEGURA. APARTE DE ELEGIR LA VERSIÓN ADECUADA DE M365, LA CLAVE PARA UNA IMPLEMENTACIÓN SATISFACTORIA ES LA PLANIFICACIÓN, LA FORMACIÓN DE LOS USUARIOS FINALES Y ASEGURARSE DE QUE EL PERSONAL INFORMÁTICO COMPRENDA SU NUEVA FUNCIÓN.

1.1: OFFICE 365

Hace bastantes años que Microsoft ha dejado de centrarse tanto en Office 365 y seguirá así. Mientras que para las empresas de menos de 300 empleados deja de ser viable, a las empresas más grandes se les recomienda considerar los planes de Microsoft 365 (ver más abajo).

Algunos servicios mencionados en este capítulo se analizan más a fondo en capítulos posteriores. Utilizaremos el término SKU (las siglas de «código de referencia» en inglés), que describe diferentes niveles de licencia.

Lo primero que debes decidir es si necesitas SKU Empresa o Enterprise. Escoge la primera opción si tienes un máximo de 300 usuarios. Si tienes una empresa más grande (o esperas crecer), quédate con Enterprise.

En otras palabras, **Aplicaciones de Microsoft 365 para empresas** (lo que se llamaba **Office ProPlus**) es el nuevo nombre de las aplicaciones de escritorio como Word, Excel, etc. que están disponibles para Windows y Mac. Algunos SKU lo incluyen, y otros no. Por otro lado, todos los planes incluyen Office Online (ahora llamado solo «Office» para evitar confusiones), por lo que Word, PowerPoint, etc. funcionan en el navegador.

Ten en cuenta que la funcionalidad de estas versiones en línea de Office está limitada en comparación con sus versiones de escritorio, pero son útiles para cambios rápidos.

En las versiones Enterprise (es solo un nombre y no tiene por qué ser para una gran empresa; por ejemplo, podrían ser cinco abogados que manejan datos muy sensibles en una PYME utilizando Enterprise E5) hay **Aplicaciones para empresas**, que solo te proporciona Aplicaciones para empresas y almacenamiento de archivos en OneDrive, pero ningún otro servicio en la nube. **E1** te ofrece Office (Online) y Exchange, OneDrive, SharePoint, Teams, Yammer y Stream, **E3** te ofrece Aplicaciones de Microsoft 365 para empresas además de los servicios en la nube de E1, y **E5** añade PowerBI como servicio en la nube, junto con varias características de seguridad (consulta el capítulo 15).

Echa un vistazo a la **comparación oficial** para ver claramente las diferencias entre estos planes.

En Opciones de planes **de Microsoft 365 y Office 365** encontrarás todos los planes, incluidas las versiones a medida para educación, administración pública y versiones específicas para China y Alemania.

Lo más importante es que los distintos SKU de cada familia no son mutuamente excluyentes. En una pequeña empresa de manufactura, los trabajadores de la fábrica pueden funcionar con Empresa Essentials, el personal de oficina con Empresa, y los ejecutivos con Empresa Premium. En el caso de una empresa más grande, los usuarios podrían estar repartidos entre las licencias E1, E3 y E5.

En **Descripción del servicio de la plataforma de Microsoft 365 y Office 365** encontrarás información detallada sobre todo lo que ofrece la plataforma.

1.2: MICROSOFT 365

Partiendo de los planes de O365 anteriores, M365 añade Windows 10 Enterprise, Endpoint Manager (Intune) y Azure Active Directory Premium.

Para empresas (hasta 300 usuarios) hay tres opciones: **M365 Empresa Básico** te da acceso a Office (solo en línea), correo electrónico, uso compartido de archivos, Teams y características de seguridad. **M365 Empresa Estándar** añade la versión de escritorio de Office «Aplicaciones de Microsoft 365 para negocios», mientras que **M365 Empresa Premium** añade gestión de dispositivos iOS, Android y Windows 10/11 y aplicación de políticas de Intune, además de muchas características de seguridad avanzadas. Ver más.

La versión **Enterprise**, **F3** (para trabajadores con contacto con el público, anteriormente llamada F1) te da acceso a Office (Online), Windows 10 Enterprise, Active Directory Premium P1, Azure Information Protection P1 e Intune, además de O365 E1. **E3** añade Active Directory Premium P1, Advanced Threat Analytics (ATA), Azure Information Protection P1, Windows 10 Enterprise e Intune, además de O365 E3. Por último, **E5** añade Active Directory Premium P2, Microsoft 365 Defender, Microsoft Defender para puntos de conexión, Microsoft Defender para Office 365, Microsoft Defender para Identity y Azure Information Protection P2, Windows 10 Enterprise, una serie de características de seguridad e Intune, además de O365 E5.

Es tentador pensar «soy una pequeña empresa, así que puedo ahorrarme algo de dinero con los SKU de Empresa», pero debes ser consciente de algunas limitaciones. OneDrive para Empresas está limitado a 1 TB por usuario en Empresa, mientras que en Enterprise puedes aumentarlo con una llamada al servicio de asistencia.

Microsoft ha realizado cambios sustanciales en el plan Empresa Premium, y ahora incluye todas las características de **Azure AD Premium Plan 1**, por lo que además de las características de seguridad ya incluidas (acceso condicional, restablecimiento de contraseñas de autoservicio y MFA), se añade Cloud App Discovery, Azure AD Application Proxy, grupos dinámicos y autenticación sin contraseña. Hay muchas características de seguridad valiosas en los planes Enterprise, especialmente en el M365 E5 (consulta el capítulo 15).

Ten en cuenta que puedes mover las licencias entre diferentes SKU (tanto subir como bajar de nivel) y que puedes actualizar SKU de Empresa a SKU de Enterprise. Este debate se ha centrado en los SKU completos y las características que contienen, pero también es posible adquirir características individuales, como Azure Active Directory Premium P1 como característica independiente. En función de las necesidades de (algunos) de los usuarios de tu empresa, puedes personalizar un paquete exacto con solo las características que necesiten.

Una buena forma de entender todas las partes de M365, cómo encajan entre sí y una rápida descripción de cada servicio es la **tabla periódica de Microsoft 365.**

La principal conclusión de este capítulo es que no debes dar por sentado que si eres una pequeña empresa debes optar automáticamente por un SKU de Empresa; investiga exactamente qué características serán útiles para las necesidades de tu empresa y no tengas miedo de mezclar diferentes SKU para diferentes funciones de los trabajadores.

CAPÍTULO 2:

GESTIÓN DE O365 Y M365

UNA VEZ TENGAS TU TENANT CONFIGURADO EN M365, DEBERÁS GESTIONARLO. EN ESTE CAPÍTULO REPASAREMOS LAS DIFERENTES INTERFACES QUE PUEDES UTILIZAR.

SI NO DISPONES DE UN TENANT DE O365/M365, REGÍSTRATE PARA OBTENER UN TENANT DE PRUEBA. SOLO DEBES HACER CLIC EN PROBAR GRATIS DEBAJO DE E3 O E5. ESTOS TENANTS DE PRUEBA DURAN 30 DÍAS, AUNQUE PUEDES AMPLIAR LA PRUEBA OTROS 30 DÍAS PONIÉNDOTE EN CONTACTO CON EL SERVICIO DE ASISTENCIA.

2.1: PORTALES WEB

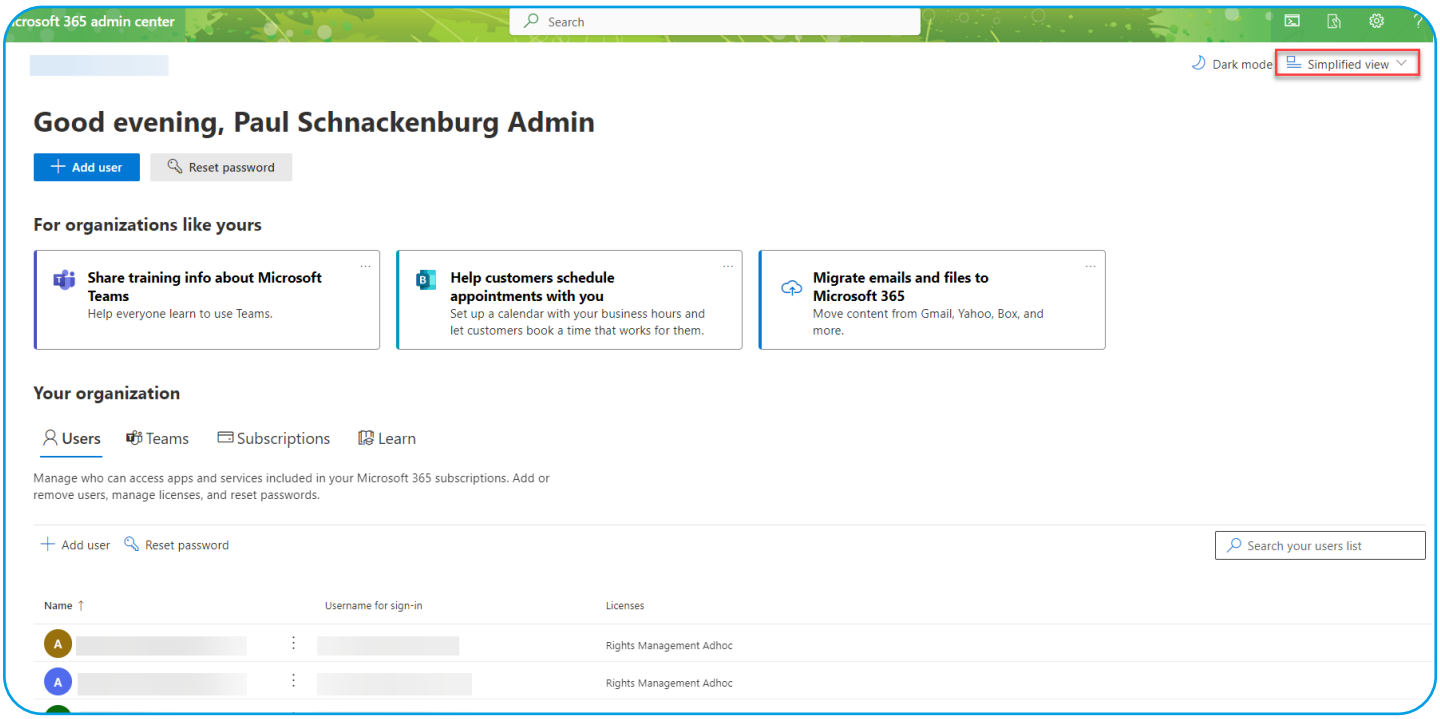
El portal principal es **admin.microsoft.com**, al cual también puedes llegar haciendo clic en el icono Admin de **www.office.com**. En la parte izquierda hay enlaces para gestionar Usuarios, Grupos, Facturación y Configuración, etc. y más abajo, en Centros de administración, hay enlaces a los portales individuales de Exchange, Teams, SharePoint, OneDrive y otros. En función del SKU, te aparecerán unos enlaces u otros.

Para el trabajo diario, destaca la posibilidad de, por ejemplo, seleccionar varios usuarios (Usuarios - Usuarios activos) y cambiar sus licencias. Puedes gestionar usuarios externos invitados con los cuales se hayan compartido documentos desde OneDrive o SharePoint, por ejemplo, en Usuarios - Usuarios invitados. También puedes restaurar un usuario eliminado recientemente (30 días o menos).

Puedes gestionar Grupos y Buzones compartidos, como «ventas@miempresa.com» (al que acceden varias personas diferentes), y Recursos como Salas y Equipos (reserva de salas de conferencias o coches de empresa). Facturación es el área donde puedes adquirir licencias adicionales, gestionar tus suscripciones y métodos de pago. Soporte es donde se presentan las solicitudes de servicio. En Configuración hay un área donde puedes configurar diferentes Servicios y complementos, mientras que los ajustes te permiten gestionar tus Dominios de correo electrónico. Informes tiene informes tanto de Uso como de Seguridad, mientras que Estado contiene dos áreas importantes: Estado del servicio te muestra si hay algún problema en la nube con tus recursos, y Centro de mensajes ofrece una lista de actualizaciones y cambios que están por llegar.

Cada Centro de administración te permite gestionar un servicio específico, como Azure Active Directory o Teams. **Msportals.io** tiene enlaces actualizados a la mayoría de los diferentes portales a los que puedes acceder directamente sin pasar por el portal principal.

Ten en cuenta que, si eres una pequeña empresa, existe la opción de tener el centro de administración en Vista simplificada (en lugar de Vista de panel), que oculta la mayor parte de la complejidad y proporciona un acceso sencillo a las tareas básicas de gestión de usuarios, grupos, Teams y dispositivos. Haz clic en Vista simplificada en la parte superior derecha de la página de inicio del centro de administración.



Vista simplificada del Centro de administración de M365

2.2: POWERSHELL

Es probable que los tenants pequeños nunca tengan que adentrarse más allá del portal web, pero si tienes una gran cantidad de usuarios seguramente querrás automatizar tareas comunes en PowerShell utilizando el nuevo **módulo de Azure AD**.

Para instalar el módulo, en una ventana elevada de PowerShell simplemente ejecuta:

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

Para conectarte (y opcionalmente autenticarte con MFA), usa:

```
Connect-AzureAD
```

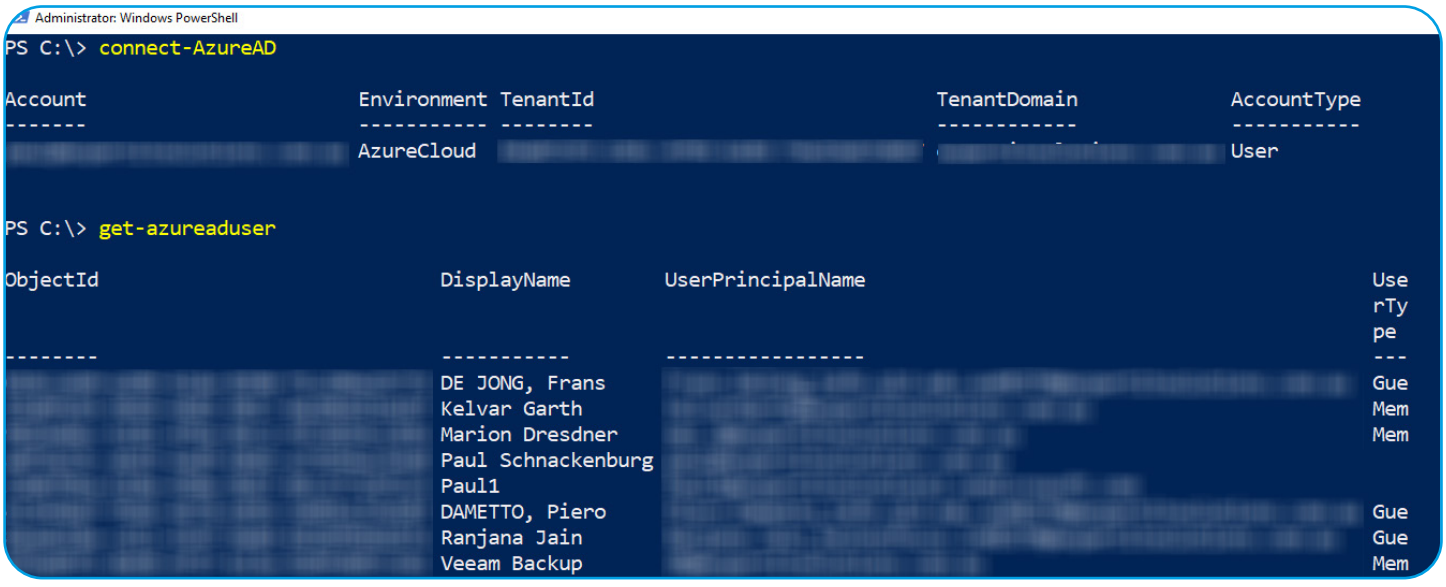
Para comprobar que todo funciona, usa:

```
Get-AzureADUser
```

Así obtendrás una lista de los usuarios que forman parte de tu tenant. Consulta las **instrucciones completas**, que incluyen información por si necesitas conectarte a tenants gubernamentales o chinos/alemanes.

Una vez conectado, hay muchas tareas que es posible que te interese realizar y quizás automatizar, como **la gestión de cuentas de usuario y licencias**, **la creación de sitios de SharePoint y la gestión de usuarios y grupos**, **la configuración de Exchange**, **la gestión de migraciones de correo electrónico** (capítulo 3) y **la configuración de la información de Teams**. Ten en cuenta que varios de ellos requieren la instalación de módulos adicionales.

Microsoft ha **documentado por fin** una forma oficial, con scripts, de ejecutar una única sesión PowerShell conectada a todos los servicios diferentes, tanto si usas MFA (capítulo 7) como si no.



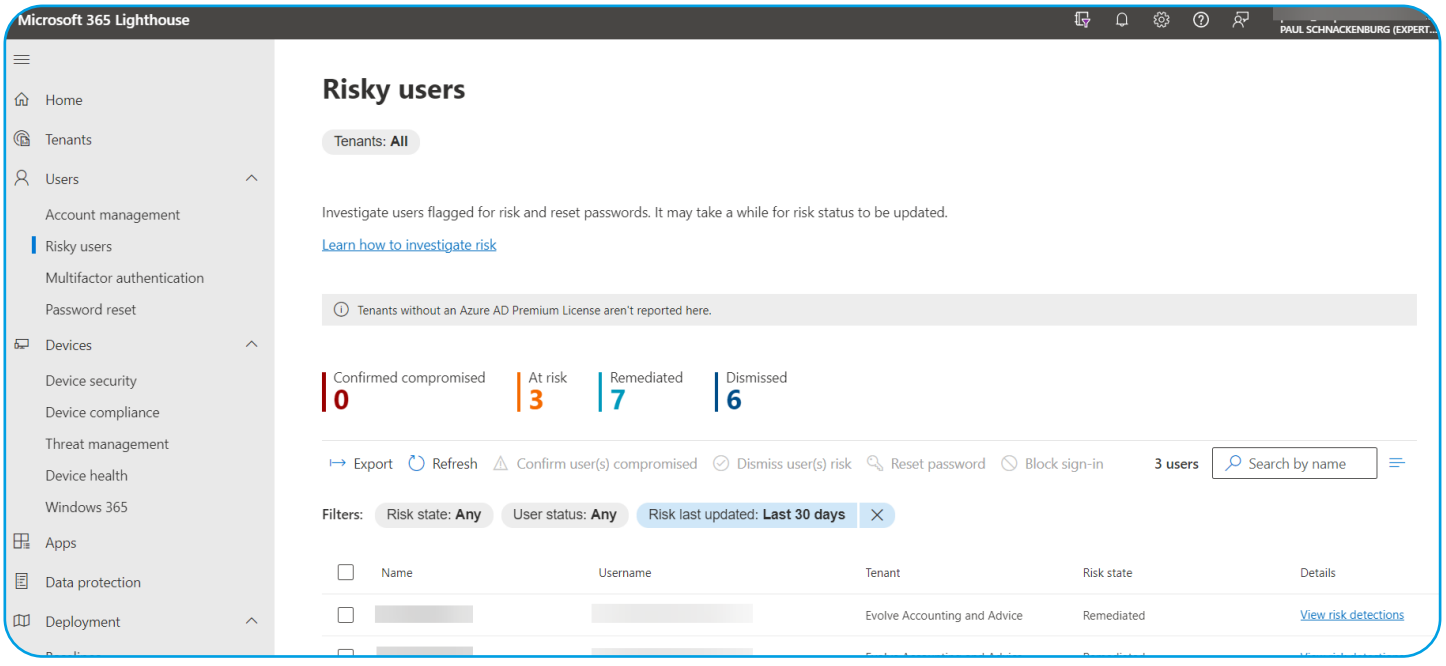
Conexión con PowerShell

Para SharePoint (tanto online como en versión local 2013/2016/2019) existe una alternativa/complemento de código abierto llamado **PnP PowerShell** al módulo oficial de SharePoint por el equipo de Patterns and Practices (PnP). Los cmdlets oficiales de SharePoint Online están enfocados en crear/gestionar sitios y usuarios, mientras que los cmdlets PnP son útiles para trabajar con objetos dentro de sitios que ya han sido creados.

Si necesitas gestionar la configuración de tenants de M365 o las extensiones de SharePoint Framework (SPFX), echa un vistazo a **CLI para Microsoft 365**, también del equipo PnP, que **funciona en Windows, macOS y Linux**. Y si no quieres instalar CLI en tu equipo, puedes **ejecutarlo directamente en Azure Cloud Shell**.

2.3: MICROSOFT 365 LIGHTHOUSE

Si eres un proveedor de servicios gestionados (MSP, por sus siglas en inglés) y te encargas de varios tenants de M365, deberías utilizar Microsoft 365 Lighthouse, que no debe confundirse con Azure Lighthouse. Ambas son tecnologías que permiten a los proveedores de servicios gestionar clientes de varios tenants, pero mientras que Azure es una forma de proporcionar a los usuarios de los proveedores de servicios un acceso limitado a los recursos de Azure, M365 Lighthouse es un portal que permite incorporar varios tenants y aplicar políticas y gestión (incluido el restablecimiento de contraseñas para cualquier usuario, en cualquier tenant) en una única consola.



Microsoft 365 Lighthouse

CAPÍTULO 3:

MIGRACIÓN A O365

SI TU EMPRESA ES NUEVA, ESTE CAPÍTULO NO ES RELEVANTE: SIMPLEMENTE CREA CUENTAS DE USUARIO EN LA NUBE, UNE TUS DISPOSITIVOS WINDOWS 10/11 A ENTRA ID Y GESTIONA TUS DISPOSITIVOS IOS Y ANDROID CON ENDPOINT MANAGER.

3.1: MIGRACIÓN

La mayoría de las empresas, sin embargo, disponen de inversiones en tecnología de forma local y necesitan migrar a M365. Este capítulo te presenta las opciones que tienes:

- Migración de traslado
- Migración por fases
- Migración híbrida exprés
- Migración híbrida mínima
- Migración híbrida
- Migración basada en PST
- Migración IMAP
- Herramientas de terceros

Si no tienes Exchange de forma local (es decir, si utilizas **Lotus Notes**/Domino, otro sistema de correo electrónico, **Google Workspace** u otra solución de correo electrónico en la nube, tendrás que recurrir a una migración IMAP o a servicios de migración de terceros.

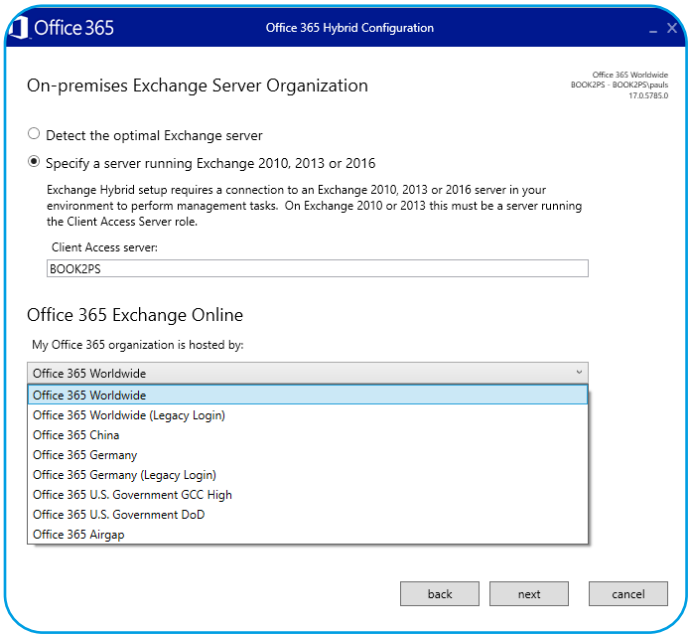
La mayoría de los otros métodos de migración se basan en la sincronización de directorios, en la que las cuentas de AD locales se sincronizan con Azure AD, que veremos en el capítulo 7.

Si todavía utilizas Exchange 2007, 2010 o 2013 (todos ellos ya no son compatibles), una configuración **Por fases** te **permite migrar los buzones de correo por lotes** una vez que hayas configurado la sincronización de directorios. Ten en cuenta que tendrás que volver a configurar manualmente el perfil de Outlook de cada usuario para que se dirija a O365 cuando se haya migrado su buzón de correo.

Para entornos más pequeños, el enfoque **Traslado** es el más sencillo. Microsoft sugiere **este método** para menos de 2.000 buzones (Exchange 2003 o superior), pero en realidad probablemente se ajuste a unos 100-150 buzones, dependiendo del ancho de banda de Internet. La idea es trasladar los buzones de correo de todo el mundo de la instalación local a la nube durante un fin de semana u otro período de inactividad adecuado.

Si utilizas Exchange 2010 o superior y quieres trasladar todos los buzones a la nube en unas semanas, valora la opción **Híbrida exprés**. Si tu organización es más grande y cuentas con unos meses de migración, considera la alternativa **Híbrida mínima**. Si tienes un entorno más grande (Exchange 2010 o superior) y tienes previsto estar en un estado híbrido durante un tiempo prolongado porque necesitas la capacidad de mover buzones de correo de la nube de nuevo a una instalación local (offboarding), valora la **Híbrida completa**. Para un desglose completo de los distintos tipos de migraciones híbridas, consulta **aquí**. Los distintos tipos de migraciones híbridas **proporcionan una coexistencia enriquecida** con una lista global de direcciones unificada, uso compartido de información de calendario libre/ocupado y traslados de buzones de correo sin problemas para los usuarios finales; cuando se haya trasladado su buzón de correo, solo se les pedirá que reinicien Outlook.

Si necesitas mantener un servidor Exchange (o varios) de forma local, recuerda **tenerlo siempre actualizado para que no se vea limitado** y, si es posible, **intenta retirarlo** utilizando en su lugar los cmdlets de PowerShell para gestionar los atributos de Exchange en AD.



Asistente de configuración híbrida

La **documentación de Microsoft** te conducirá al **asesor de migración de correo**, que podría dirigirte al Asistente de configuración híbrida (HCW) en función de las opciones que elijas en el asesor. El HCW te guiará por cada paso en función de la ruta que tomes, incluidas las versiones híbridas, Por fases y Traslado.

Las **migraciones IMAP** te permiten trasladarte desde sistemas que no sean Exchange y que admitan IMAP con un límite de 500.000 objetos por buzón y un tamaño máximo de correo electrónico de 35 MB.

Si tienes archivos PST con correo electrónico de forma local, **puedes migrarlos a Office 365**. Incluso tienes la herramienta PST Collection para localizarlos en tu red y recopilarlos. Si tienes muchos, tienes la opción de enviarlos en discos a Microsoft.

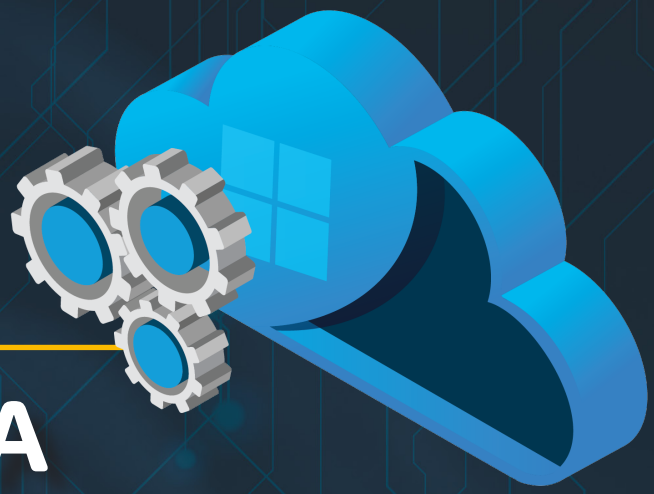
Una vez completada la migración, deberás tener en cuenta **el registro DNS del intercambiador de correo (MX)**, que habrá estado dirigiéndose a tu servidor de correo local y ahora deberás cambiarlo para que apunte a Exchange Online.

También deberás revisar tus **registros DNS de detección automática**, que es la forma en que Outlook y otros clientes de correo electrónico encuentran el servidor Exchange correcto de forma automática.

Si buscas una experiencia de migración de buzón sencilla, Hornetsecurity ofrece la Herramienta de migración de buzones (MMT) como parte de **365 Total Protection Enterprise**/**Enterprise Backup**.

CAPÍTULO 4:

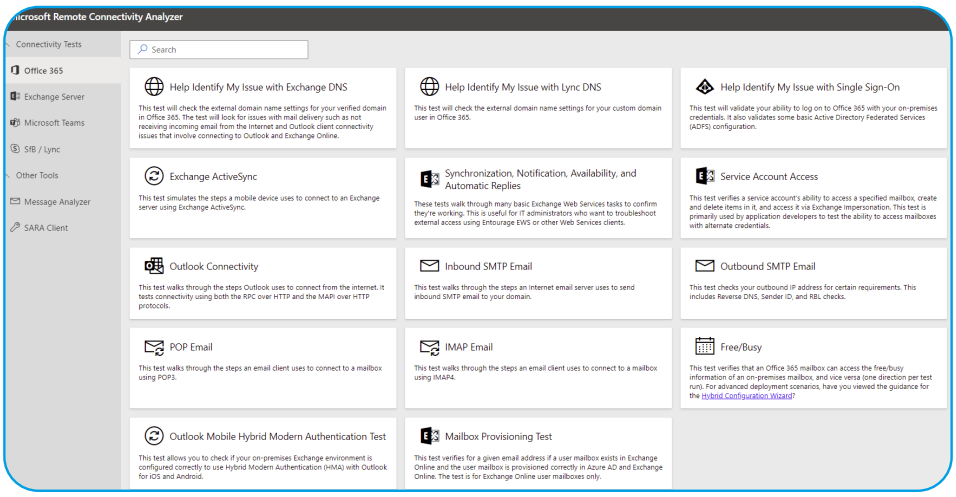
ASISTENCIA PARA M365



UNA GRAN DIFICULTAD CON LA QUE NOS ENCONTRAMOS EN EL MUNDO DE LA INFORMÁTICA, AL MENOS AL PRINCIPIO, ES LA PÉRDIDA DE CONTROL QUE CONLLEVA LA NUBE. SI TIENES UN PROBLEMA LOCAL EN LA ENTREGA DEL CORREO ELECTRÓNICO, PUEDES COMPROBAR CADA PARTE DE LA CADENA PARA VER DÓNDE ESTÁ EL PROBLEMA. UNA VEZ QUE HAS MIGRADO A M365, AHORA ES UNA RESPONSABILIDAD COMPARTIDA ENTRE TÚ Y MICROSOFT. EN ESTE CAPÍTULO VEREMOS DOS HERRAMIENTAS DE AYUDA AUTÓNOMA QUE UTILIZO CUANDO TENGO PROBLEMAS Y, A CONTINUACIÓN, VEREMOS CÓMO ABRIR Y TRAMITAR UN CASO DE ASISTENCIA TÉCNICA CON MICROSOFT.

4.1: PROBAR LA CONECTIVIDAD

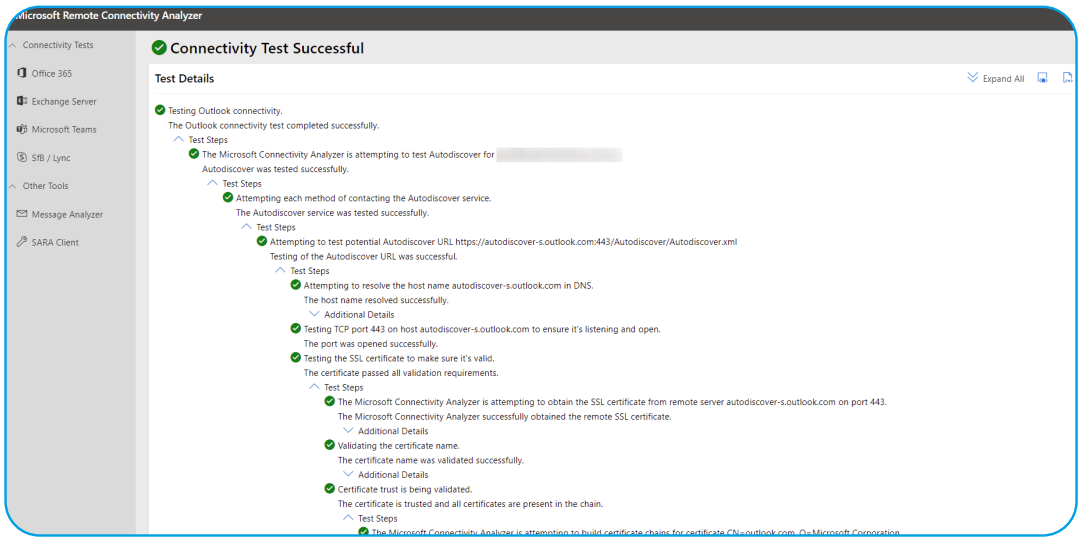
La conectividad es una causa frecuente de problemas para el correo electrónico y Teams. Microsoft ofrece una herramienta útil: el Analizador de conectividad remota de Microsoft (MRCA o RCA) en **https://testconnectivity.microsoft.com/** .



Analizador de conectividad remota

Aquí puedes probar varias cosas: entradas DNS, conectividad ActiveSync a Exchange, Outlook y funcionalidad Outlook Autodiscover, correo electrónico SMTP entrante y saliente, etc. Escoge la prueba que quieras realizar e introduce la información requerida. En función de la prueba, es posible que tengas que introducir un nombre de usuario y una contraseña válidos. Te sugiero que restablezcas la contraseña de esta cuenta después de haber completado la resolución de problemas. La verificación Captcha dura 30 minutos, por lo que si realizas varias ejecuciones a medida que cambias los valores, no tendrás que verificar que eres un humano cada vez.

El resultado de la prueba es exhaustivo y debería ayudarte a localizar el problema con bastante rapidez.



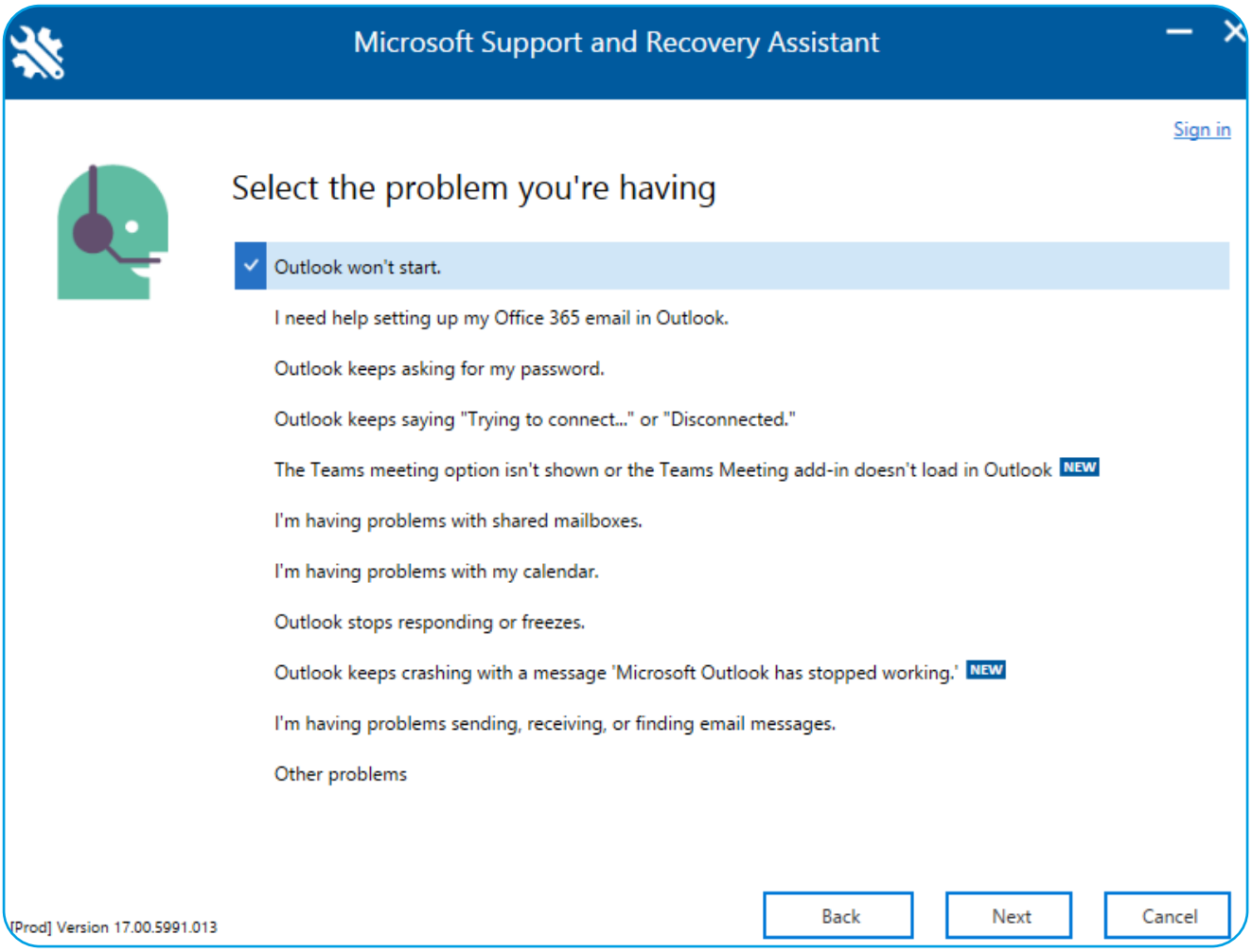
Informe de prueba de conectividad

4.2: HERRAMIENTAS DE CLIENTE

Si el problema no está relacionado con la conectividad y sospechas que se trata de un problema en un dispositivo cliente concreto, debes utilizar el **Asistente para soporte y recuperación de Office 365 (SARA)**, que te ayudará a identificar problemas de Outlook, Dynamics 365 y OneDrive para Empresas, así como problemas con Aplicaciones para empresas.

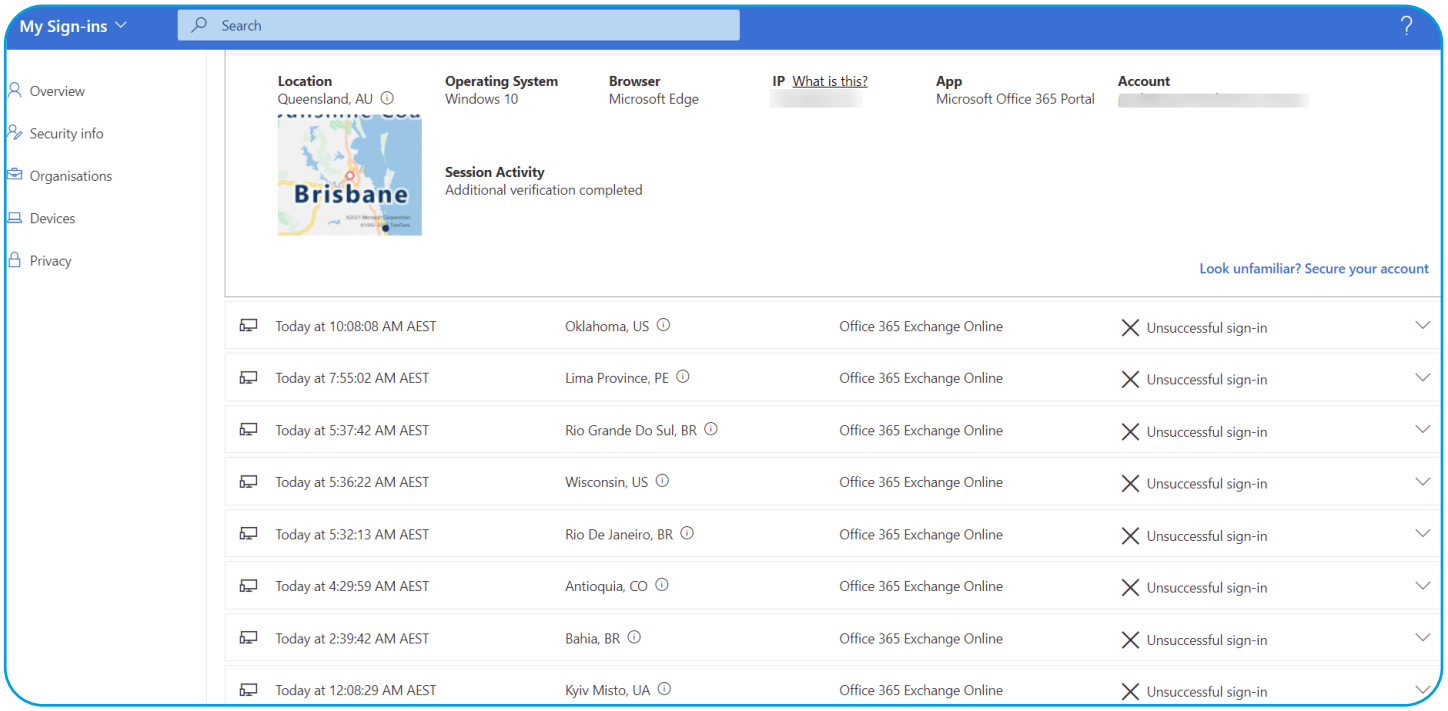
Se trata de una sencilla descarga que se ejecuta en el dispositivo afectado y que te guiará a través de una serie de preguntas para localizar el problema.

Por lo que he podido comprobar, cuando tienes problemas de perfil o de conexión intermitente (que no se deben a una mala configuración del servicio - véase RCA), la herramienta SARA suele ser bastante efectiva para detectar la causa.



Asistente para soporte y recuperación

Otra forma de ayudar a los usuarios finales a solucionar el problema sin ayuda externa son los sitios **Mis inicios de sesión**, **Mis grupos** y **Mis accesos**, que junto con **Mis aplicaciones** ofrecen a los usuarios una buena forma de gestionar su acceso a los servicios de M365. Mis inicios de sesión es también una excelente herramienta de información, ya que enumera tanto los inicios de sesión exitosos como los fallidos de los atacantes. Aquí tienes una lista de lo que pasa en mi cuenta en un día cualquiera (esta cuenta tiene la MFA activada):



Mis inicios de sesión con intentos de inicio de sesión de atacantes

4.3: SOLICITUDES DE ASISTENCIA

Cuando hayas agotado las opciones de autoservicio, pulsa el botón «¿Necesitas ayuda?» de la esquina inferior derecha del portal. En primer lugar, describe el problema para obtener algunos resultados sobre problemas frecuentes y su solución. Una vez que pulses Intro, se iluminará la opción Contactar con el servicio de asistencia en la parte inferior. Introduce tu información de contacto y si prefieres el contacto por teléfono o correo electrónico. También puedes adjuntar capturas de pantalla o archivos de registro (hasta cinco, cada uno de menos de 25 MB), elegir una zona horaria y un idioma para la comunicación.

En mi experiencia, la asistencia de M365 funciona bien y, por lo general, localiza el problema mucho más rápido de lo que yo lo haría por mi cuenta buscando en foros y probando diferentes soluciones.

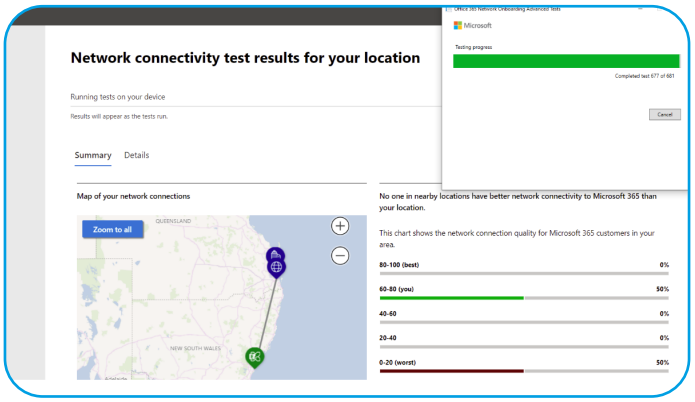
Si quieres saber cómo funciona, en el caso de que el ingeniero de asistencia técnica necesitara acceder a un servidor que aloje tus datos, usaría un «sistema de caja de seguridad» para solicitar el acceso y un supervisor te concedería una solicitud de tiempo limitado. Si usas O365/M365 E5, es posible que hayas activado la **Caja de seguridad del cliente**. Si es así, formarás parte del proceso y también tendrás que aprobar la solicitud.

Sin embargo, si el problema se encuentra en tu lado, los ingenieros de asistencia técnica utilizan Quick Assist en Windows para conectarse a tu servidor o PC cliente en modo de solo visualización y resolver el problema contigo.

4.4: ESTADO DEL SERVICIO

La sección Estado del centro de administración informa sobre el estado general de los diferentes servicios de M365 y si hay alguna interrupción o incidentes que afecten a tu tenant, siempre que puedas acceder al portal. Si la interrupción afecta al portal o a su sección de estado, prueba con **https://status.office365.com/**. No olvides seguir a @Office365Health y @MSFT365Status en Twitter.

La sección Estado también ofrece una nueva e interesante herramienta llamada **Conectividad de red**, que combina el cliente OD4B, el Servicio de localización de Windows y pruebas manuales opcionales de recopilación de datos para identificar la **calidad de la conectividad a Office 365** de cada cliente. Incluso tiene su **propio portal**.



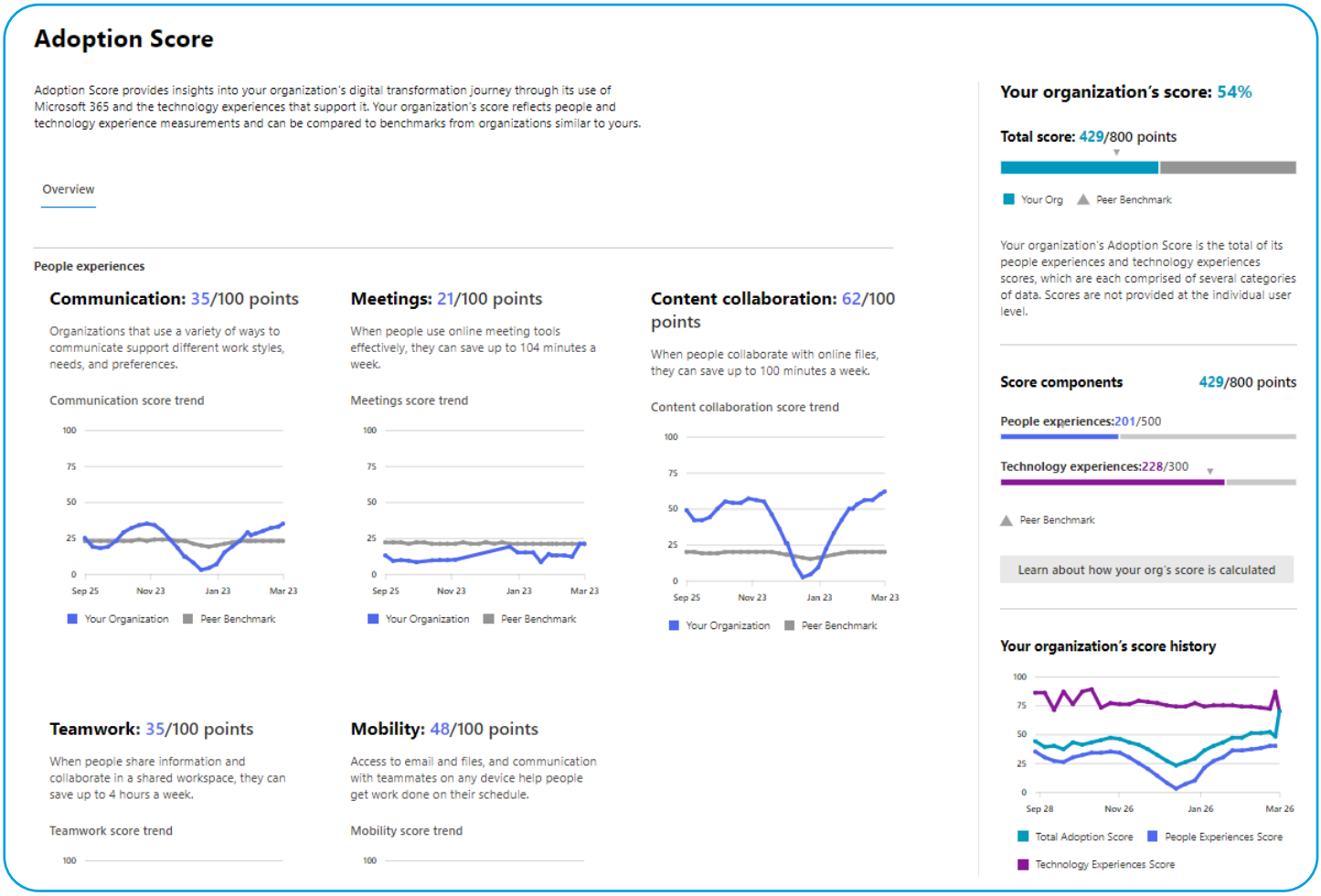
Prueba manual de conectividad de red a Office 365

4.5: CONECTIVIDAD DE LA RED

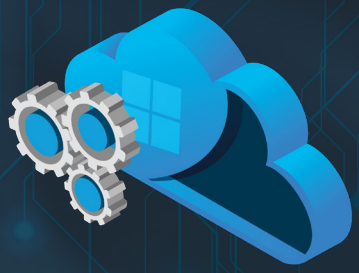
Muchas empresas ofrecen una experiencia deficiente a sus usuarios al obligarles a utilizar conexiones VPN de vuelta a la oficina y luego a Office 365 (la experiencia se vuelve más lenta en general y resulta imposible hacer llamadas y videollamadas en Teams) o incluso cortar con un proxy todo el tráfico saliente para la «seguridad». Esto último se basa en la suposición errónea de que todos los servicios web/sitios de Internet son «malos» y todo

el tráfico debe inspeccionarse, en lugar de diferenciar entre, por un lado, los servicios empresariales prestados por Microsoft y otros en los que se puede confiar y, por otro, los sitios web dudosos con los que cabe gestionar el tráfico adecuadamente. Aquí tienes un **artículo excelente** en el que se describen las técnicas de optimización necesarias y opcionales para M365. Microsoft también se ha asociado con muchos ISP, socios de intercambio de Internet (IXP) y proveedores de interconexión en la nube definida por software (SDCI) para una conectividad óptima a M365, Dynamics 365 y Azure mediante el **servicio Azure Peering**.

Si tu empresa utiliza una red WAN definida por software (SD-WAN), existe una función denominada **enrutamiento de red informado** que te ayudará a optimizar aún más tu conectividad al permitir el intercambio de datos entre Microsoft y el proveedor de SD-WAN para redirigir automáticamente el tráfico cuando sea necesario.



Puntuación de adopción de Microsoft 365



Por ahora solo es compatible IOS XE SD-WAN de Cisco, pero se espera que se añadan otros a medida que avance la versión preliminar.

La nueva **Puntuación de Adopción** está diseñada para que puedas ver en qué punto se encuentra tu empresa en su viaje hacia la transformación digital, para lo cual realiza un seguimiento de las métricas en dos categorías: experiencias de personas y experiencias tecnológicas.

4.6: CONFIGURACIÓN DE ESTADO DESEADO DE MICROSOFT 365

Hace mucho que PowerShell tiene una característica llamada Configuración de estado deseado (DSC); se define qué aspecto debe tener un sistema (máquina virtual, aplicación, etc), se aplica la política y el Administrador de configuración local se asegura de que el sistema tenga la configuración correcta y comprueba periódicamente que no haya desviaciones. Esto se denomina Infraestructura como código y **ahora está disponible para M365**, por lo que puedes tener un tenant de prueba donde evaluar nuevas configuraciones y ajustes que luego podrás exportar y aplicar a tu tenant de producción. También puede utilizarse para exportar todas tus configuraciones como «copia de seguridad», informar periódicamente sobre los cambios en la configuración y comparar la configuración de tu tenant con las prácticas recomendadas.

CAPÍTULO 5:

CLIENTES

HAY MUCHOS PROGRAMAS QUE SE PUEDEN UTILIZAR PARA CONECTARSE A M365. EN ESTE CAPÍTULO LOS EXAMINAREMOS Y VEREMOS CÓMO GESTIONARLOS DESDE EL PUNTO DE VISTA DE LA GOBERNANZA.

5.1: OPCIONES DE ESCRITORIO

Microsoft recomienda la última versión de Chrome, Edge, Firefox o Safari o Internet Explorer 11 para acceder a M365.

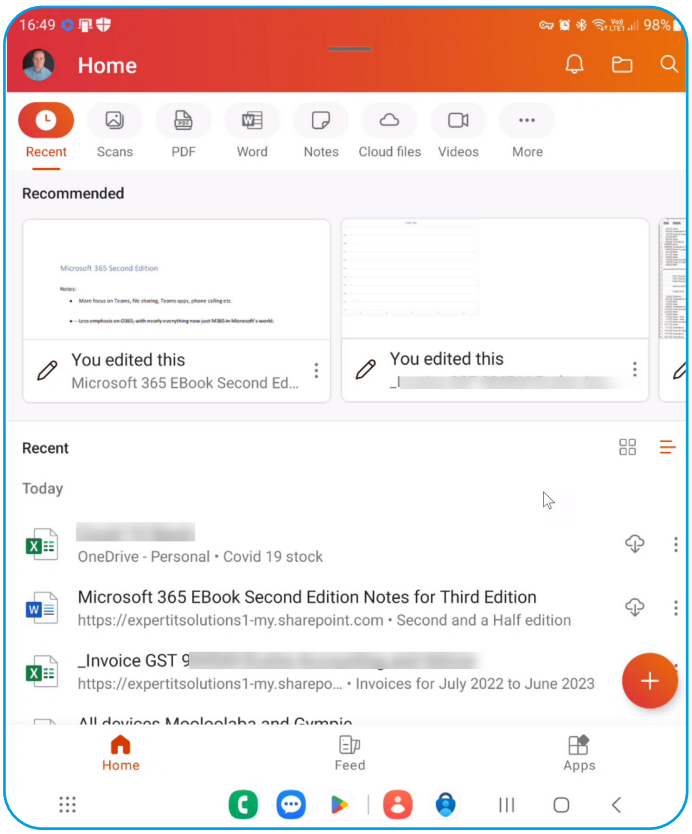
Si tienes instalado el cliente de escritorio enriquecido de Office, todas las versiones compatibles deberían funcionar con M365, pero es preferible utilizar la versión Aplicaciones para empresas para Windows y Mac que se incluye con Empresa Premium y E3+. Puedes **controlar qué usuarios obtienen** el Canal actual recomendado y quién obtiene el Canal empresarial mensual o el Canal empresarial semestral. Si quieres estar a la última, puedes inscribirte en el **programa Office Insider** para probar las nuevas características.

Mención especial merece Outlook Web App (OWA) o Outlook para la web, ya que es extremadamente capaz y no una versión «diluida» de Outlook que se ejecuta en un navegador. De hecho, Microsoft suele probar nuevas características y enfoques en el cliente web porque puede implementar los cambios mucho más rápido. Puedes utilizar las políticas de OWA para **controlar qué características** están disponibles para tus usuarios finales.

Puedes controlar qué protocolos pueden utilizar los usuarios para conectarse a Exchange con **Reglas de acceso de cliente**.

5.2: OPCIONES MÓVILES

Durante muchos años, la forma preferida de conectarse a Exchange en línea para el correo electrónico era utilizar ActiveSync, un protocolo compatible tanto con el cliente de correo de iOS como de Android (más o menos, ya que no todas las características eran compatibles con ambos proveedores). Microsoft ahora recomienda utilizar la aplicación de cliente gratuita Outlook, que permite a Microsoft introducir nuevas características mucho más rápido sin tener que esperar a que Apple o Google se pongan al día. Esta aplicación ha ido creciendo constantemente en capacidad hasta incluir la posibilidad de conectarse a Gmail y otros servicios de correo electrónico. Ahora la usan más de 100 millones de personas.



Aplicación M365 (Office) para dispositivo móvil

Antes había aplicaciones autónomas de Word, Excel, etc. para móviles, pero ahora todas están unificadas en la aplicación Microsoft 365 (Office), que permite abrir los distintos tipos de documentos de Office y editarlos en el móvil. Su instalación es gratuita, pero su funcionalidad depende de la cuenta con la que inicies sesión.

5.3: ONEDRIVE PARA EMPRESAS

El cliente de sincronización se instala automáticamente en Windows o Mac OS cuando se instala Aplicaciones para empresas, y puedes controlar su comportamiento mediante **esta plantilla de Directiva de grupo**. Enseña a tus usuarios a usar OneDrive para Empresas. El poder de tener tus archivos disponibles en cualquier dispositivo no debería subestimarse, muy especialmente la opción de coger cualquier dispositivo (si no tienes ningún dispositivo tuyo a mano), iniciar sesión en **www.office.com** en cualquier navegador y editar esos mismos archivos.

5.4: TEAMS

La aplicación Teams (capítulo 11) es el cliente de colaboración todo en uno de Microsoft. Admite chats de mensajería instantánea, chats de grupo, llamadas de voz, videollamadas y, si cuentas con la licencia, llamadas RTC a y desde teléfonos normales. Teams substituye a Skype for Business y desde principios de 2019 el cliente se instala automáticamente al instalar Aplicaciones para empresas. Si necesitas implementarlo con tu herramienta de implementación de software favorita, utiliza este **MSI**.

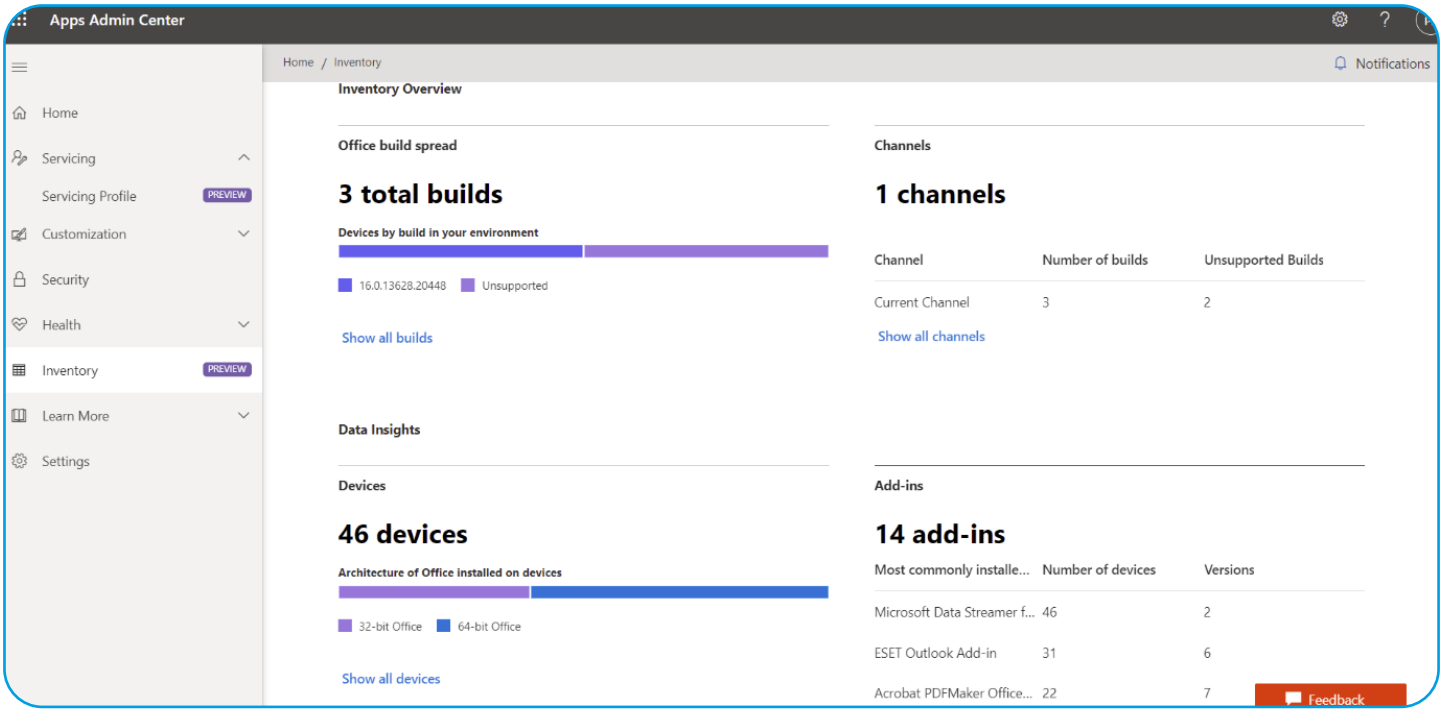
En el momento de escribir estas líneas, una nueva aplicación cliente de Teams que está en fase de versión preliminar pública debería solucionar las dos principales quejas que la gente tiene con el cliente actual: el rendimiento (el cliente es una aplicación electrónica y

utiliza mucha CPU y memoria) y el cambio entre diferentes tenants.

5.5: CENTRO DE ADMINISTRACIÓN DE APLICACIONES

El Centro de administración de aplicaciones de Microsoft 365 es una propuesta muy interesante de gestión en la nube para Aplicaciones para empresas (Office en el escritorio de Windows). En lugar de gestionar la configuración de personalización mediante la **Herramienta de implementación de Office (ODT)**, se utiliza el portal en la nube para crear los archivos XML necesarios. Sin embargo, el Centro de administración de aplicaciones puede hacer mucho más: realiza un inventario de las instalaciones de Office en todo el tenant, detecta qué versiones y números de compilación están instalados, cuáles ya no disponen de asistencia técnica y permite crear Perfiles de mantenimiento para implementar versiones más recientes de Office. También utiliza Security Policy Advisor para analizar el uso actual de las aplicaciones y te permite crear e implementar configuraciones de políticas en todas las instalaciones de Aplicaciones para empresas (sin depender de GPO o MDM), además de realizar un seguimiento de los complementos que se utilizan en todos tus dispositivos.

Si tienes muchos usuarios, es posible que no quieras que los usuarios descarguen Aplicaciones para empresas desde www.office.com (Portal M365 - Configuración - Servicios y complementos - Configuración de descarga de software de Office), sino implementarlas mediante tu método favorito. Si tu empresa utiliza System Center Configuration Manager, puedes usarlo para **implementar y actualizar Aplicaciones para empresas**.



Centro de administración de aplicaciones

Puesto que no se requieren licencias adicionales para el Centro de administración de aplicaciones, deberías valorar si te podría facilitar la vida como administrador de Office 365.

Si necesitas proporcionar un entorno de impresión moderno a tus usuarios sin tener que preocuparte de servidores de impresión ni de instalar controladores individuales para cada impresora en cada dispositivo, valora usar **Impresión universal**.

Otra forma de saber hasta qué punto están integrados los distintos componentes de M365 es mediante la **Búsqueda**, que te permite buscar en varios lugares de M365 y obtener contenido relevante para ti mostrándote solo aquel al que tengas acceso desde dentro de tu tenant.

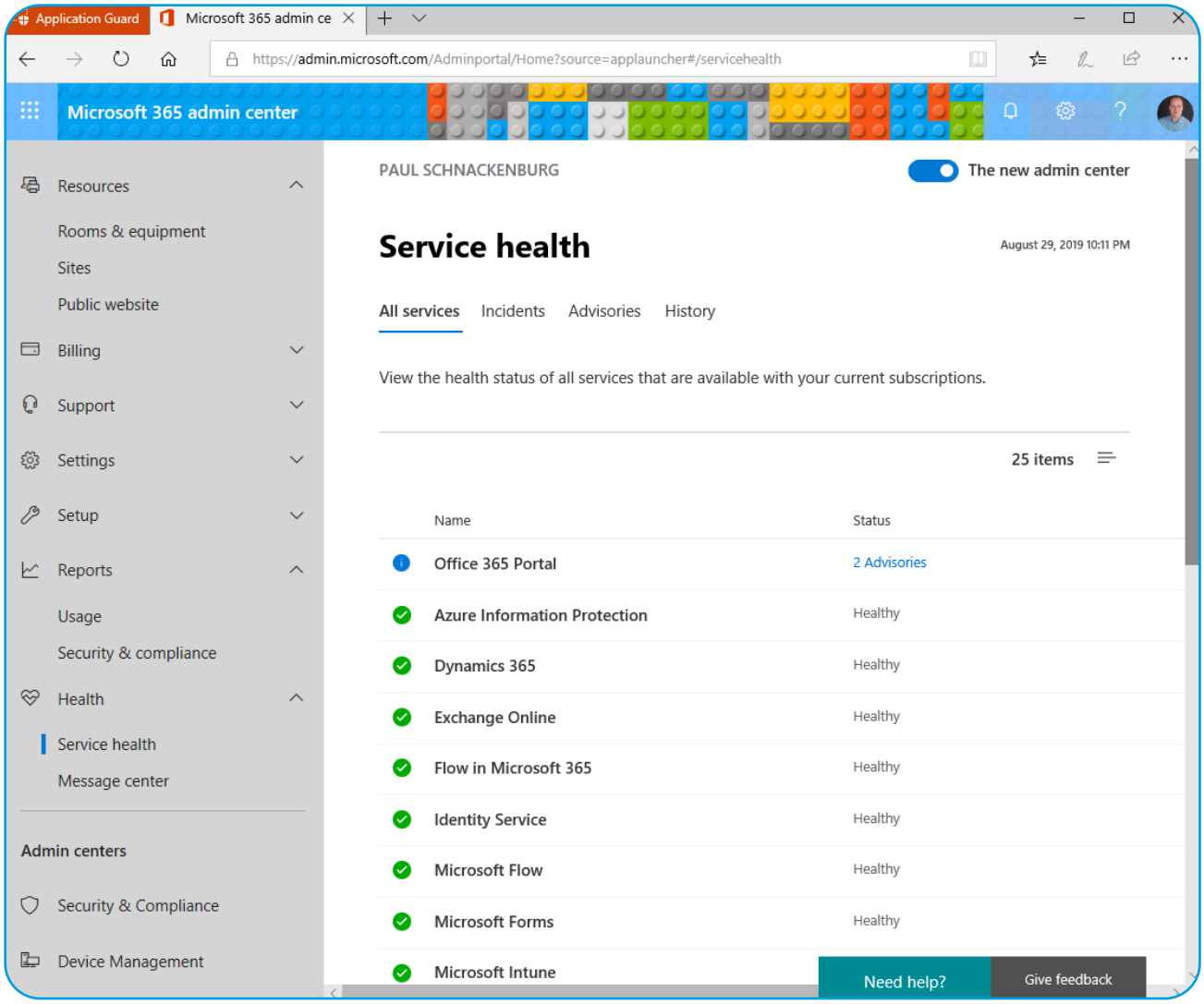
CAPÍTULO 6:

WINDOWS 11 ENTERPRISE

EL ÚLTIMO PILAR DE M365 ES WINDOWS 11 ENTERPRISE, CINCO DISPOSITIVOS POR CADA USUARIO CON LICENCIA QUE PASARÁN AUTOMÁTICAMENTE DE WINDOWS 11 PRO A ENTERPRISE EN CUANTO EL USUARIO INICIE SESIÓN. EN ESTE CAPÍTULO VEREMOS QUÉ CARACTERÍSTICAS DE SEGURIDAD ADICIONALES APORTA ESTO A TU EMPRESA.

6.1: WINDOWS 11 ENTERPRISE

Enterprise añade **Defender Application Guard** y Defender Application Control a las características de seguridad de Windows 11 Pro. **Application Guard** protege a tus usuarios cuando navegan por sitios potencialmente maliciosos utilizando Edge de forma aislada por hardware. Esta tecnología también **se ha ampliado a Word, Excel y PowerPoint**. **Application Control**, por su parte, se basa en versiones anteriores de AppLocker y bloquea la ejecución de aplicaciones no fiables, como plug-ins y complementos.



Navegación por una ventana Application Guard

Always On VPN no requiere Windows 11 Enterprise y es sucesor de **Direct Access** en caso de que aún necesites utilizar una VPN de cliente en tu empresa.

Aunque no es exclusivo de Windows 11 Enterprise, echa un vistazo a **Windows Hello para empresas** para mejorar la experiencia de inicio de sesión de tus usuarios y tu seguridad dejando atrás las contraseñas. Este es uno de esos casos en los que todo el mundo gana en seguridad.

Si quieres implementar un gran número de dispositivos Windows 11 y quieres ahorrarte el trabajo de limpiar cada dispositivo nuevo e instalar tu imagen personalizada, **valora el uso de Windows Autopilot**, una potente forma de «implementar» Windows 11 simplemente transformando la imagen preinstalada que te entrega tu OEM.

PARTE 2

GESTIÓN, MANTENIMIENTO Y ASISTENCIA TÉCNICA DE MICROSOFT 365

Aquí veremos características y configuraciones más avanzadas de M365 como Entra, para proteger las identidades de usuarios y cargas de trabajo, gestionar Exchange y SharePoint Online, Teams y cómo configurar de forma centralizada todos los dispositivos mediante Intune.

CAPÍTULO 7:

ENTRA ID

DETRÁS DE M365 HAY UN DIRECTORIO QUE CONTIENE CUENTAS DE USUARIO, GRUPOS Y OTROS OBJETOS DE SEGURIDAD. DURANTE MUCHOS AÑOS, ESTO SE CONOCÍA COMO AZURE ACTIVE DIRECTORY, AUNQUE TENÍA MUY POCO EN COMÚN CON ACTIVE DIRECTORY LOCAL. EN JULIO DE 2023, AZURE AD HA PASADO A LLAMARSE ENTRA ID. EN ESTE CAPÍTULO NOS CENTRAMOS EN ENTRA ID Y EN CÓMO SE USA EN RELACIÓN CON M365.

7.1: ENTRA, PRIVA Y PURVIEW

Antes de sumergirnos en Entra ID, echemos un vistazo al nuevo portal desde el que accederás a él: **entra.microsoft.com**. Todos los servicios relacionados con la identidad se alojan aquí, mientras que todas las características relacionadas con la Gobernanza de la información se encuentran en **compliance.microsoft.com**, en lo que se llama el portal Purview (capítulo 14), y tiene una sección con todas las características relacionadas con la privacidad llamada Priva.

Aparte de Entra ID, el portal Entra también alberga **Administración de permisos de Entra**, que inventaria y dimensiona los permisos administrativos en Azure, AWS y GCP (IaaS y PaaS). Esto no tiene relación con los permisos de Microsoft 365. También está Verified ID, que será útil en el futuro con las nuevas contrataciones y la gestión de identidades externas, y Global Secure Access, aunque estos temas quedan fuera del ámbito de este libro.

7.2: FAMILIARÍZATE CON ENTRA ID Y LA IDENTIDAD HÍBRIDA

AD utiliza Kerberos y Directiva de grupo, tiene una estructura jerárquica y se basa en LDAP, ninguno de los cuales es compatible con la nube. Entra ID opera sobre HTTPS, se puede acceder desde una API REST y admite protocolos de autenticación modernos como Security Assertion Markup Language (SAML), WS-Federation y OpenID Connect para la autenticación, así como OAuth para la autorización. También es compatible con la federación, por lo que podrás conectarte a otros sistemas de autenticación.

Hay tres tipos de autenticación compatibles con Entra ID: **basada en la nube, sincronización de directorios e inicio de sesión único (SSO) con AD FS.** La primera es adecuada si no cuentas con AD de forma local (o quieres eliminarlo) y solo creas cuentas en la nube. Es claramente la más fácil de configurar. Para las otras dos, es necesario que vincules tu AD local a tu tenant de Entra ID a través de la herramienta gratuita **AAD Connect**.

7.3: AAD CONNECT, TU CORDÓN UMBILICAL

AAD Connect (que seguramente pasará a llamarse Entra ID Connect) ha tenido varios predecesores a lo largo de los años con diferentes nombres. Si encuentras una instalación que use DirSync o AAD Sync, asegúrate de actualizar a AAD Connect porque esas herramientas ya no son compatibles. AAD Connect **permite conectar varios directorios locales a AAD.** También existía la versión 1 de AAD Connect, que está obsoleta, por lo que deberías utilizar la versión 2, que se actualiza automáticamente.

Puedes instalar la herramienta directamente en un DC o en un servidor miembro. No existe una verdadera opción de HA activa/activa, pero puedes configurar una segunda instalación de **AAD Connect** en un servidor independiente en **modo Provisional** y realizar una conmutación por error manual si el servidor principal va a estar fuera de línea durante algún tiempo.

AAD Connect sincronizará las cuentas de usuario y grupo en las OU que selecciones (o todo el directorio, cosa que no se recomienda) con Entra ID. Entonces, asignas licencias a esas cuentas de usuario y ya podrán empezar a utilizar los servicios en la nube. Ten en cuenta que esto también significa que la instalación local es siempre el lugar para crear nuevas cuentas y actualizar, desactivar o eliminar las existentes.

Existen **varias opciones** para gestionar las contraseñas en AD. La más sencilla es utilizar la **Sincronización de hash de contraseñas**, que toma los hash de contraseñas locales, los vuelve a hashear con un algoritmo moderno y almacena el hash del hash en la nube. Esto proporciona SSO a tus usuarios (aunque técnicamente es «el mismo inicio de sesión», ya que las dos cuentas de usuario están en dos directorios diferentes). Otra ventaja de este método es que Microsoft puede alertarte cuando encuentre credenciales en la web/dark web con cuentas de tu tenant en las que coincidan las contraseñas.

Si quieres evitar que las contraseñas de tus usuarios se almacenen en la nube (**ni siquiera un hash de un hash**), la **autenticación de paso a través (PTA)** es otra opción. **Configura agente**s en varios servidores (mínimo 3, máximo 40) de Windows Server 2012 R2 o superior (no se requieren puertos de entrada) y cuando un usuario inicie sesión en, por ejemplo, **www.office.com**, Entra ID verificará que se ha suministrado la contraseña correcta comunicándose con su AD local a través de los agentes PTA.

Tanto el PTA como la Sincronización de hash de contraseñas te permiten activar opcionalmente el **Inicio de sesión único de conexión directa** (Seamless SSO), en el que el usuario inicia sesión en AD y cuando accede a **www.office.com**, inicia sesión automáticamente.

Un elemento complementario es **AAD Connect Cloud Sync**, que se configura desde la nube y solo depende de agentes locales sencillos, lo que también significa que tendrás alta disponibilidad incorporada siempre y cuando implementes varios agentes. Poco a poco, las características de Cloud Sync **se han ido igualando** con las de AAD Connect y las principales características que faltan hoy en día son la compatibilidad con objetos de dispositivo, la posibilidad de sincronizar desde directorios LDAP que no sean de AAD, la compatibilidad con PTA, algunas opciones de filtrado y grupos grandes con más de 250 000 miembros. Sin embargo, el obstáculo para muchos será que no admite la reescritura híbrida de Exchange. Supongo que Cloud Sync acabará sustituyendo a AAD Connect.

La forma tradicional de no almacenar hash de contraseñas en la nube es utilizar **Servicios de federación de Active Directory (AD FS)**. Este método es **mucho más complejo y requiere configurar varios servidores** de forma local (o como máquinas virtuales en Azure), pero ofrece más flexibilidad. Si tu organización ya ha implementado AD FS para otros fines, configurar la federación con O365 no es un proyecto ingente, pero mi recomendación (y la de Microsoft) es seguir con PTA o con la Sincronización de hash de contraseñas. Dada la disrupción de la cadena de suministro de Solarwinds y la posterior intrusión en varias organizaciones que utilizan AD FS, además de la recomendación de Microsoft en los últimos años de migrar de AD FS a Azure AD, si tienes AD FS implementado, **es hora de hacer el cambio** a Azure AD.

7.4: MFA DE AZURE

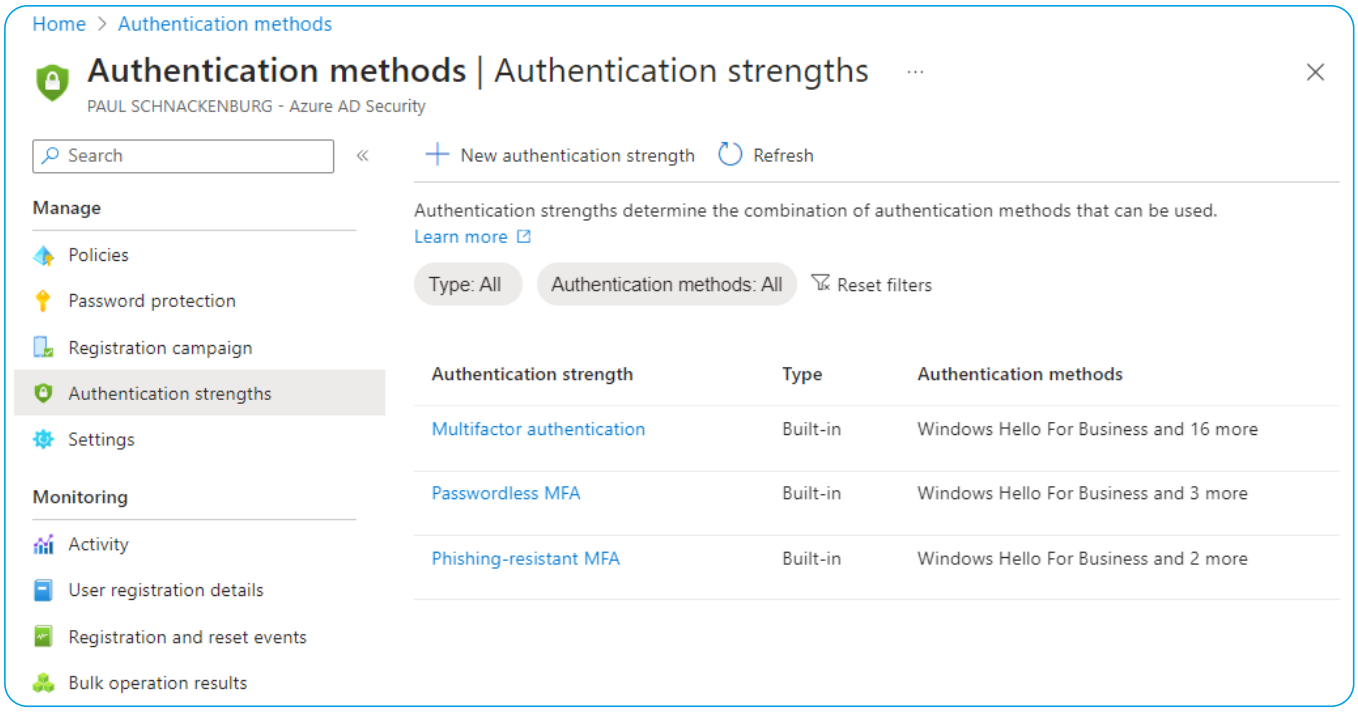
Una de las mejores cosas que permite Entra ID es la fácil configuración de la autenticación multifactor (MFA) para los usuarios. Las contraseñas son uno de los eslabones más débiles del panorama informático actual, y la mayoría de las brechas de seguridad que vemos se deben a que las credenciales de algún usuario se han visto comprometidas. Una solución a este problema es utilizar la MFA (a veces conocida como 2FA o autenticación en dos pasos), en la que la autenticación no solo requiere un nombre de usuario y una contraseña, sino también la presencia de un dispositivo o un gesto biométrico. Esto reduce drásticamente (en un **99 %, según Microsoft**) el éxito de los ataques de credenciales.

El sistema MFA puede llamarte por teléfono, enviarte un mensaje SMS con un código, una notificación o pedirte un código desde la aplicación gratuita **Microsoft Authenticator**. A menos que sea absolutamente necesario, no utilices las llamadas telefónicas ni los SMS, ya que son más inseguros que las opciones por aplicación.

De entrada, todas tus cuentas privilegiadas (Global/Exchange/SharePoint/administradores de cumplimiento, etc.) DEBEN usar la MFA. **Es gratis en todos los niveles de O365**, es **fácil de configurar** y la experiencia del usuario es relativamente fluida si instalas la aplicación en tu smartphone. Si eres responsable de la toma de decisiones de IT, seguro que tus administradores te pedirán que retires este método, pero este paso es ineludible para conseguir un nivel de seguridad aceptable: todos los administradores DEBEN usar la MFA. Dicho sea de paso, llevo muchos años utilizando la MFA de Azure sin ningún problema para mi propio tenant empresarial y para todos los tenants de los clientes que llevo.

Sin embargo, debes estar preparado para los **momentos en los que la MFA de Azure no está disponible**, y esto incluye la creación de una o, a ser posible, dos cuentas de administrador global en la nube que estén exentas de MFA y de cualquier política de CA. Estas cuentas deben tener contraseñas muy largas y complejas que solo estén disponibles para los administradores de alto rango, además de tener activada la supervisión para que, si alguna vez se utilizan, salten las alarmas. Estas cuentas de acceso de emergencia solo deben utilizarse para recuperar el acceso de los usuarios. Por ejemplo, si la MFA de Entra ID no funciona, puedes desactivar los requisitos de MFA mientras dure la interrupción para que los usuarios puedan iniciar sesión y ser productivos.

Activar la MFA para tus usuarios finales requiere cierta planificación y formación del usuario final. El nivel de conocimiento tecnológico de tus usuarios y el hecho de que trabajen normalmente desde oficinas corporativas influyen en la forma de implantar la MFA. Los administradores siempre cuentan con autenticación multifactor (MFA) de forma gratuita y los usuarios SKU de Empresa tienen la MFA incorporada, pero ambos carecen de las características avanzadas que ofrecen Entra ID Premium P1 (M365 E3) o Entra ID Premium P2 (M365 E5). Estas incluyen Omisión por única vez, IP de confianza/**ubicaciones con nombre**, cosa que te permite definir rangos de direcciones IP de oficinas corporativas donde no se solicitará a los usuarios la MFA. Ten en cuenta que todos los niveles de MFA te permiten (si activas esta característica) recordar la MFA en un dispositivo de confianza durante un número determinado de días (7-60).



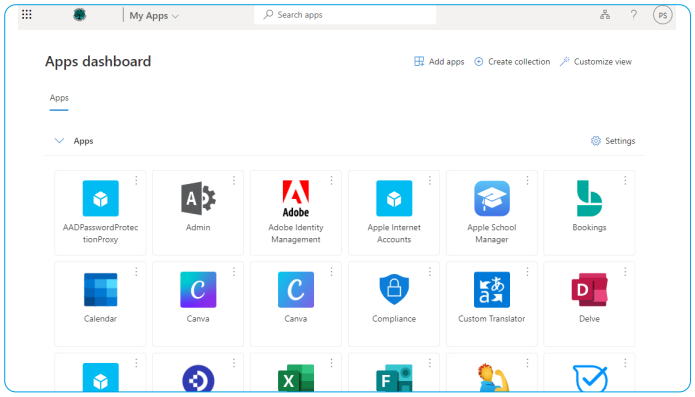
Niveles de intensidad de la autenticación MFA

Si un usuario ha iniciado sesión en un dispositivo y ha realizado correctamente la MFA, no se le volverá a solicitar en el mismo dispositivo durante ese período de tiempo. Si pierde el dispositivo o se lo roban, el usuario o tú podéis «dejar de confiar» en estos dispositivos fácilmente. En mayo de 2023, Microsoft activó la coincidencia de números para todas las aprobaciones de Microsoft Authenticator, por lo que en lugar de simplemente pulsar Aprobar o Rechazar, debes introducir un código de dos dígitos que aparecerá en la pantalla del ordenador. La aplicación también te mostrará la ubicación geográfica de la que procede la solicitud de MFA. Ambas funciones están diseñadas para combatir los ataques de fatiga contra la MFA, en los que el atacante intenta iniciar sesión repetidamente y genera tantas solicitudes en tu teléfono que al final algunos usuarios simplemente pulsan Aprobar para que pare.

Microsoft ahora introduce los **Valores predeterminados de seguridad** para todos los nuevos tenants. Puedes **activarlos manualmente** para tus tenants actuales. Esto aplicará la MFA para todos los usuarios y administradores únicamente con el uso de la aplicación Microsoft Authenticator, bloqueará la autenticación heredada (consulta el capítulo 15) y controlará el acceso al portal de Azure AD. Aunque estos elementos de seguridad son un buen punto de partida para una pequeña empresa con requisitos limitados, aconsejo ser cauto en organizaciones más complejas, ya que no hay forma de excluir de la MFA a las cuentas de acceso de emergencia o las cuentas de asistencia técnica, ni tampoco formas de gestionar a los usuarios que no tengan o no puedan acceder a la aplicación Authenticator mediante un teléfono.

7.5: PUBLICAR APLICACIONES

Una de las características más potentes de Entra ID es la capacidad de **publicar aplicaciones** (de terceros y **locales**) para tus usuarios finales. Aparecen junto a las aplicaciones normales de Office en **myapplications.microsoft.com** o **www.office.com** para que los usuarios las inicien con un solo clic.



MyApps portal

Por ejemplo, una cuenta de Twitter corporativa en la que varios usuarios tienen el nombre de usuario y la contraseña para enviar tuits en nombre de la empresa.

No solo tendrás que restablecer la contraseña en cuanto alguien abandone la empresa (porque seguro que no querrás que nadie ajeno a la organización tuitee en su nombre), sino que tendrás poco control sobre con quién más se comparte esa contraseña. Si publicas Twitter a través de Entra ID y creas un grupo AD para poner a los usuarios que quieras que tengan acceso, simplemente añades una cuenta de usuario a ese grupo y automáticamente tendrán acceso de inicio de sesión único a Twitter en el portal Aplicaciones sin conocer nunca la contraseña. Cuando ya no estén en la empresa y su cuenta se desactive, ya no podrán acceder. Para algunas de las más de 2.400 aplicaciones compatibles, puedes incluso configurar el **aprovisionamiento automático** para que cuando añadas un usuario al grupo Salesforce de AD, se le cree automáticamente una cuenta en Salesforce (sin que conozca la contraseña).

Una opción popular es utilizar la aplicación Single Sign-On de AWS **para integrar AAD y AWS**.

7.6: FUNCIONES PREMIUM

Entra ID Premium P1 no solo da acceso a más funciones de MFA, sino que también te permite **prohibir contraseñas de uso común** en tu AD local (incluyendo **una lista de palabras personalizadas**), autorizar a los usuarios a que **restablezcan sus propias contraseñas** cuando las hayan olvidado, unificar **MFA y Acceso condicional** y permitir a los usuarios registrarse tanto en la MFA como en el restablecimiento de contraseñas de autoservicio (SSPR) en **la misma experiencia**.

El nivel P2 añade la experiencia completa de Entra Identity Protection, donde se obtienen **informes y se pueden bloquear autenticaciones** en función del nivel de riesgo de la cuenta de usuario y el inicio de sesión, o incluso activar un **aviso MFA «extra»** basado en el perfil de riesgo del intento de autenticación. P2 también incluye la **Administración de identidades privilegiadas (PIM)** para convertir todas las cuentas administrativas en cuentas aptas y dar a los usuarios la opción de solicitar su elevación cuando necesiten realizar tareas administrativas (lo que se conoce como «administración Just in Time»).

En lugar de asignar funciones administrativas en Entra ID a cuentas de usuario individuales, **ahora puedes utilizar grupos para conceder acceso de administrador**. Los grupos necesitan un atributo específico (isAssignableToRole) configurado como «true» y una suscripción de cuenta de usuario estática (en lugar de dinámica, que asigne automáticamente cuentas de usuario a un grupo basado en un atributo como «departamento» en el directorio).

Mientras que AD tiene una estructura jerárquica basada en unidades organizativas (OU) para estructurar tus cuentas de usuario, máquina y grupo basadas en departamento, ubicación geográfica u otro parámetro, Entra ID tiene una estructura plana. Las **unidades administrativas (UA) son una característica** que pretende cambiar esto; mediante UA puedes estructurar cuentas de usuarios y grupos y luego **delegar permisos administrativos** a una sola UA o varias. Los administradores de UA necesitan una licencia Premium de Entra ID. Ten en cuenta que, a diferencia de las OU, en las que una cuenta solo puede estar en una única OU, una cuenta de grupo o de usuario puede ser miembro de varias UA (hasta 30).

Si tienes un entorno grande y licencias Premium P2, valora utilizar la **administración de derechos,** una forma de agrupar la aplicación, la pertenencia a grupos (incluido Teams) y el acceso al sitio en un único paquete de acceso.

Son útiles para los usuarios internos («eres la nueva persona de Marketing, aquí tienes el paquete que te da acceso a todo lo que necesitas») y también pueden utilizarse para conceder acceso a usuarios externos. Para las organizaciones asociadas con las que trabajes frecuentemente, puedes incluso configurarlo para que sus usuarios puedan solicitar paquetes, al estilo autoservicio. La administración de derechos también puede liberar al departamento de TI de la función de asignar permisos delegando la asignación de paquetes a los usuarios empresariales.

7.7: DIRECTIVAS DE ACCESO CONDICIONAL

P1 y P2 dan acceso a otra potente característica de Entra ID, **Acceso condicional (CA)**. CA te permite crear políticas de acceso a las aplicaciones (tanto en la nube como de forma local) basadas en la cuenta de usuario y los grupos a los que pertenezca, la aplicación a la que acceda, el estado de su dispositivo, su ubicación, el riesgo de inicio de sesión y el tipo de aplicación cliente desde la que acceda. Estas reglas de «si esto, haz aquello» implican una gran mejora de la seguridad de tus datos mediante la gestión de los factores de riesgo que afectan a la identidad y el acceso en M365.

Para facilitar aún más el establecimiento de buenas políticas de CA, existen **plantillas** (en versión preliminar en el momento de redactar este documento) que tratan los siguientes temas: Fundamentos seguros, Confianza cero, Trabajo a distancia, Protección de administradores y Amenazas emergentes.
Para asegurarse de no crear por error una directiva que bloquee al consejero delegado cinco minutos antes de su presentación ante la junta directiva, la opción de implementar políticas de CA en **Modo de solo informe** te permite evaluar el impacto que tendrán las políticas sin aplicarlas realmente.

Hay una **API para acceder a las directivas de CA**. Esto permite realizar copias de seguridad (mediante PowerShell, por ejemplo) de tus directivas de CA, restaurarlas, supervisar los cambios y tratarlas como código en lugar de gestionarlas manualmente en el portal. También puedes probar las políticas en un tenant de prueba antes de exportarlas desde allí e importarlas en tu tenant de producción después de que pasen la validación.

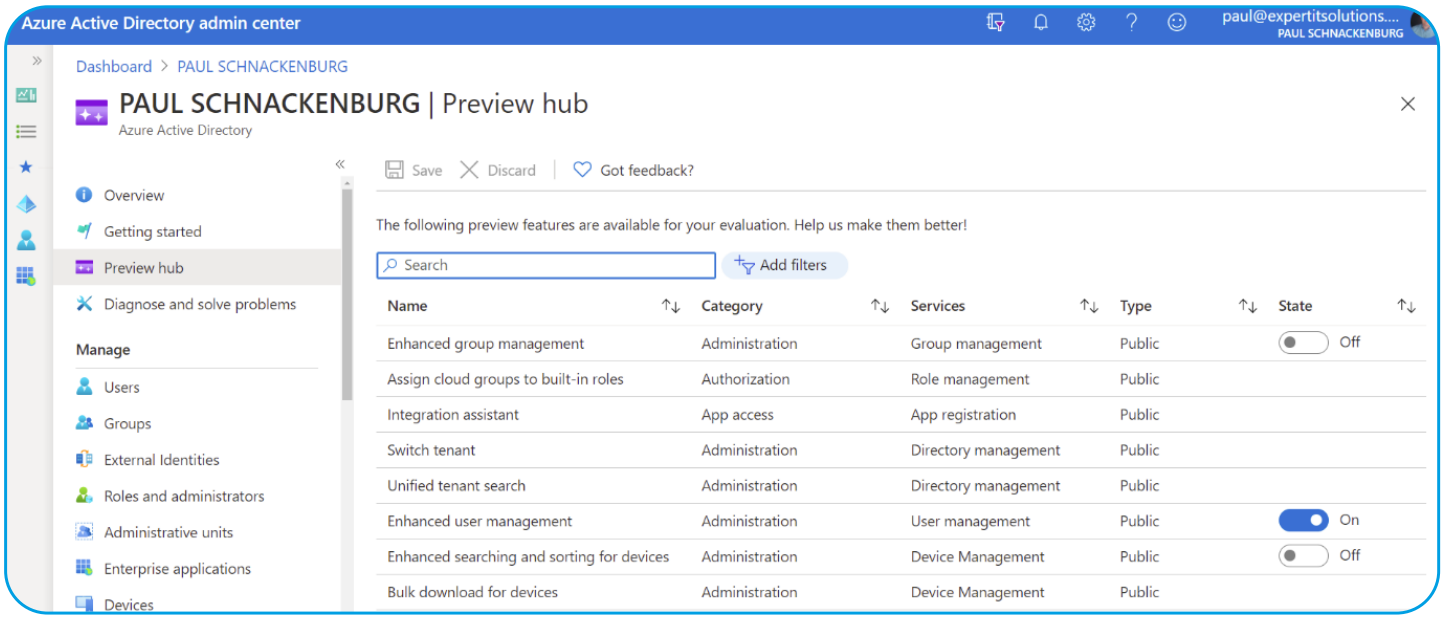
7.8: GESTIÓN DEL CICLO DE VIDA DE LAS CUENTAS

Una vez que implantes AAD Connect, no te olvides de actualizar la documentación de tus procesos para tener en cuenta el ciclo de vida completo de las cuentas de usuario, por ejemplo, asegurándote de que reciben las licencias adecuadas, que se añadan a los grupos adecuados y, cuando llegue el momento de desactivar la cuenta, que se sigan los **pasos correctos**.

Para asegurarte de que los usuarios (e invitados) no acumulen accesos que ya no necesitan, usa **Revisiones de acceso** (Premium P2), que ahora te permite **revisar todas las cuentas de invitado en una sola operación**, en lugar de hacerlo por Equipo/Grupo M365.

En el caso de un tenant de O365 o M365 más pequeño, lo más probable es que ni siquiera necesite acceder al portal completo de Azure AD y que, en su lugar, se limite a gestionar los usuarios en el portal de M365 (capítulo 2). No obstante, es una buena idea explorar el portal Entra «completo» en **https://entra.microsoft.com**.

Si te interesa probar las próximas funciones de Entra ID, utiliza el centro de Versión preliminar para conocer y activar las funciones de versión preliminar pública.



Centro de Versión preliminar de Azure AD

CAPÍTULO 8:

EXCHANGE ONLINE

EL CORREO ELECTRÓNICO ES LA SAVIA DE LA COMUNICACIÓN EMPRESARIAL, INCLUSO EN ESTA ERA DE TEAMS Y SLACK Y OTRAS MUCHAS HERRAMIENTAS DE COMUNICACIÓN. ES EL MÍNIMO DENOMINADOR COMÚN: LA ÚNICA HERRAMIENTA QUE SIEMPRE PUEDES UTILIZAR PARA CONTACTAR CON ALGUIEN SI TIENES SU DIRECCIÓN DE CORREO ELECTRÓNICO. Y EL CORREO ELECTRÓNICO ES UN PRODUCTO BÁSICO: TODAS LAS EMPRESAS LO NECESITAN, PERO NINGUNA VA A SER MÁS COMPETITIVA POR GESTIONARLO «MÁS EFICIENTEMENTE» QUE OTRA.

8.1: ES UN MUNDO HÍBRIDO

Gracias a la amplia presencia de Microsoft en los centros de datos corporativos de todo el mundo, uno de los puntos fuertes de M365 frente a Google Workplace, por ejemplo, es la clara ruta de migración a la nube de todo lo que tengas hasta el momento.

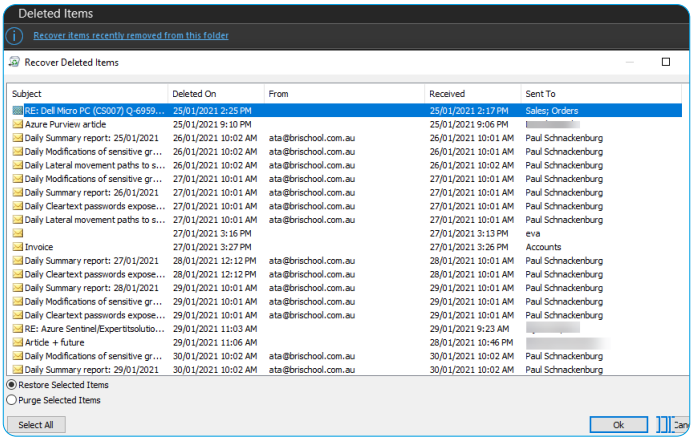
Si tienes Exchange 2013 o superior de forma local, puedes elegir cualquiera de los métodos de migración que vimos en el capítulo 3, algunos de los cuales proporcionan una coexistencia híbrida. La opción híbrida completa te permite seguir utilizando tu infraestructura local durante todo el tiempo que quieras y trasladar los buzones por lotes a la nube según tu propia planificación. Si lo necesitas, incluso puedes volver a trasladar los buzones de correo a una instalación local. Como es de esperar, hay muchos detalles que gestionar en una **configuración híbrida**, como los **requisitos previos**, la **conectividad de ActiveSync** y los **permisos de los buzones de correo**, especialmente si un usuario local tiene permisos para un buzón de correo en la nube o viceversa.

Si lo que buscas es una forma sencilla de mover buzones de Exchange a Exchange Online, Hornetsecurity tiene una gran **Herramienta de migración de buzones**.

8.2: COPIAS DE SEGURIDAD Y PROTECCIÓN DE DATOS NATIVA

Una cosa a tener en cuenta acerca de O365 es que Microsoft se asegurará de que no pierdas los datos de tu buzón de correo mediante la protección de datos nativa en Exchange: mantener tres copias de los datos de tu buzón de correo en servidores separados y una «copia retrasada» (a la zaga, para los casos en que los datos se corrompen en lugar de perderse) en un cuarto servidor.

Sin embargo, NO guardan copias de seguridad de tus datos que se remontan al pasado, lo que podría ser un problema para tu empresa en función de tus necesidades normativas. Existen varios servicios de terceros en el mercado que realizan copias de seguridad de los datos en línea de Exchange y SharePoint. Hornetsecurity **365 Total Backup** es una excelente solución de copia de seguridad, para buzones de correo, Teams, OneDrive para Empresas, SharePoint y archivos en endpoints. Consulta el **capítulo 16**.



Recuperar elementos eliminados de Outlook

Una cuenta de usuario y un buzón eliminados **pueden recuperarse** si no han transcurrido más de 30 días.

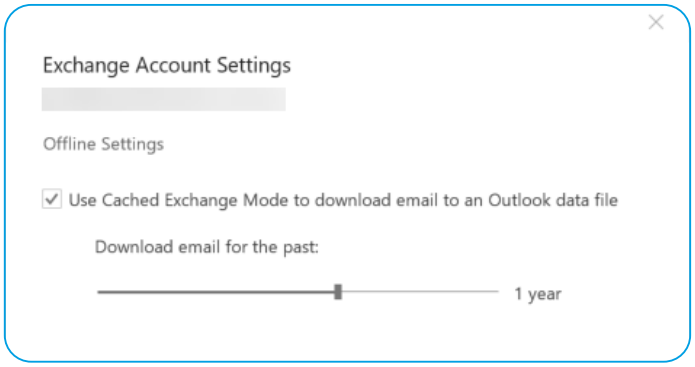
8.3: DETECCIÓN AUTOMÁTICA

Tanto si tu servidor Exchange está en la nube como en tu entorno local, es importante que las aplicaciones cliente puedan detectarlo: este es el trabajo de los registros de Detección automática en DNS. Hay otros registros DNS necesarios para M365 y los puedes consultar en **este artículo**.

Si tienes una implementación híbrida de Exchange, los registros de detección automática deben apuntar a tu servidor de buzones de Exchange 2016/2019 local.

8.4: GESTIÓN DE BUZONES

Hay muchas tareas asociadas a la gestión de buzones de correo, una de las cuales es la **gestión de cuotas**. Las licencias F3 tienen cuotas de 2 GB, las E1 están fijadas en 50 GB (con un archivo de 50 GB) y las E3 y superiores tienen cuotas de 100 GB con buzones de archivo que pueden ser de 1,5 TB como máximo. La diferencia entre un buzón y un buzón de archivo es que el archivo solo está disponible cuando tienes conexión. Puedes controlar cuántos datos del buzón se almacenan sin conexión en cada dispositivo con un control deslizante en Outlook. ensure they're smaller than 100 GB and no item is larger than 150 MB before starting the move.



Configuración de la caché sin conexión de Outlook

Si vas a migrar buzones de correo de gran tamaño a Office 365, asegúrate de que sean inferiores a 100 GB y de que ningún elemento supere los 150 MB antes de iniciar el traslado.

En la consola de Exchange puedes configurar las opciones de un buzón, como añadir alias de correo electrónico, ver el uso de cuotas, controlar qué clientes (OWA, Unified Messaging) y los protocolos (EAS, MAPI, IMAP y POP) puede utilizar el usuario, la retención de mensajes y la delegación de buzones. Esta última opción te permite configurar la opción **Enviar como** (para que otros usuarios envíen correos electrónicos como el usuario), **Enviar en su nombre** (para que el destinatario vea que el correo electrónico se envía en nombre del usuario) y **Acceso completo**.

8.5: ARCHIVO DE BUZÓN

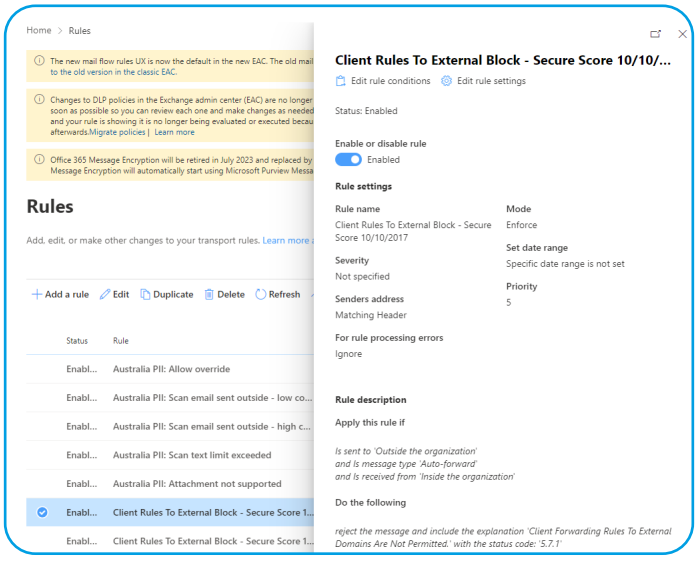
Como se mencionó anteriormente, puedes crear un Buzón de archivo para el contenido del buzón, que esencialmente sirve como un área de almacenamiento «sin fondo» para el contenido antiguo con la esperanza de que los usuarios dejen de adoptar archivos PST como solución de archivo. El cliente móvil de Outlook (iOS y Android) no puede acceder a los Buzones de archivo. Puedes activar la **expansión automática de archivos para usuarios con licencia E3 y E5** mediante PowerShell:

```
Set-OrganizationConfig -AutoExpandingArchive
```

También puedes activar los Buzones de archivo usuario por usuario. Ten en cuenta que la carpeta Archivo, que se crea en un buzón cuando haces clic con el botón derecho del ratón en un elemento y seleccionas archivar, no está relacionada con el Buzón de archivo.

8.6: REENVÍO DE CORREO ELECTRÓNICO

Recuerda que los usuarios pueden configurar sus buzones para que reenvíen el correo a una dirección de correo electrónico externa (con la opción de entregarlo en ambos buzones). Esto es algo que se debe vigilar porque, aunque puede haber razones comerciales legítimas para reenviar el correo, también es un vector de ataque favorito de los hackers, que leen los correos en silencio y los utilizan para diversos fines perversos. Hay un informe en el panel Flujo de correo que te muestra qué reglas de reenvío existen. También puedes **bloquear la opción de los usuarios de reenviar correos** de varias formas.



Regla de Flujo de correo para bloquear el reenvío externo de correo electrónico

8.7: BUZONES COMPARTIDOS

Cuando se tiene un equipo de usuarios que acceden al mismo alias, hay ocasiones en las que es preciso un buzón que no «pertenezca» a un usuario concreto, como por ejemplo ventas@ o asistencia@. Mientras el **Buzón compartido** no tenga una cuota superior a 50 GB o utilice un Buzón de archivo, no contará como una licencia. También es una opción para manejar el personal que ya no esté en la empresa mientras sigas necesitando supervisar su correo electrónico para los correos entrantes. Si conviertes su buzón a un buzón de correo compartido y asignas acceso al personal adecuado, se liberará la licencia y podrá asignarse a un nuevo usuario. Desde el punto de vista de la seguridad, asegúrate de que el acceso directo a los buzones compartidos esté bloqueado: los usuarios solo deberían acceder a los buzones compartidos añadiéndolos como buzón adicional en Outlook.

8.8: CONTACTOS Y USUARIOS DE CORREO ELECTRÓNICO

Tanto **Contactos** como **Usuarios** de correo aparecen en Todos los contactos, la Lista global de direcciones (GAL) y la Libreta de direcciones sin conexión (OAB). Un **contacto** apunta a una dirección de correo electrónico en un sistema externo, mientras que un **usuario** también apunta a una dirección externa, pero el usuario tiene credenciales de O365 para poder acceder a SharePoint Online o OneDrive para Empresas. Este último es un remanente de Exchange local. El uso compartido externo actual, como Teams, Planner y otros, utilizan la colaboración **Azure Business to Business (B2B)** para el acceso de invitados.

8.9: LISTAS DE DISTRIBUCIÓN

Agrupar direcciones de correo electrónico para facilitar la comunicación con equipos de personas es algo que los sistemas de correo electrónico llevan haciendo desde hace décadas: en el Centro de administración de Exchange Online (EAC) puedes crear listas de distribución (DL). Ten en cuenta que el valor predeterminado es crear un **Grupo M365** en su lugar y, de hecho, **Microsoft está presionando para reemplazar las DL por Grupos**. Los **grupos dinámicos** facilitan el mantenimiento de los miembros, ya que basan la pertenencia en un atributo de Entra ID como «departamento»: si se establece en Marketing, por ejemplo, el usuario se incluye automáticamente en el grupo correcto.

CAPÍTULO 9:

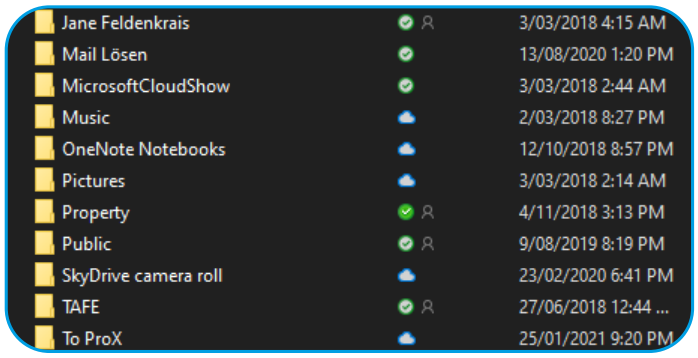
ONEDRIVE PARA EMPRESAS Y SHAREPOINT

COMPARTIR ARCHIVOS Y PROPORCIONAR UNA PLATAFORMA DE INTRANET ES UNA PARTE FUNDAMENTAL DE M365. EN ESTE CAPÍTULO VEREMOS ONEDRIVE PARA EMPRESAS (OD4B) PARA EL ALMACENAMIENTO Y USO COMPARTIDO DE ARCHIVOS PERSONALES, ASÍ COMO LA COLABORACIÓN BASADA EN LA WEB DE SHAREPOINT.

9.1: ONEDRIVE PARA EMPRESAS

OD4B se basa en SharePoint Online para proporcionar a cada usuario con licencia su propio almacenamiento de documentos: 1 TB para la mayoría de SKU. Esta cuota **puede incrementarse** a 5 TB en el caso de ciertas licencias.

Como hemos comentado, cuando almacenas archivos en OD4B puedes acceder a ellos desde cualquier dispositivo, a través de clientes para Android, iOS, Windows, macOS y una interfaz web. Hay que tener en cuenta **algunas limitaciones** en cuanto a nombres, tipos y tamaños de los archivos. El cliente de sincronización OD4B te permite **ver todos los archivos** en un dispositivo que hayas sincronizado. Pueden estar en estado de **Solo con conexión**, en el que los ves, aunque no estén realmente presentes en el dispositivo. Cuando abres un archivo de este tipo, se descarga y se almacena en caché y, por lo tanto, está **disponible localmente**. Un usuario también puede elegir uno o más archivos para **mantener siempre en este dispositivo**.



Archivos solo en la nube y anclados en OD4B

Puedes restringir la sincronización a solo los **dispositivos que formen parte del dominio**. Para ayudar a los usuarios a gestionar el contenido de las carpetas comunes, puedes utilizar **Desplazamiento de carpetas conocidas (KFM)** para sincronizar el contenido de las carpetas Escritorio, Documentos e Imágenes con OD4B y, por tanto, entre dispositivos.

9.2: SHAREPOINT

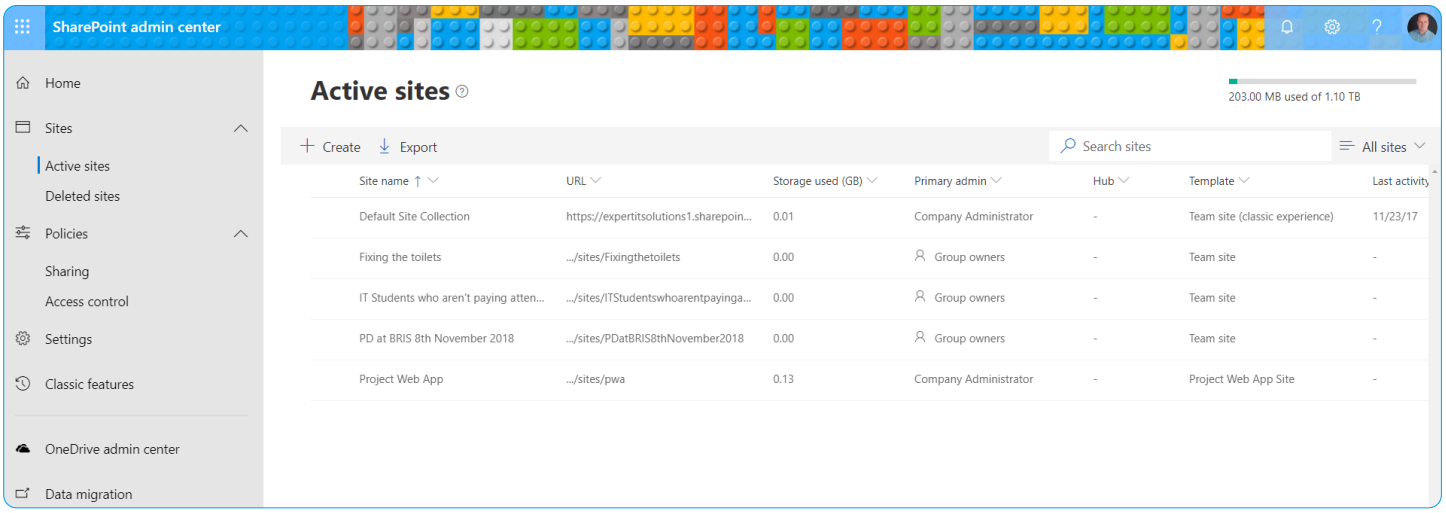
Si eres administrador de SharePoint local, estarás familiarizado con la gestión de la infraestructura subyacente de tus servidores, así como con la compleja red de sitios y flujos de trabajo de documentos que los usuarios finales utilizan sobre ella. Si son tus primeros pasos con SharePoint en la nube, es probable que tengas una experiencia muy diferente y que veas SharePoint simplemente como el almacenamiento de documentos subyacente para otras aplicaciones (Teams, Grupos, Planner) y quizás como la plataforma para la intranet de tu empresa.

Los elementos básicos de SharePoint son los **sitios** donde se almacena el contenido, y puedes controlar el diseño, el tema, la navegación y la seguridad con estilos clásicos y modernos. Si estás empezando o quieres crear nuevos sitios, los sitios Modernos **son tu opción**, y hay varios tipos disponibles, tales como **sitios de comunicación**, **sitios de grupo** y **sitios centrales**. Como parte de una visión más amplia de SharePoint, los sitios y páginas modernos son muy útiles, ya que se adaptan a las resoluciones de pantalla de los smartphones y a los distintos tamaños de pantalla de ordenador.

La función **Búsqueda** te permite encontrar sitios, archivos (incluidos los de OneDrive para Empresas), personas y contenido de noticias y, si hay imágenes en el contenido, la Inteligencia Artificial (IA) habrá extraído metadatos y, en su caso, contenido de texto de esas imágenes. Si has configurado una **implementación híbrida**, tus documentos locales también aparecerán en los resultados de búsqueda. Las **Aplicaciones** son complementos/partes web que amplían la funcionalidad de los sitios, mientras que las **Colecciones de sitios** son una forma de agrupar sitios con un propósito similar.

Si quieres configurar varios sitios, usa las **plantillas de sitios** para empezar. Si quieres crear un sitio de intranet, **Lookbook** es un servicio excelente con sitios muy bonitos para ofrecer experiencias modernas.

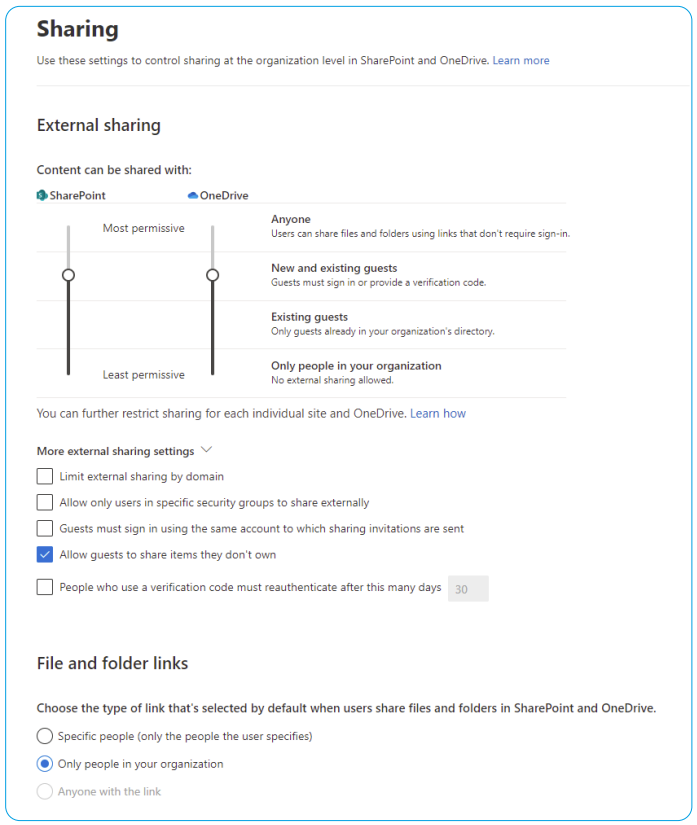
SharePoint Syntex es una tecnología que utiliza IA y aprendizaje automático (ML) para automatizar el procesamiento de contenidos y los transforma en conocimiento. Entiende tus documentos, procesa formularios y es aplicable a grandes organizaciones con flujos de trabajo y procesos complejos.



Centro de administración de SharePoint Online

Ten en cuenta los **límites de SharePoint Online**, en particular el almacenamiento total disponible (1 TB + 10 GB por licencia adquirida). La búsqueda es un área que **deberías tratar de personalizar** para que los usuarios finales disfruten de una buena experiencia. El uso compartido es otro aspecto que conviene controlar, ya que **la forma en que los usuarios pueden compartir contenidos** internamente y (sobre todo) externamente influye directamente en el equilibrio entre colaboración y seguridad.

La migración de contenido desde SharePoint Server local y archivos compartidos de red a M365 es una tarea de la **Herramienta de migración de SharePoint**, así como de numerosos servicios de terceros. Si un usuario borra archivos accidentalmente o un ransomware cifra los archivos almacenados, puedes utilizar la interfaz **Restaurar archivos** para restaurar archivos y carpetas o bibliotecas enteras de hasta 30 días atrás. También está la **Papelera de reciclaje** (93 días de retención) para restaurar archivos individuales y **Restaurar archivos** para OneDrive.



Control de uso compartido externo de SharePoint y OD4B

CAPÍTULO 10:

GRUPOS DE MICROSOFT 365

LOS GRUPOS DE M365 SON UN ELEMENTO BÁSICO EN DIFERENTES SERVICIOS, Y EN ESTE CAPÍTULO VEREMOS SUS DIVERSOS USOS.

10.1: TIPOS DE GRUPOS

Un aspecto que suele ser complicado para los nuevos administradores de O365 son los distintos tipos de grupos. Aquí tienes un breve resumen para resolverlo:

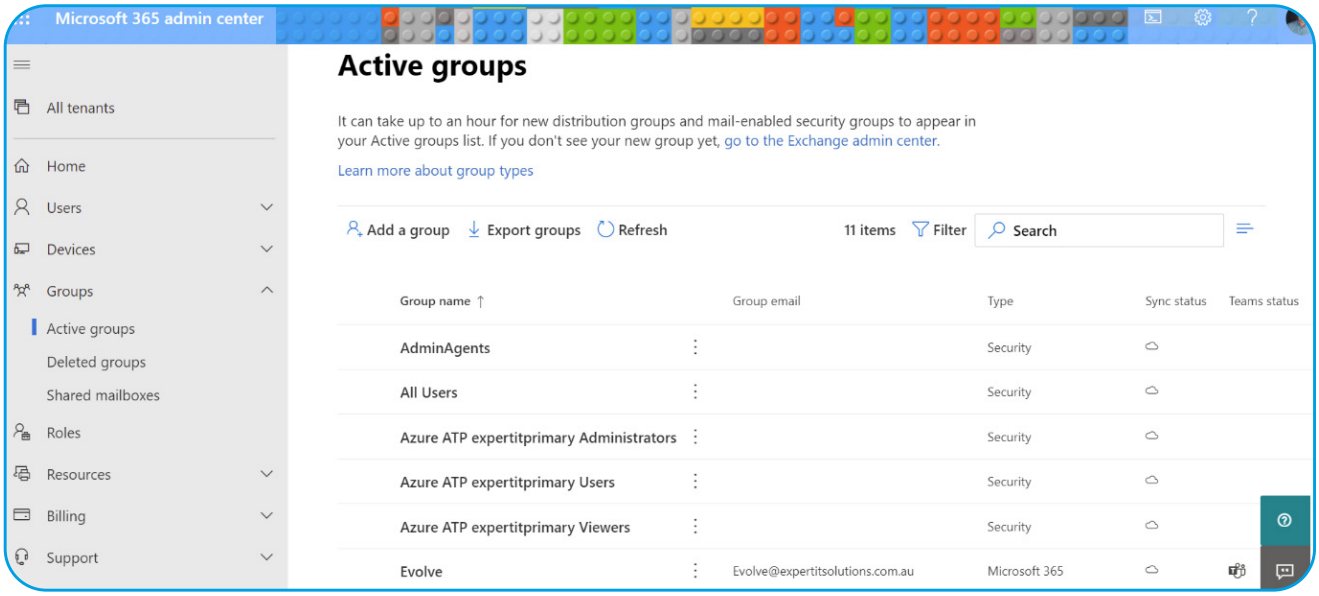
- **Grupos de Microsoft 365** (tratado en este capítulo)
- **Grupos de distribución** (capítulo 8)
- **Grupos de seguridad** que sirven para conceder acceso a recursos
- **Grupos de seguridad** con capacidad para correo que también sirven para conceder acceso y pueden enviarse por correo electrónico, lo que significa que todos los miembros recibirán una copia del mensaje.
- **Buzones compartidos** (capítulo 8)

Aunque puedes crear grupos de Microsoft 365 directamente, es más probable que interactúes con ellos como un elemento básico que proporciona una identidad única para todo M365 y que usan servicios como Teams, Yammer y otros. Además, Outlook puede utilizar los grupos de M365. Los sitios Modern Team de SharePoint se basan en ellos, y Stream y PowerBI los utilizan para controlar el acceso.

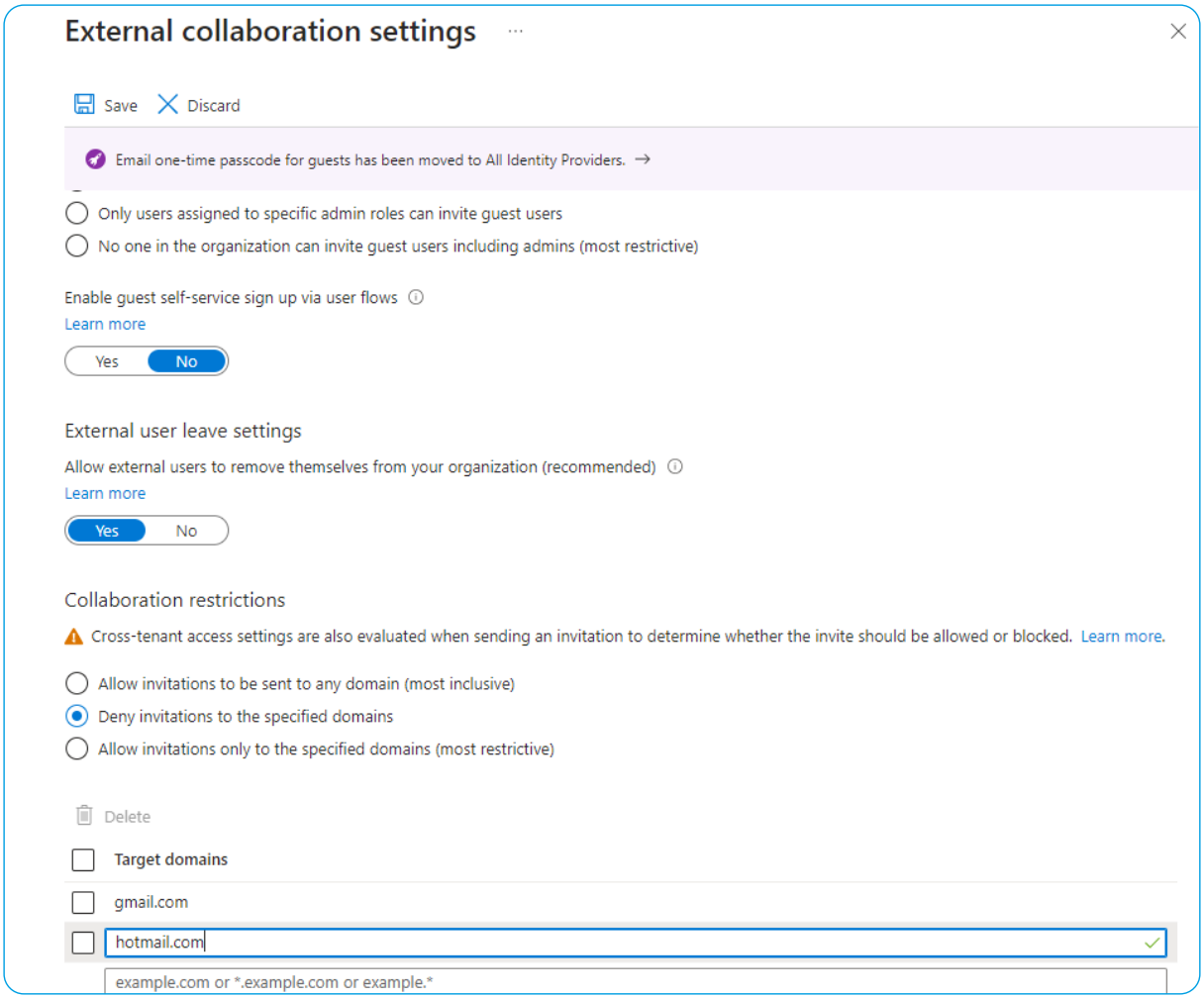
Si se configura de este modo, puedes escribir grupos de M365 en tu AD local, donde aparecen como grupos de distribución. Los grupos de M365 no pueden anidarse en otros grupos y solo pueden contener cuentas de usuario de M365 reales, mientras que los Grupos de distribución de Exchange pueden contener cuentas de usuario, usuarios de correo y contactos (consulta el Capítulo 8). A menos que hayas cambiado los valores predeterminados, cualquier usuario de tu tenant puede crear un grupo M365, lo que podría **dar lugar a problemas de gobernanza.** En lugar de esto, puedes **designar usuarios** con el permiso para crear grupos. También puedes usar varias **configuraciones de directivas** para controlar el comportamiento de grupo de O365 en tu tenant, como las **directivas de expiración** para gestionar el ciclo de vida de los grupos y puedes controlar la **nomenclatura de los grupos** a través de directivas.

Compartir contenido desde un grupo de M365 con usuarios externos es fácil. Además, los grupos de M365 son también un repositorio compartido de contenido histórico, ya que cualquiera que sea miembro puede ver todo el contenido que se remonta a cuando se creó el grupo por primera vez. Antes, cada usuario con licencia en tu tenant te proporcionaba cinco **licencias de invitado** B2B y podías utilizar **códigos de acceso de un solo uso** para los invitados externos que no tuvieran una cuenta de Google, una cuenta de Microsoft (MSA) o una cuenta en Azure AD.

Ese modelo de licencia para usuarios externos ha cambiado; Microsoft unificará Azure B2B y B2C (utilizando Azure como almacén de identidades de usuarios para tu aplicación desarrollada internamente) y el nuevo modelo de licencia significa que cada inquilino puede tener hasta 50.000 usuarios externos sin coste adicional. Ten en cuenta que, por defecto, los invitados tienen acceso total a todos los contenidos del grupo. Puedes **controlar de qué dominios** tienen que ser (o no pueden ser) los usuarios externos para disponer de acceso externo.



Grupos en el Centro de administración de M365



Configuración de Colaboración externa en Entra; bloqueo de dominios especificados

Ahora puedes crear un grupo **privado** para que los propietarios del grupo deban aprobar las solicitudes para unirse o puedes hacer un grupo **público** y cualquiera podrá unirse. Puedes cambiar la configuración predeterminada del tenant, lo que garantizará que los nuevos grupos sean públicos, o puedes cambiar la configuración de un grupo después de haberlo creado. Cada grupo puede tener hasta 100 propietarios y más de 1.000 usuarios; un usuario individual no puede crear más de 250 grupos. Al igual que otras estructuras de M365, tienes 30 días para **restaurar un grupo** una vez que se ha eliminado. Por su parte, los documentos individuales del grupo se alojan en la papelera de reciclaje de SharePoint durante 93 días.

Los **Grupos dinámicos** son una buena forma de reducir la sobrecarga administrativa de gestionar manualmente la pertenencia a grupos. Se basa en la consulta de atributos de Entra ID, aunque hay que tener en cuenta que requiere licencia Premium P1 de Entra ID.

CAPÍTULO 11:

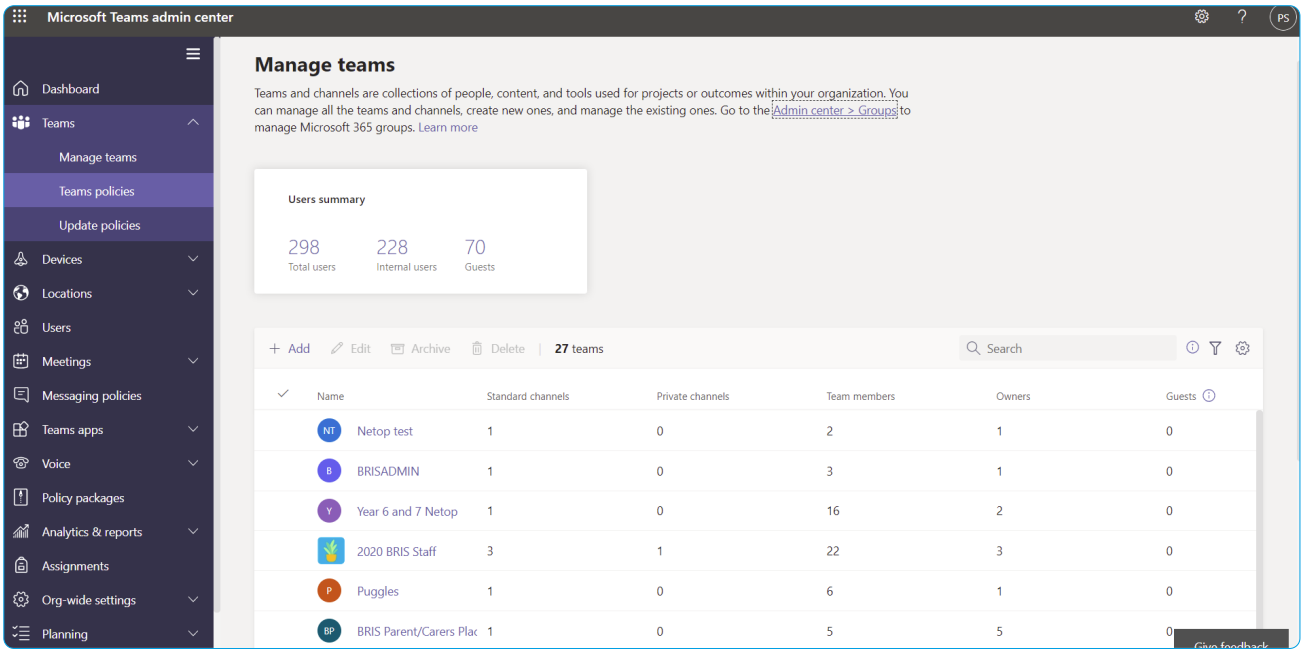
TEAMS

HA HABIDO MUCHAS APLICACIONES DE MENSAJERÍA INSTANTÁNEA/CHAT QUE HAN INTENTADO HACERSE CON LA COMUNICACIÓN EMPRESARIAL Y, SIN DUDA, TEAMS DE MICROSOFT ES LA MEJOR HASTA LA FECHA. ESTO LO FOMENTÓ EN GRAN PARTE LA PANDEMIA DE COVID-19, DURANTE LA CUAL EL USO DE TEAMS PASÓ DE 13 MILLONES DE USUARIOS ACTIVOS DIARIOS EN JULIO DE 2019 A MÁS DE 300 MILLONES (!) EN 2023. EN ESTE CAPÍTULO VEREMOS LO QUE TEAMS PUEDE HACER POR LAS COMUNICACIONES Y LA COLABORACIÓN DE TU EMPRESA.

11.1: ESTO ES TEAMS

Se está dedicando mucho desarrollo a Teams para garantizar que sea el mejor lugar para que grupos de personas trabajen juntos. La prueba más reciente es la **nueva aplicación cliente de Teams** (versión preliminar pública de marzo de 2023).

Un equipo de Teams **puede tener hasta 25.000 usuarios** pero, según mi experiencia, funciona mejor con equipos más pequeños (hasta unos cientos). Si organizas un seminario web de solo visualización, hay un límite de 20 000 asistentes. Existen aplicaciones cliente para Windows, MacOS (ambas actualizadas quincenalmente), iOS y Android, así como una interfaz basada en la web (actualizada semanalmente). Como muchas otras cosas de M365, hay dos componentes clave para una adopción satisfactoria: la parte técnica y la formación de los usuarios.



Centro de administración de Teams

Si tienes salas de conferencias, asegúrate de tener en cuenta la tecnología de la que las dotas. Las **Salas de Teams** son una forma eficaz de utilizar la tecnología para conectar al personal de la oficina con el que trabaja desde casa. Las Salas de Teams se dividen en Básico (gratuita, hasta 25 sistemas pueden tener este tipo de licencia) y Pro, que incorpora muchas **funciones adicionales de seguridad, comodidad y colaboración**. La antigua licencia Premium de Salas de Teams ha sido eliminada.

Hasta hace poco, solo existía la licencia de pago de Teams (como parte de la licencia de M365) y otra gratuita para equipos pequeños (que está en proceso de supresión). En febrero de 2023 pasó a estar disponible un nuevo nivel de licencias de pago denominado Teams Premium. Al igual que con cualquier conjunto de funciones de M365, es necesario evaluar cuidadosamente si las funciones adicionales podrían ser útiles a nivel empresarial para los usuarios para los que se adquiera la licencia (no todo el mundo necesita tener Teams Premium). Entre las **funciones premium** hay reuniones protegidas con marcas de agua en las grabaciones (con la dirección de correo electrónico de la persona que graba), etiquetas de sensibilidad para las reuniones y cifrado de extremo a extremo, así como plantillas y temas personalizados para las reuniones. Para los webinars hay muchas funciones adicionales que mejoran la experiencia general y, por último, las citas virtuales gestionan este tipo de reuniones, incluidas las notificaciones por SMS.

11.2: TEAMS PHONE

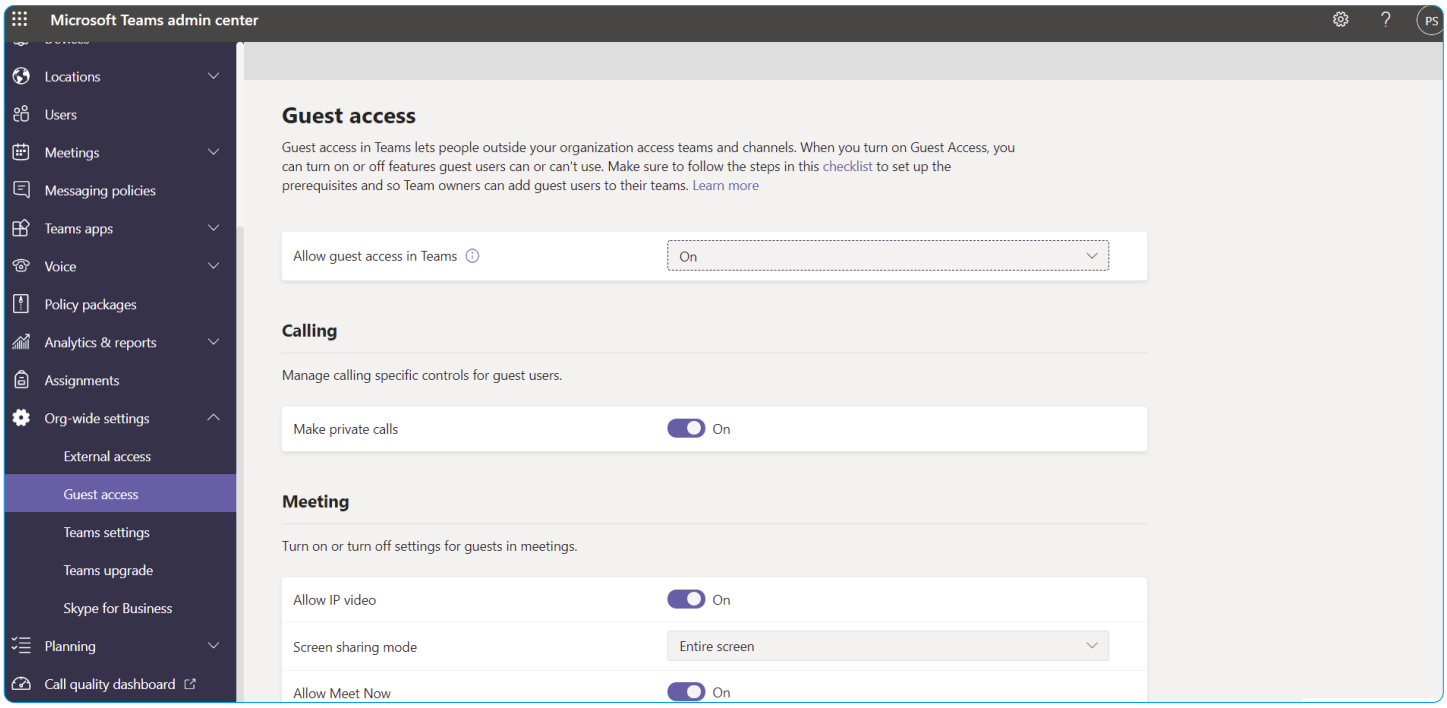
Una gran ventaja de Teams es que puede **conectarse** a la red telefónica conmutada (RTC), lo que permite a tus usuarios llamar a cualquier persona del mundo desde su cliente de Teams (en cualquier

plataforma) y tener un número de teléfono para que cualquier persona pueda llamarlos. Esta combinación de llamadas telefónicas externas, llamadas VOIP/videollamadas internas y reuniones por videoconferencia o webinars, facilidad en el **uso compartido de archivos y la coautoría**, además de mensajería instantánea asíncrona y chat es lo que ha convertido a Teams en el centro de colaboración y comunicación de facto en muchas empresas.

Hay varias opciones para conectarse y, dependiendo de tu ubicación geográfica en el mundo, no todas estarán disponibles. Puedes usar **Planes de llamadas**, en los que Microsoft será efectivamente tu proveedor de telecomunicaciones, u **Operator Connect** si tu actual empresa de telecomunicaciones participa en el programa y puede facilitar la conectividad. También está disponible **Phone Mobile**, en el que una empresa de telecomunicaciones existente utiliza números de teléfono móvil con SIM con Teams. Por último, con **Enrutamiento directo** conectas la infraestructura local a Teams. Asimismo, en los entornos más grandes puede que se use una combinación de varios.

11.3: GESTIÓN DE EQUIPOS

Tu interfaz principal es el **Portal de administración de Teams**, y dispones de un **módulo PowerShell**. Debajo de cada equipo hay un Grupo de M365 (capítulo 10) con los mensajes de chat almacenados en Azure table storage, los archivos compartidos en la biblioteca SharePoint del equipo en cuestión y los archivos personales en el OD4B de cada usuario. El buzón de voz y los calendarios se almacenan en los buzones Exchange de los usuarios y las grabaciones de las reuniones en Azure media services. Si tu



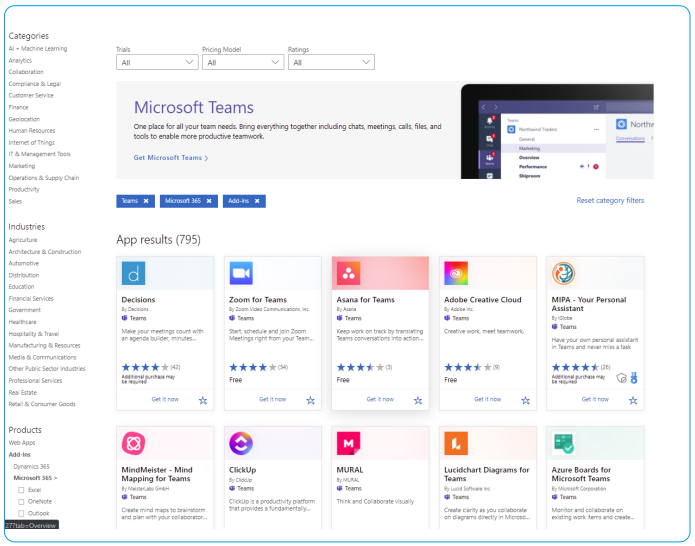
Configuración de acceso de invitados a Teams

empresa es grande, asegúrate de **planificar la gobernanza** de Teams al principio de la implementación. Consulta la **Configuración de acceso de invitados** a Teams de tu tenant para asegurarte de que en tu empresa haya un buen equilibrio entre seguridad y colaboración. Otra función útil es la posibilidad de utilizar **plantillas para la creación de equipos**, incluida la creación de plantillas personalizadas.

Cada equipo tiene un canal General por defecto, y puedes crear más canales para organizar las comunicaciones. Dentro de cada canal puedes añadir pestañas de Planner, OneNote, PowerBI, Stream, Wiki, sitios web y aplicaciones de terceros. Para limitar la proliferación de equipos en tu organización, puedes **limitar quién puede crear equipos** (por defecto, todos los usuarios pueden), así como utilizar **Canales privados en un equipo**. Por ejemplo, podrías tener un equipo para el departamento de ventas con un canal privado para que solo los jefes de ventas hablen de información confidencial.

También existe la posibilidad de **compartir un canal** con un usuario externo, en lugar de compartir todo un equipo. La principal ventaja para el usuario invitado es que puede iniciar sesión con su propia cuenta de tenant y acceder al chat y a los documentos del canal compartido sin necesidad de cerrar sesión y volver a iniciarla en Teams con su cuenta de invitado. Solo es posible crear un nuevo canal como canal compartido; no puedes convertir un canal normal en un canal compartido.

Es frecuente dar presentaciones en Teams. La **función PowerPoint Live** lo hace más interactivo, ya que permite a los asistentes interactuar con la presentación a su propio ritmo, y el **modo Presentador** ofrece un mayor control sobre el aspecto de la presentación para el público. Para practicar tus presentaciones (en PowerPoint en general), utiliza **Asesor para oradores**.



Complementos de terceros para Teams

Una función muy práctica son las **salas para subgrupos**, que te permite enviar o pedir a los usuarios que elijan «salas» en las que pueden colaborar con un subconjunto de usuarios de un equipo durante una reunión y volver a la reunión principal más tarde.

Las grabaciones de las reuniones de Teams (incluidas las **transcripciones**) antes se almacenaban en Stream. Ahora **se guardan en OD4B/SharePoint**, donde pueden compartirse fácilmente (incluso con asistentes externos). Un buen consejo es ser consciente de la caducidad por defecto de las grabaciones de las reuniones: 120 días. Puedes cambiarlo (para las grabaciones en tu tenant) en el Centro de administración de Teams - Reuniones - Directivas de reuniones - Grabación y transcripción. Hablando de transcripciones: si tienes Teams Premium, puedes activar los **subtítulos traducidos** para que una reunión emitida en inglés pueda verla un espectador alemán con subtítulos en su idioma y otro espectador pueda disponer de subtítulos en chino, por ejemplo.

11.4: USO DE TEAMS

Si estás acostumbrado a comunicarte por correo electrónico, aquí tienes algunas pautas para trabajar con eficacia en Teams. Usa las @menciones para llamar la atención de un miembro concreto del equipo, de un canal o de todo el equipo. Sé generoso con tus elogios cuando alguien haga algo bueno por el equipo y, si quieres agradecer un mensaje, simplemente dale a Me gusta, en lugar de aumentar el ruido con una respuesta escrita. Cuando vayas a publicar sobre algo, comprueba si ya existe un tema relacionado con ello y añádelo donde corresponda. Además, puedes usar los estilos de texto (o un GIF, sticker o meme) cuando quieras transmitir tu punto de vista y reacciones de tristeza, enfado o alegría para contribuir a la conversación cuando sea apropiado.

Puedes difuminar el fondo cuando estés en una reunión de vídeo o **sustituir la imagen de fondo** y, si tienes trabajadores de cara al público que necesiten comunicarse con otros, utiliza la función de pulsar para hablar **Walkie Talkie**. También puedes utilizar **un avatar** en lugar de tu imagen en vídeo. En esas reuniones del lunes por la mañana en las que no te has podido peinar, esto te ayudará a no aparecer hecho un cromo.

Teams **traducirá automáticamente los mensajes** en otros idiomas al idioma establecido en tu configuración personal. Y también hay **funciones sin conexión**; si no estás en línea, Teams guardará los mensajes que no hayas enviado y los enviará cuando vuelvas a estarlo.

Cuando estés en una reunión, puedes utilizar el **modo Juntos**, que mostrará el vídeo de cada participante como si todos estuvieran sentados en una sala de conferencias, con lo que desaparecerá el aspecto extraño de la cuadrícula tradicional de distintos vídeos.

11.5: VIVA

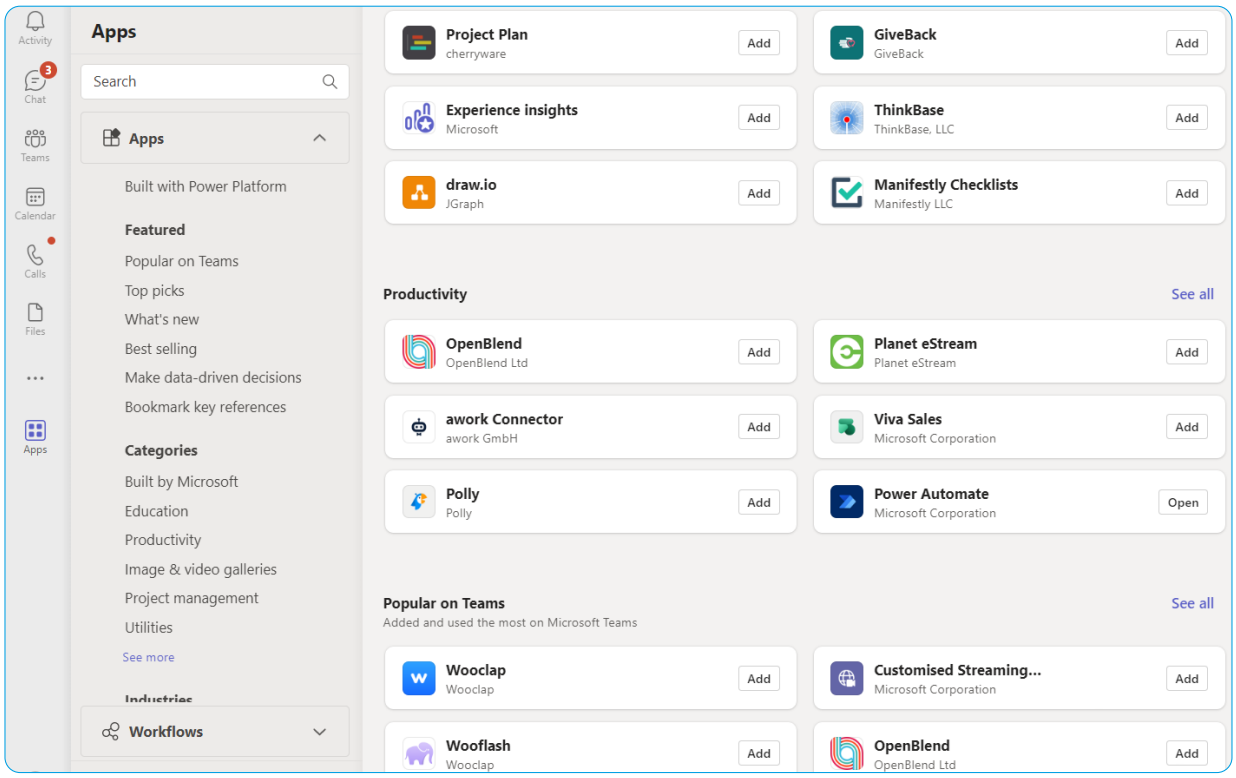
Si necesitabas otra prueba de lo importante que se ha convertido Teams para la visión y la hoja de ruta de Microsoft a nivel de colaboración y trabajo en el mundo actual, la tienes en la plataforma de experiencia del empleado (EXP) de **Viva**. Viva tiene ocho pilares, todos presentes en Teams: **Viva Connections** toma tu sitio de inicio de SharePoint Online, las aplicaciones de línea de negocio (LOB) y otras fuentes de noticias internas y te permite dirigir las noticias y conexiones de la empresa a las personas adecuadas. **Viva Insights** es la siguiente iteración de MyAnalytics para ayudar al personal a gestionar el tiempo y evitar el agotamiento, la integración con Headspace para meditaciones guiadas y una función de viaje virtual para concluir la jornada laboral. Los gestores disponen de una vista no identificada para ver cómo funciona un equipo desde el punto de vista del estrés, la salud mental y la productividad. También hay una vista de líderes para que los ejecutivos vean el estado general de su personal. El tercer pilar es **Viva Learning**, que ofrece **cursos de formación y contenidos de microaprendizaje** a la vez que se integra con **otros sistemas de gestión del aprendizaje** (Cornerstone OnDemand, Saba, SAP SuccessFactors y Workday) para hacer del aprendizaje una parte natural del trabajo diario de todos. Los gestores pueden programar cursos de formación y los miembros del personal pueden compartir entre ellos cursos que les parezcan especialmente buenos. Todos ellos están disponibles directamente en Teams. **Viva Topics** se basa en Cortex/Syntex y utiliza la IA para organizar el contenido de toda la empresa (proyectos internos, productos o acrónimos) y la experiencia del personal y mostrarlo como tarjetas o páginas temáticas en Teams, Microsoft Search, SharePoint y Office. Considéralo una Wikipedia de tu empresa.

Viva Goals aplica el poder del marco de objetivos y resultados clave (OKR) para ayudar al personal a seguir su progreso con respecto a las metas. Por otro lado, **Viva Engage** conecta a las personas de toda la organización (en realidad es el nuevo nombre de lo que antes era Yammer). El nuevo **Viva Sales** se integra con cualquier CRM (incluido, por supuesto, Microsoft Dynamics 365) para obtener una visión e implicación más profundas de los clientes. Y, por último, **Viva Pulse** (en versión preliminar pública en el momento de escribir estas líneas) ayuda a los líderes y gestores a recibir y actuar en función de los comentarios internos de una organización.

Como probablemente puedas deducir de estas breves descripciones, es probable que la mayoría de los módulos Viva encuentren su espacio en las grandes empresas, ya que es allí donde son más evidentes los retos de «gestión de personas» adaptándose a las necesidades.

11.6: EXPANSIÓN DE TEAMS

Otra potente función es **añadir aplicaciones** a Teams a través de Teams Store. Microsoft prueba y valida estas aplicaciones. Hay cientos de aplicaciones diferentes para integrarse con otras plataformas, aumentar la productividad, mejorar las reuniones, la gestión de las relaciones con los clientes (CRM) y mucho más. Una aplicación muy popular es **Microsoft Whiteboard**, gratis en todas las plataformas, que puedes utilizar tanto dentro de Teams como de forma independiente para intercambiar ideas y planificar en colaboración.



Teams Store con aplicaciones de terceros

Como administrador, tienes un control granular: puedes **permitir o bloquear aplicaciones**, **controlar los permisos** que se les da, **gestionar cómo las aplicaciones se ponen a disposición de los usuarios** y la capacidad de **informar sobre el uso de aplicaciones.** También puedes hacer que se desarrollen **aplicaciones a medida**.

Puedes **ampliar Teams aún más con bots** que pueden interactuar con tus usuarios de forma natural a través del chat o un bot de notificación que puede enviar información relevante a tus usuarios.

Con la llegada de Slack (el principal competidor de Teams) y Teams, mucha gente ha confirmado la muerte del correo electrónico. Como de costumbre, tendemos a ver la nueva tecnología como un sustituto directo de la antigua, mientras que la realidad tiene más matices. Teams me parece más eficaz para el trabajo en grupo. Supera al correo electrónico en el uso compartido de archivos y la comunicación, pero la comunicación fuera de los proyectos de clientes en los que participo sigue dependiendo del correo electrónico. Además, puedes utilizar el correo electrónico para enviar mensajes al canal de un equipo de Teams.

CAPÍTULO 12:

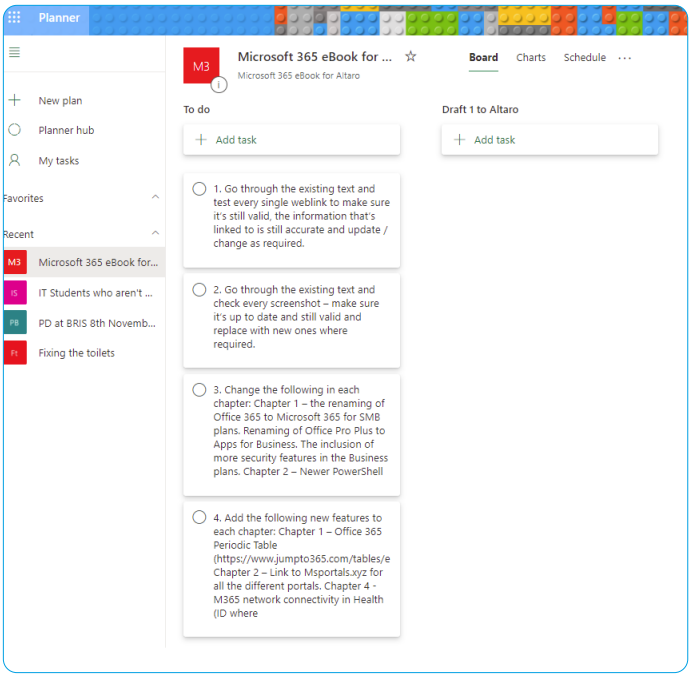
OTRAS APLICACIONES DE OFFICE 365

HAY MUCHAS OTRAS APLICACIONES Y SERVICIOS EN EL PORTFOLIO DE O365, Y EN ESTE CAPÍTULO VEREMOS ALGUNOS DE ELLOS CON UNA BREVE INTRODUCCIÓN.

12.1: PLANNER

Microsoft cuenta desde hace años con Project para la gestión de proyectos a gran escala, pero para las pequeñas y medianas empresas resulta excesivo (la curva de aprendizaje es muy pronunciada), y aquí es donde brilla Planner. Si alguna vez has utilizado Trello, deberías sentirte cómodo con el flujo de trabajo de Planner.

Hay una interfaz basada en web, para clientes iOS y Android, pero no para PC. Si añades una pestaña de Planner a un equipo, puedes crear un nuevo plan o adjuntar uno existente. Organiza las tareas en paquetes, asígnalas a distintas personas y controla el progreso de las mismas. Las tareas también pueden visualizarse en una vista de planificación (calendario), y es posible exportar un plan a Excel.



Un plan en Planner

Otras ofertas de gestión de tareas de Microsoft son To-Do (con clientes para móvil, web y PC), que se integra con las tareas de Outlook.

12.2: STREAM

Es la mejor forma de compartir **vídeos** dentro de tu empresa y es similar a YouTube. Hay clientes para iOS y Android y una interfaz web, pero actualmente no hay licencias para compartir vídeos con personas ajenas a tu tenant.

Cuando cargas un vídeo, se procesa y, si las personas que aparecen en él hablan inglés, chino, francés, alemán, italiano, japonés, portugués o español, **generará automáticamente subtítulos** con opción de búsqueda en Stream, lo que facilita encontrar el vídeo o el punto del vídeo concreto. También intentará reconocer a las personas que aparezcan en el vídeo y, si lo consigue, las incluirá en una lista en la información del vídeo. Antes Teams usaba Stream para almacenar las grabaciones de las reuniones, pero ahora se almacenan en OD4B/SharePoint.

12.3: KAIZALA

Se trata de una aplicación como Teams pero diseñada para trabajadores de cara al público/temporales con mala conectividad. Considérala una versión gestionada de WhatsApp.

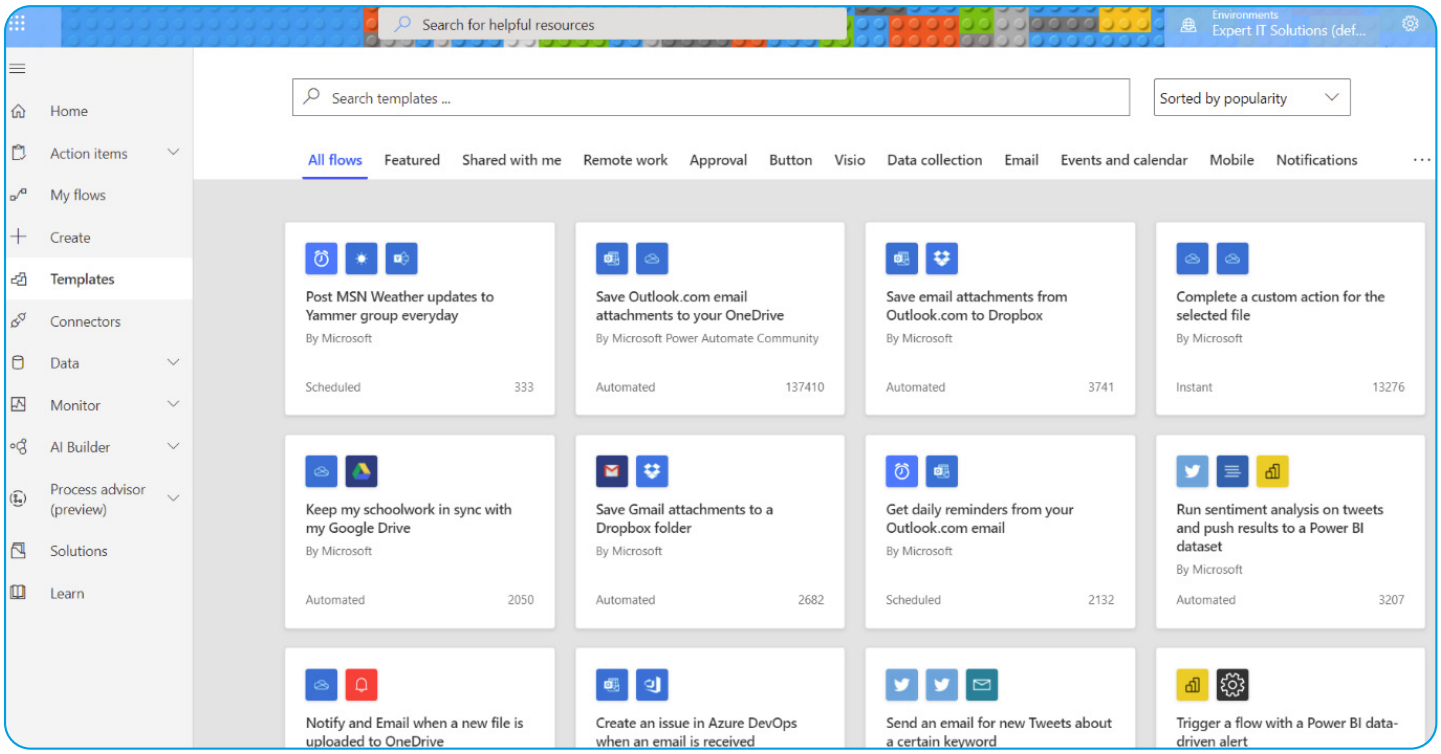
12.4: POWERBI

La visualización de datos es importante para cualquier empresa moderna que quiera estar basada en datos, y **PowerBI** es la respuesta de Microsoft. Hay un cliente de escritorio en el que se crean los cuadros de mando y también existe una interfaz web. Conseguir licencias **es un poco difícil** y va en función de lo que hayas construido y con quién quieras compartirlo.

Es muy divertida de usar y los resultados pueden ser muy útiles para muchos aspectos de tu negocio.

12.5: POWER AUTOMATE

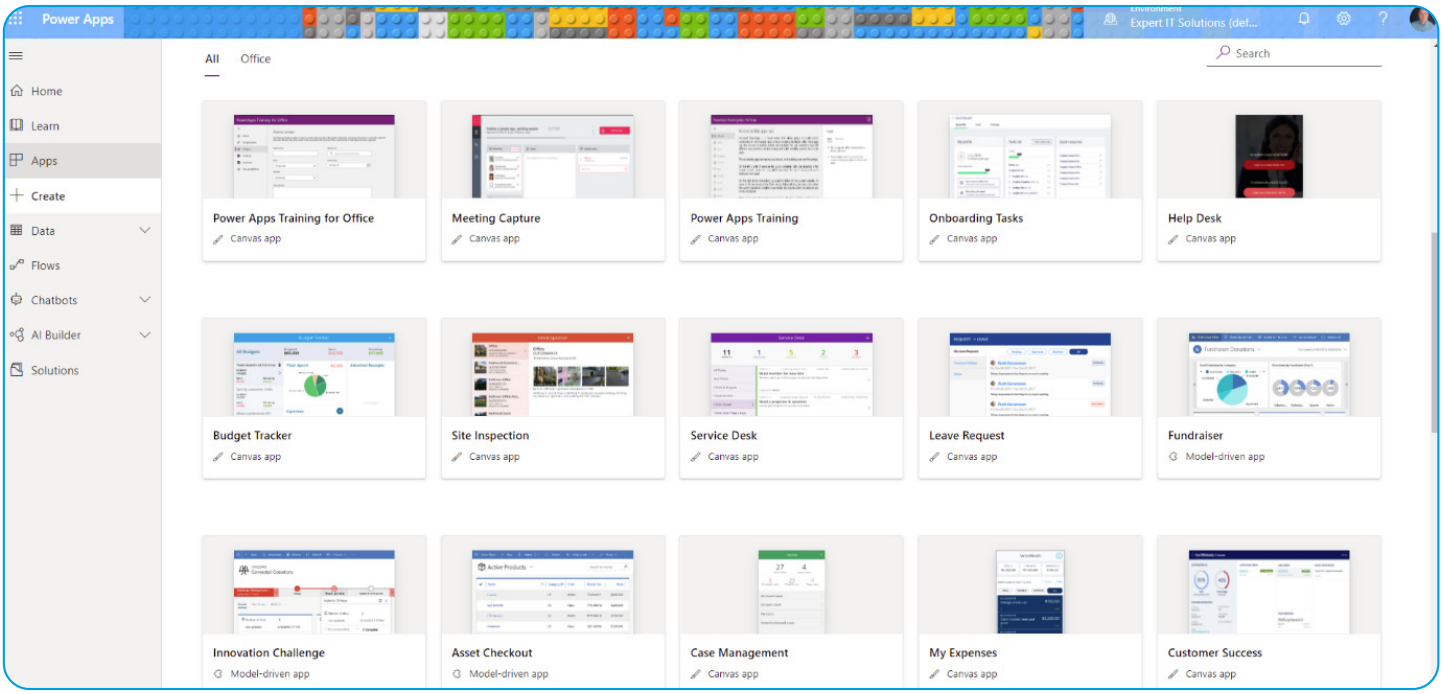
Esta herramienta web, aparentemente sencilla, está diseñada para automatizar tareas sin tener que escribir código (antes se llamaba Flow). Basta con arrastrar acciones, conectarlas a sistemas externos y programarlas para que se ejecuten regularmente o se activen a partir de un evento. Hay muchas plantillas que te ayudarán a empezar, así como conectores para acceder a Microsoft y a sistemas de terceros. Si has utilizado If This Then That o Zapier, te será fácil empezar a utilizar **Power Automate**.



Plantillas de Power Automate

12.6: POWERAPPS

¿Alguna vez has querido proporcionar a tu personal una aplicación móvil personalizada para recopilar o acceder a datos sobre el terreno y has visto que los costes de desarrollo eran demasiado elevados? **PowerApps** es la solución, ya que proporciona un entorno de desarrollo de bajo código/sin código para crear aplicaciones que se conectan a SharePoint, Excel, O365, Dynamics 365 o SQL server de forma local o en la nube; o la plataforma **Dataverse**. Las aplicaciones resultantes funcionan en iOS, Android, en un navegador web o en Teams y SharePoint Online. Si necesitas gestionar datos en tus aplicaciones, tienes **Dataverse** para Teams y la versión completa de Dataverse.



Plantillas de PowerApps

12.7: LISTAS MICROSOFT

Sí, el antiguo concepto de lista de SharePoint ha recibido un impulso gracias, entre otras cosas, a su **aplicación independiente** y también está disponible en Teams. Úsala para hacer un seguimiento de listas de «cosas» y gestionar información.

12.8: MICROSOFT LOOP

Loop es, posiblemente, la tecnología más confusa que Microsoft ha lanzado en los últimos años y ahora está en versión preliminar pública. La idea es bastante sencilla: tienes componentes de Loop que puedes incrustar en varias ubicaciones (como documentos, chats de Teams o un correo electrónico) para que siempre estén sincronizados en diferentes lugares. Las páginas de Loop permiten reunir componentes, enlaces, tareas y otros datos. Por último, los espacios de trabajo de Loop son espacios compartidos que reúnen páginas y componentes. Creo que Loop es más útil en las primeras fases de un proyecto o una idea: para hacer un brainstorming, trabajar con otros en un concepto y mantener todas las ideas en sintonía con todos los que trabajan contigo.

La dificultad actual es que, dado que el almacenamiento subyacente de los componentes de Loop está en el OneDrive para Empresas personal del usuario, compartir elementos fuera de una organización no funciona realmente, e incluso puede ser difícil dentro de un mismo tenant. Si Microsoft consigue resolver estas dificultades, Loop tiene un futuro interesante.

CAPÍTULO 13:

MICROSOFT INTUNE

M365 E3 Y E5 TE OFRECEN MICROSOFT INTUNE, EL SERVICIO EN LA NUBE DE ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES (MDM) DE MICROSOFT. EN ESTE CAPÍTULO VEREMOS CÓMO PUEDE AYUDARTE A GESTIONAR DISPOSITIVOS Y PCS, APLICACIONES MÓVILES, PROTEGER LOS DATOS DE LA EMPRESA Y APLICAR DIRECTIVAS DE SEGURIDAD.

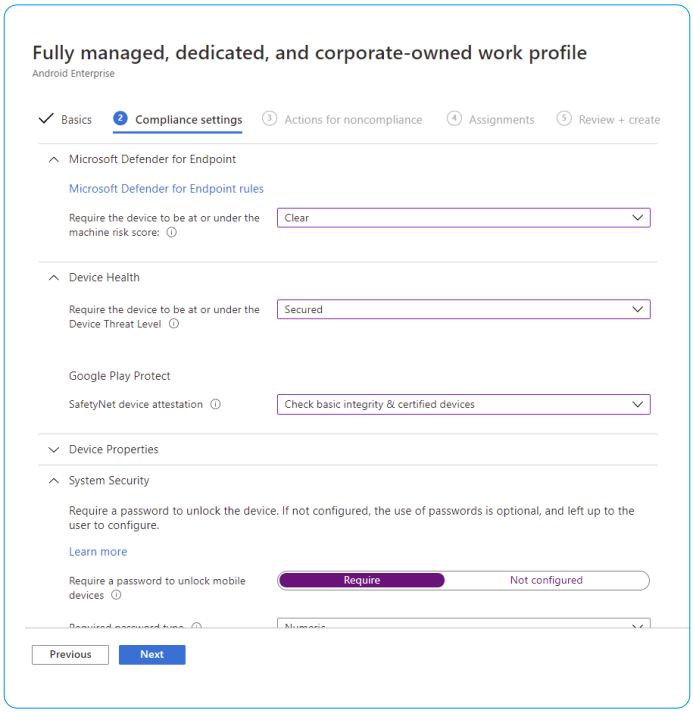
Antes existía un producto local llamado System Center Configuration Manager (SCCM), ahora denominado **Microsoft Configuration Manager,** que se puede integrar estrechamente con Intune.

Antes era necesario que los administradores de Intune tuvieran licencia de Intune, **pero ya no es así.** Una parte interesante de Intune es el **Análisis de puntos de conexión** que utiliza las señales de tus dispositivos para identificar los ordenadores problemáticos o lentos, y forma parte de la **puntuación general de adopción**.

Si tienes dispositivos Windows 10/11 que desempeñen funciones específicas (en una fábrica o en un puesto de enfermería de un hospital, por ejemplo), puedes utilizar Configuración en la nube para **administrarlos fácilmente en su totalidad mediante Intune**, con ajustes de configuración de referencia mediante secuencias de comandos.

13.1: ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES

Hay un par de formas de utilizar Intune: si tienes dispositivos (teléfonos inteligentes, tabletas, portátiles) propiedad de la empresa, puedes **inscribirlos en Intune**. Esto te da un gran control sobre el dispositivo, incluida la capacidad de gestionar los ajustes, las aplicaciones y la opción de borrar el dispositivo en caso de pérdida o robo. También puedes utilizar Intune para gestionar las actualizaciones del sistema operativo de los dispositivos Windows, distribuir aplicaciones a los dispositivos, configurar perfiles Wi-Fi e implementar certificados, así como bloquear dispositivos Android rooteados y con jailbreak de iOS.



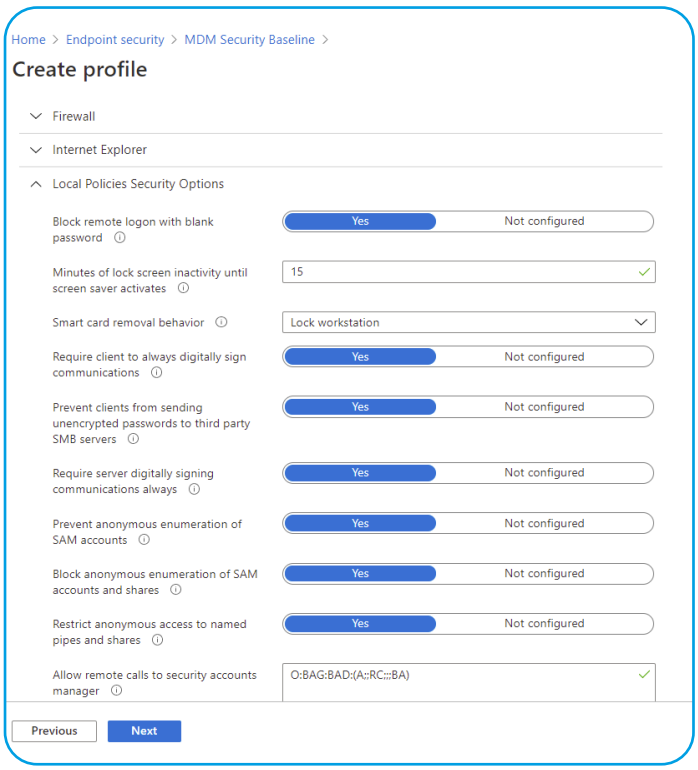
Directiva de cumplimiento de Android en Endpoint Manager

Si se trata de un dispositivo personal propiedad del empleado, es posible que éste no se sienta cómodo registrando el dispositivo, por lo que puedes utilizar la administración de aplicaciones móviles (MAM) para esos dispositivos.

13.2: ADMINISTRACIÓN DE APLICACIONES MÓVILES

Este enfoque menos intrusivo permite crear **directivas de protección de aplicaciones (APP)** en aplicaciones específicas, siendo el correo electrónico el ejemplo clásico. Los usuarios quieren acceder al correo electrónico de la empresa en su smartphone personal, por lo que se establecen políticas para que solo puedan utilizar Outlook (aplicación móvil gratuita para Android e iOS) pero no las aplicaciones de correo integradas, y se pueden proteger aún más los datos corporativos para que un usuario no pueda copiar datos de la empresa en una aplicación que no sea de la empresa (aplicación de correo electrónico personal, etc.). Si pierdes o te roban el dispositivo, puedes borrar los datos corporativos y dejar intactas las fotos personales, etc.

La elección entre MDM y MAM va a depender de muchos factores, como la base de usuarios, los contratos de trabajo, las necesidades empresariales y de seguridad, etc. Asegúrate de dedicar algo de tiempo a la **fase de planificación** para hacerlo bien. Otra parte de la gestión de aplicaciones móviles podría ser conectarlos de nuevo a los recursos locales de forma segura. Microsoft ahora proporciona **Tunnel**, su propia VPN para iOS y Android integrada en Microsoft Defender para Endpoint.



Referencia de seguridad de MDM

13.3: MICROSOFT CONFIGURATION MANAGER

Si has implementado MCM de forma local para gestionar tus servidores y PC cliente tradicionales, puedes integrar Intune en el flujo de gestión a través de la administración conjunta para aprovechar lo mejor de cada casa y preparar tu entorno para una migración gradual a la gestión en la nube. No lo confundas con MDM híbrida, que es el enfoque más antiguo y obsoleto de unir SCCM e Intune.

13.4: INTUNE SUITE

Al más puro estilo Microsoft, existen **complementos para Intune** que podrías valorar incorporar en tu empresa en caso de que te resuelvan un problema empresarial concreto. Hay complementos independientes, un plan Intune P2 y el paquete Intune completo, que incluye lo siguiente: **Análisis avanzados de puntos de conexión** para realizar un seguimiento y optimizar las experiencias de los usuarios finales, **Administración de privilegios de puntos de conexión**, que permite a los usuarios finales realizar ciertas tareas administrativas en su dispositivo Windows sin ser un administrador local, y **Microsoft Tunnel para MAM**, que amplía la función VPN por aplicación para aplicaciones Android e iOS a MAM. También existe **Ayuda remota**, que es una forma segura de permitir que el servicio de asistencia acceda a la pantalla de miembros del personal para ayudarles y **Administración de dispositivos especializados** como cascos AR/VR y dispositivos inteligentes de gran tamaño.

PARTE 3

SEGURIDAD, COPIA DE SEGURIDAD Y CUMPLIMIENTO

MICROSOFT 365
GUÍA ESENCIAL

CAPÍTULO 14:

SEGURIDAD EN O365

EN LOS INICIOS DE LA COMPUTACIÓN EN LA NUBE HABÍA MUCHA PREOCUPACIÓN POR LA SEGURIDAD DE LOS DATOS TRASLADADOS A UN «CENTRO DE DATOS AJENO». CREO QUE LA MAYORÍA DE LOS JEFES DE SEGURIDAD DE LA INFORMACIÓN (CISO) TIENEN CLARO HOY EN DÍA QUE LOS GRANDES PROVEEDORES PROPORCIONAN MÁS SEGURIDAD INFORMÁTICA QUE LA MAYORÍA DE LAS EMPRESAS, YA SEA POR PRESUPUESTO O POR OTROS MOTIVOS. TAMBIÉN TIENEN UN INCENTIVO CLARO: SI SE PRODUJERA UNA BRECHA IMPORTANTE, PODRÍA AFECTAR A MILES DE EMPRESAS, POR LO QUE INVIERTEN MUCHO DINERO EN ASEGURARSE DE QUE SUS NUBES SEAN LO MÁS SEGURAS POSIBLE.

Sin embargo, eso no significa que puedas dejarlo todo en manos de Microsoft; existe el **Modelo de responsabilidad compartida** y todos los proveedores de servicios en la nube tienen alguna versión de este modelo. Hay algunas áreas que siguen siendo responsabilidad tuya, como los puntos de conexión que tus usuarios utilizan para acceder a los servicios en la nube, cualquier infraestructura local que esté funcionando en modo híbrido con O365 y el aprovisionamiento y desaprovisionamiento de usuarios. También hay muchos controles de seguridad en O365 que debes personalizar para adaptarlos a tu empresa. En este punto, la seguridad es una responsabilidad compartida entre tú y Microsoft. En este capítulo veremos estos controles y dónde y cómo configurarlos.

La forma de concebir la seguridad debe ser de Confianza Cero. En lugar de confiar en una conexión en función de su procedencia («si está en la LAN interna es segura, si proviene del exterior es peligrosa»), cada acceso se comprueba con tus reglas de acceso condicional, lo que te proporciona un nivel de seguridad mucho mejor. Además, debes basar la seguridad en la identidad, que es el nuevo cortafuegos, y **estar al día de las novedades en el ámbito de la seguridad**.

Cuando pienses en cómo defender tus sistemas, ten siempre en cuenta que l**os atacantes se pueden desplazar de lo local a la nube**, como vimos en el **caso de Solarwinds**. Si dispones de una licencia M365 E5, puedes utilizar la formación de simulación de ataques para poner a prueba a tus usuarios con mensajes falsos de correo electrónico de phishing y proporcionarles automáticamente una miniformación en función de su propensión a caer en ellos. Si quieres un mayor control y optimización, prueba el **Servicio de concienciación sobre seguridad** de Hornetsecurity, que ofrece una evaluación comparativa totalmente automatizada, simulación de spear-phishing y formación en línea para sensibilizar y proteger a los empleados frente a las ciberamenazas.

No te olvides de Entra ID Premium P1 y P2, que puedes comprar como complementos de O365 (incluidos en M365). Hemos hablado de sus características de seguridad en el capítulo 7.

Se podría argumentar fácilmente que hay un conflicto de intereses si se confía en Microsoft tanto para proporcionar la plataforma (Office 365) como para ofrecer funciones de seguridad avanzadas de pago. Al fin y al cabo, Microsoft podría incluir más funciones de seguridad en la plataforma básica (Office 365 E3 y Microsoft 365 E3, por ejemplo), en lugar de cobrarlas aparte. Por ello, muchas empresas optan por un servicio de terceros para obtener servicios de seguridad avanzados además de la plataforma base, como 365 Total Protection de Hornetsecurity.

14.1: 365 TOTAL PROTECTION

365 Total Protection es una solución de seguridad basada en la nube que cubre todos los aspectos de la gestión de la seguridad y la protección de datos de Microsoft 365 de una organización: seguridad del correo electrónico, copia de seguridad y recuperación, cumplimiento, gestión de permisos y concienciación sobre la seguridad. La solución está específicamente desarrollada para Microsoft 365 y no requiere hardware, software ni mantenimiento, a la vez que proporciona capas muy necesarias de seguridad adicional y protección de datos contra spam, malware y amenazas avanzadas.

365 Total Protection de Hornetsecurity está disponible en cuatro planes:

1. **365 Total Protection Business** te ofrece seguridad de vanguardia para el correo electrónico, protección contra spam y malware, firmas y correo electrónico cifrado.
2. **365 Total Protection Enterprise** añade el archivo de correos electrónicos, conservación durante 10 años, eDiscovery, Protección contra amenazas avanzadas (ATP) mediante sandboxing de correos sospechosos, escaneo de URL y analizador de códigos QR.
3. **365 Total Protection Enterprise Backup** añade copia de seguridad automatizada de buzones de correo, Teams, OneDrive y SharePoint y recuperación sencilla, copia de seguridad y recuperación de puntos de conexión de Windows.
4. **365 Total Protection Compliance & Awareness** añade Permission Manager, Security Awareness Service y AI Recipient Validation.

Esta amplia gama de funciones de seguridad y cumplimiento para Microsoft 365 está disponible en **un solo paquete y en una sola licencia**.

14.2: ADMINISTRADOR DE PERMISOS 365

Uno de los tres pilares de la Confianza Cero, el uso del acceso del mínimo privilegio, es muy difícil de conseguir a gran escala. Esto es particularmente evidente en SharePoint y OneDrive, donde no solo tienes un complejo conjunto de opciones de permisos superpuestos, sino también el intercambio de archivos y sitios con usuarios externos, ya sea a través de SharePoint, OneDrive, y ahora también con frecuencia a través de Teams.

Para inventariar todos estos permisos que se han concedido e informar sobre ellos es necesario navegar por varias pantallas o ejecutar comandos de PowerShell. Tampoco existe una forma sencilla de dimensionar correctamente los permisos cuando son demasiado amplios, ni una manera rápida de revocar los permisos en todos los sitios cuando se descubre, por ejemplo, que una cuenta de usuario ha estado en peligro.

365 Permission Manager, un producto único de Hornetsecurity, palía todos estos problemas y más. Un panel centralizado te muestra todos tus sitios y el grado de cumplimiento de tus directivas de uso compartido. Para dimensionar correctamente el tamaño de los permisos, usa el botón Corregir o, en caso de que la empresa necesite una excepción a la política, Aprobar un caso especial. Las políticas integradas o personalizadas que controlan el uso compartido externo, el uso compartido interno y la configuración asociada pueden aplicarse a sitios individuales de SharePoint o ubicaciones de OneDrive, lo que mejora considerablemente la gobernanza y la gestión de riesgos.

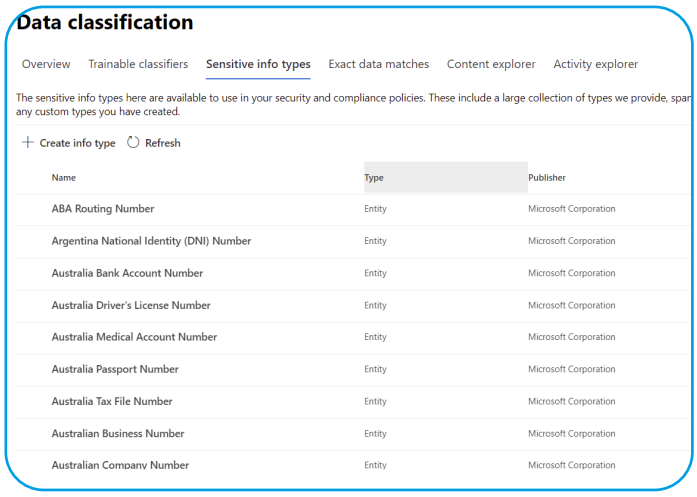
También puedes ver los permisos en SharePoint, OneDrive y Teams de un usuario seleccionado, lo que resulta muy útil cuando se sospecha que una cuenta está en peligro, o quizás en el caso de una investigación de riesgos internos.

Otra función muy útil son las Acciones rápidas, que te permiten realizar acciones en masa para gestionar los permisos y mantener una infraestructura de SharePoint, Teams y OneDrive conforme a la normativa.

14.3: MICROSOFT PURVIEW INFORMATION PROTECTION

Todas las funciones de gobernanza, prevención de pérdida de datos (DLP) y protección de la información de M365 se engloban en Purview, cuyo portal se encuentra en **compliance.microsoft.com**.

El uso de **etiquetas para clasificar los datos,** ya sea de forma manual o automática mediante el rastreo de documentos o correos electrónicos, te permite empezar a controlar la información de tu empresa. Una vez etiquetado un documento, puedes utilizar MIP u OME para protegerlo (véase más abajo), o controlar el acceso en puntos de conexión de Windows mediante directivas, así como gestionar el acceso en Office para Mac, Windows, iOS y Android.



Tipos de información confidencial (SIT)

14.4 : MICROSOFT INFORMATION PROTECTION

Una de las funciones más potentes y menos utilizadas es la posibilidad de proteger los documentos, estén donde estén. El uso compartido tradicional de archivos y documentos de SharePoint controlaba estrictamente el acceso a nivel de servidor, pero en cuanto un documento se envía por correo electrónico a alguien o se almacena en una unidad USB, se pierde ese control.

Microsoft Information Protection (MIP) te permite configurar etiquetas y reglas para cifrar los documentos y que lleven consigo su acceso de usuario para que, independientemente de cómo se compartan, solo tengan acceso las personas adecuadas. Si te estás iniciando en MIP, utilizarás el cliente integrado en las aplicaciones de Office para Windows, Mac, iOS y Android. Es importante configurar **cuentas de superusuario** para poder acceder a los documentos cuando un usuario abandone la empresa. La lista de tipos de información confidencial (TIS) es cada vez más larga y ahora es posible personalizar los niveles de confianza de las reglas, copiar las incorporadas y personalizarlas y crear diccionarios de palabras clave más amplios (captar cada mención de una etiqueta de identificación de un miembro del personal o el número de registro de un paciente).

Es posible **ser coautor de documentos protegidos en tiempo real** (¡con posibilidad de Autoguardado!). En implementaciones más grandes se pueden utilizar variables en las reglas del MIP para facilitar el marcado de contenidos por aplicación. Puedes aplicar etiquetas (y, opcionalmente, cifrado de documentos) a documentos, sitios en línea de SharePoint y usos compartidos de archivos y SharePoint de forma local. También puedes escanear imágenes utilizando el **reconocimiento óptico de caracteres (OCR)** para detectar información confidencial en capturas de pantalla y elementos similares.

Las etiquetas de material confidencial ahora también están disponibles para los **sitios de SharePoint, los grupos de M365 y Teams**. Esto no se aplica al contenido almacenado en esas ubicaciones, sino que gestiona la privacidad del contenedor, el acceso de usuarios externos y también puede integrarse con directivas de acceso condicional para bloquear el acceso desde dispositivos no gestionados, por ejemplo. No obstante, puedes configurar una **etiqueta de material confidencial predeterminada para un sitio de SharePoint**.

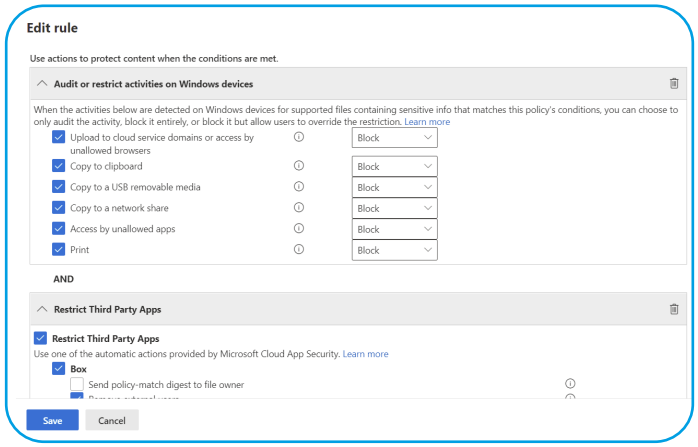
14.5: CIFRADO DE MENSAJES DE OFFICE 365

De manera similar a cómo MIP te permite compartir documentos protegidos con cualquier persona, puedes utilizar el **Cifrado de mensajes de O365** para enviar correos electrónicos a cualquier persona y saber que solo esa persona puede acceder a ese correo electrónico. Al igual que con MIP, también puedes establecer reglas para que los correos electrónicos con información específica (números de tarjetas de crédito, números de la seguridad social...) se cifren automáticamente.

14.6: PREVENCIÓN DE PÉRDIDA DE DATOS

El objetivo de la **prevención de pérdida de datos (DLP)** es ayudar a los usuarios a hacer lo correcto alertándoles cuando estén a punto de compartir datos confidenciales a través del correo electrónico, SharePoint Online, OD4B o Teams. También puede integrarse con MIP a medida que Microsoft termina de unificar el etiquetado y la protección a través de M365. La protección DLP se ha ampliado a Windows 10 y 11 con **DLP de punto de conexión**, que puede bloquear la subida de documentos con contenido confidencial al almacenamiento en la nube, la copia

de información confidencial en el portapapeles, el almacenamiento USB, los recursos compartidos de red o la impresión. También existe una extensión para Google Chrome que amplía la protección DLP a las tareas del navegador. La DLP también **se ha ampliado a las instalaciones locales** utilizando el Analizador MIP para encontrar documentos confidenciales y la gestión de alertas de infracciones de la DLP también se ha mejorado enormemente.

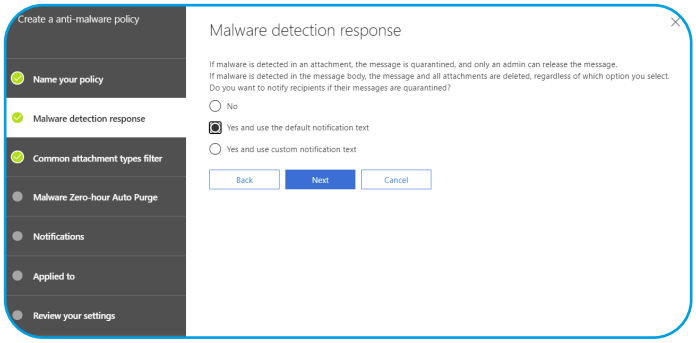


Configuración de DLP de punto de conexión

14.7: EXCHANGE ONLINE PROTECTION

Exchange Online Protection (EOP) es la solución de higiene del correo para Office 365 y también puede proteger tus buzones de Exchange locales si tienes una implementación híbrida (capítulo 8). Hay varios ajustes de EOP que puedes controlar, así como algunas configuraciones adicionales que deberías tener en cuenta para una protección completa contra el spam, como **Marco de directivas de remitente (SPF)**, **Autenticación, informes y conformidad de mensajes basados en dominio (DMARC)** y **Domain Keys Identified Mail (DKIM).**

Si consideras que EOP no intercepta suficientes correos maliciosos, Hornetsecurity ofrece una herramienta gratuita llamada **Threat Monitor** (no requiere cambios en tus registros MX) que identificará correos publicitarios (spam), amenazas y correos con amenazas avanzadas y también te permitirá eliminarlos de los buzones de correo de los usuarios. Threat Monitor proporciona valiosos datos estadísticos sobre el correo electrónico para que tu tenant sepa lo que le falta a EOP, lo que facilita la decisión de actualizar los servicios de higiene del correo electrónico.



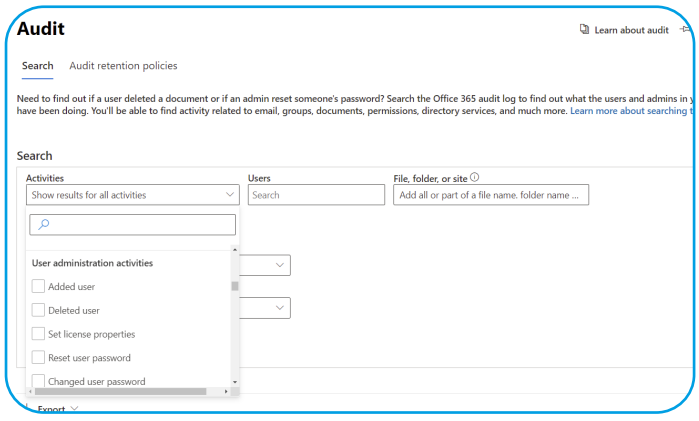
14.8: DEFENDER PARA OFFICE 365

Las **protecciones** de Defender para O365 (disponibles en O365 E5 o como complementos independientes) se basan en EOP y ofrecen la función **Datos adjuntos seguros**, gracias a la cual los archivos adjuntos de los correos electrónicos entrantes que podrían ser maliciosos se abren en una máquina virtual y se comprueban antes de entregarlos a los usuarios finales. **Enlaces seguros** comprueba que los enlaces de los correos electrónicos y los archivos de Office no sean maliciosos en el momento en que los usuarios hacen clic en ellos. **Anti-phishing** detecta los intentos de suplantación de usuarios. Estas protecciones también se extienden a SharePoint, OD4B y Teams.

Si Defender para Office 365 te parece demasiado caro (está incluido en M365 E5, E5 Security o como complemento independiente), echa un vistazo al producto de Hornetsecurity, disponible en versión Business y Enterprise. La versión Business te ofrece un control granular sobre las categorías y el contenido de los correos electrónicos para que puedas bloquear los correos no deseados. Puedes establecer firmas de correo electrónico con declinación de responsabilidades de la empresa y utilizar PGP o S/MIME para cifrar el correo electrónico, con gestión de certificados integrada. La versión Enterprise añade archivo y registro diario de correo electrónico con una retención de hasta 10 años, eDiscovery y análisis en sandbox de archivos adjuntos, reescritura y análisis de URL (tanto en correos electrónicos como en archivos adjuntos) y Cobertura de contingencias a través de un entorno de conmutación por error de correo electrónico cuando Microsoft 365 esté fuera de servicio.

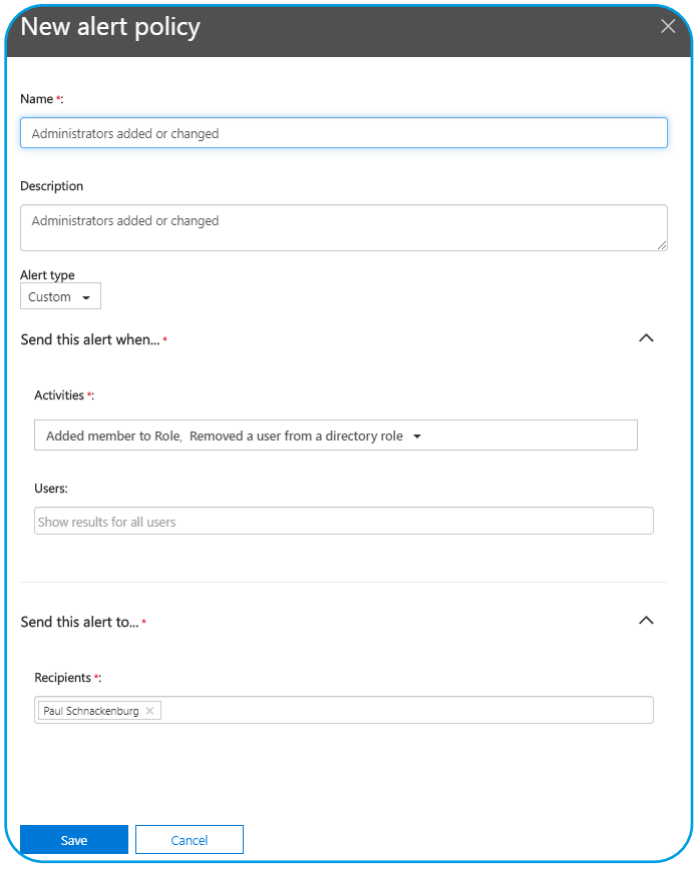
14.9: AUDITORÍA

Una de las mejores características de la plataforma unificada de O365 es la posibilidad de **auditar las acciones de usuarios y administradores** en toda la plataforma.



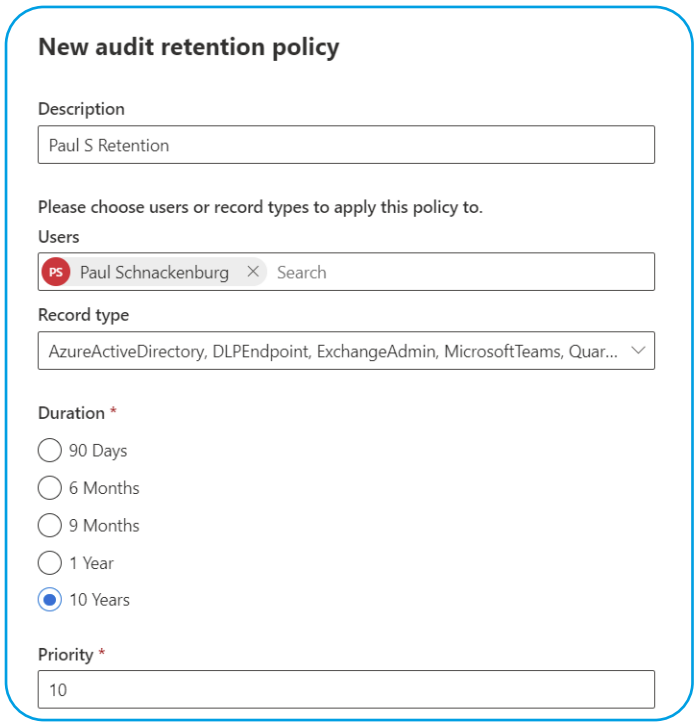
Búsqueda de registros de auditoría

Lo mínimo que necesitarás es **configurar alertas** para las acciones de Entra ID. Para ello, ve el portal de Cumplimiento - Búsqueda - Búsqueda de registros de auditoría y consulta todas las diferentes actividades para las que puedes **crear Directivas de alertas**, auditar y notificar.



Creación de una Directiva de alertas

Por defecto, los registros de auditoría de Office 365 se guardan durante 180 días (Entra ID los guarda durante 30 días), lo que puede no ser suficiente para tu negocio o para las normativas que debas cumplir. Tienes dos opciones: utilizar un servicio de terceros para exportar continuamente los registros y archivarlos durante el periodo de tiempo que necesites o bien asignar licencias M365 E5 (o M365 E5 Cumplimiento / eDiscovery y auditoría) a los usuarios cuyos registros quieras conservar durante más tiempo. Esto permite la posibilidad de conservar los registros durante 1 o 10 años.



Directiva de retención de auditorías

14.10: ¿ADIÓS A LAS CONTRASEÑAS?

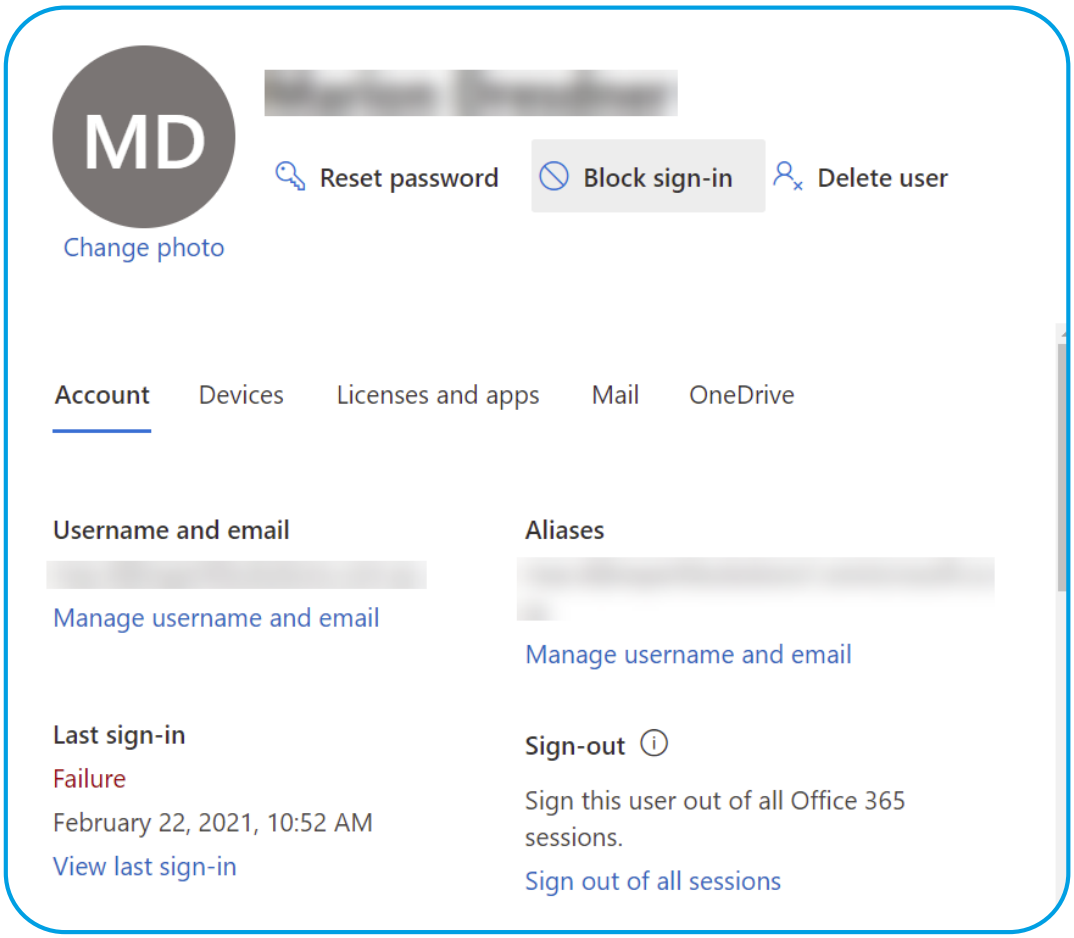
En última instancia, la mejor forma de gestionar las contraseñas es no almacenar ninguna en el directorio y que los usuarios no las utilicen; es lo que se llama el uso sin contraseñas. Hay **muchos pasos en el camino hacia este objetivo final**. Hoy en día se puede utilizar la aplicación Authenticator para iniciar sesión en una cuenta de Azure AD (no como segundo factor, sino como el factor único) o Windows Hello para empresas o una llave USB/NFC de hardware FIDO 2.
Mientras tanto, activa la **Protección de contraseñas** para prohibir las contraseñas más utilizadas (2000 en una lista mantenida por Microsoft, más hasta 1000 palabras personalizadas comunes en tu organización/ciudad/equipos deportivos). Esto funciona a la perfección para cuentas solo en la nube y puede **ampliarse fácilmente a AD local**.

Si solicitas a tus usuarios que registren una MFA, **al mismo tiempo** registrarán el restablecimiento de contraseña de autoservicio.

14.11: BLOQUEAR ACCESO DE USUARIOS

Si sospechas o confirmas que una cuenta de usuario ha estado en peligro, el primer paso debe ser desactivar el inicio de sesión de la cuenta en el Centro de administración.

Sin embargo, debes tener en cuenta que el usuario (o el atacante) no se desconecta inmediatamente de los servicios a los que accede, y que puede pasar hasta una hora hasta que el bloqueo surta efecto debido a la duración de los tokens de actualización. La solución a este problema es la **Evaluación continua de acceso**, que actualmente solo se aplica a la conectividad en línea de Exchange, Teams y SharePoint, y que bloquea el acceso casi en tiempo real (ocasionalmente hasta 15 minutos de latencia debido a la propagación de eventos).



Bloquear el inicio de sesión de una cuenta de usuario

CAPÍTULO 15:

SEGURIDAD EN MICROSOFT 365

HAY MUCHAS HERRAMIENTAS DE SEGURIDAD INTEGRADAS EN LA PLATAFORMA O365, PERO SI CAMBIAS A M365 E3 O E5 ACCEDERÁS A UNA NUEVA GAMA DE FUNCIONES AVANZADAS PARA PROTEGER TU EMPRESA. EN ESTE CAPÍTULO VAMOS A VER ESTAS HERRAMIENTAS, EXCEPTO ENDPOINT MANAGER, QUE TRATAREMOS EN EL PRÓXIMO CAPÍTULO, Y WINDOWS 11, QUE YA HEMOS VISTO EN EL CAPÍTULO 6.

15.1: MICROSOFT 365 DEFENDER

Casi todos los productos de seguridad de Microsoft centrados en M365 llevan la marca Defender, y la consola central para trabajar con ellos es **security.microsoft.com**. Aquí encontrarás un completo servicio de detección y respuesta ampliadas (XDR) que recopila datos de correo electrónico, identidad, puntos de conexión y servicios en la nube, y te alerta de intrusos en todo tu entorno M365.

Aquí tienes un resumen de los diferentes servicios de Defender:

- **Microsoft Defender para Office 365** – Proporciona protección para correos electrónicos, sitios de SharePoint, OD4B y Teams
- **Microsoft Defender for Identity** – Supervisa tu Active Directory (AD) local, se integra con tu herramienta de gestión de información y eventos de seguridad (SIEM) y te alerta de las infracciones de cuentas, los movimientos laterales y los ataques que afecten a AD.
- **Microsoft Defender para puntos de conexión** – Gestión centralizada del antimalware en todos los puntos de conexión de tu entorno (Windows, Linux, macOS, Android e iOS).
- **Microsoft Defender for Cloud Apps** – Un agente de seguridad de acceso a la nube (CASB) que añade funciones para adaptarse a la palabra de moda del momento, la **gestión del nivel de seguridad de las aplicaciones SaaS**.

Microsoft también ofrece Microsoft Sentinel, un SIEM basado en la nube; Microsoft Defender for Cloud (para cargas de trabajo de Azure, AWS y GCP IaaS y PaaS) y Entra (para la gestión y protección de identidades).

15.2: MICROSOFT DEFENDER PARA PUNTOS DE CONEXIÓN

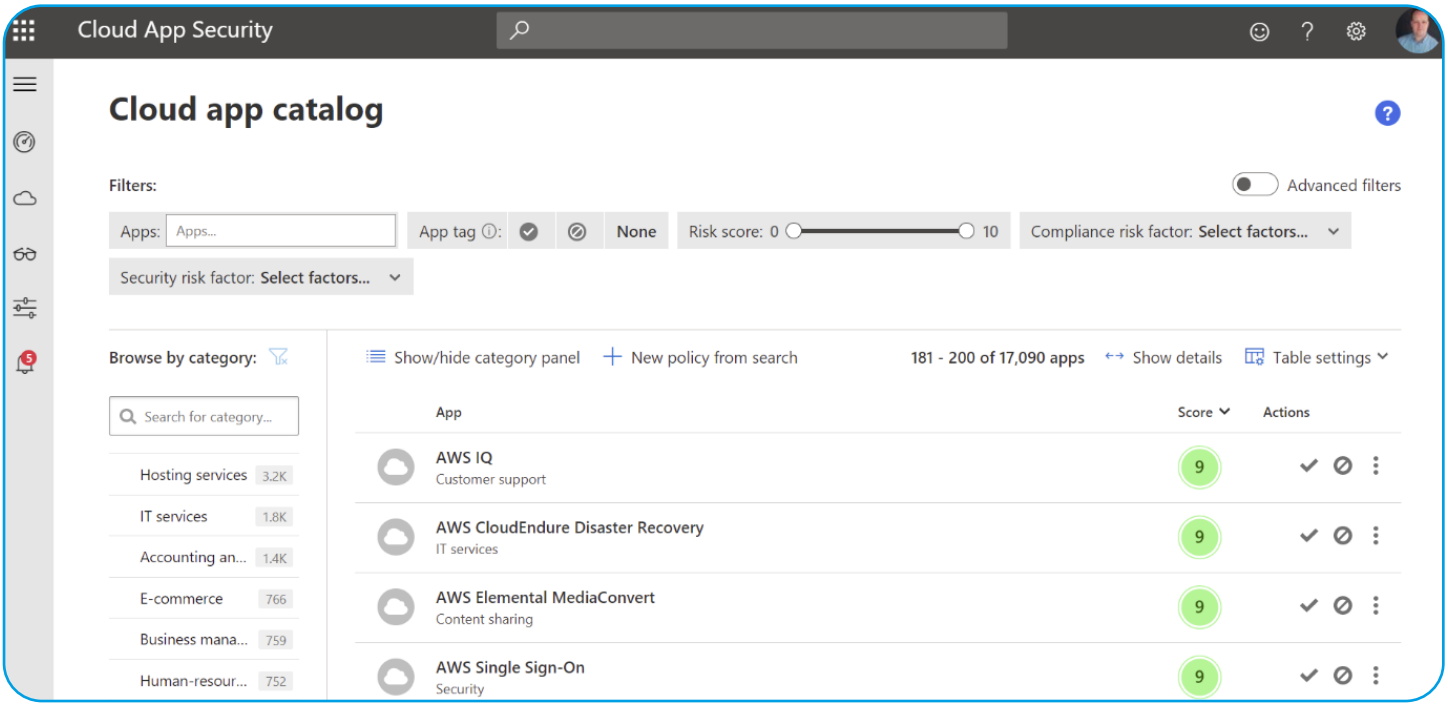
Microsoft Defender para puntos de conexión (MDE) es una solución completa de seguridad de detección y respuesta en puntos de conexión (EDR) que utiliza el análisis de comportamiento de aprendizaje automático (ML) para Windows, MacOS, servidores Linux y dispositivos iOS y Android. Cataloga las aplicaciones instaladas (Windows y MacOS) y, a través de la **gestión de amenazas y vulnerabilidades (TVM)**, prioriza las aplicaciones que entrañan los riesgos más graves para tu organización en función del grado de implementación de cada aplicación y de la gravedad de la vulnerabilidad revelada. MDE también proporciona **reglas de reducción de la superficie de ataque y protección de última generación**, junto con muchas otras características de seguridad. MDE está disponible con M365 E5 / E5 Security o como licencia independiente.

15.3: MICROSOFT DEFENDER FOR IDENTITY

Con M365 E5 puedes pasar a **Defender for Identity (MDI)**, que supervisa los controladores de dominio de Active Directory y los servidores de federación de Active Directory con agentes ligeros; del resto se encarga el servicio en la nube. Cualquier atacante que establezca un punto de apoyo en un dispositivo de tu red debe tocar AD para moverse lateralmente y escalar privilegios y MDI los interceptará cuando lo haga.

15.4: MICROSOFT DEFENDER PARA APLICACIONES EN LA NUBE

Antes, cuando los usuarios permanecían en la oficina corporativa, lo único necesario para protegerlos era un buen cortafuegos, pero en el mundo actual de «trabajo en cualquier lugar, en cualquier dispositivo» se necesita un nuevo tipo de herramienta para protegerlos, un agente de seguridad de acceso a la nube. Microsoft Defender for Cloud Apps (MDA) forma parte de M365 E5 y protege a sus usuarios en tiempo real cuando acceden a los servicios en la nube. Este catálogo de más de 31 000 servicios diferentes en la nube ofrece al departamento de TI una forma de descubrir y gestionar la TI paralela (servicios en la nube que los usuarios han aprovisionado sin que el departamento de TI lo sepa) en toda tu base de usuarios.

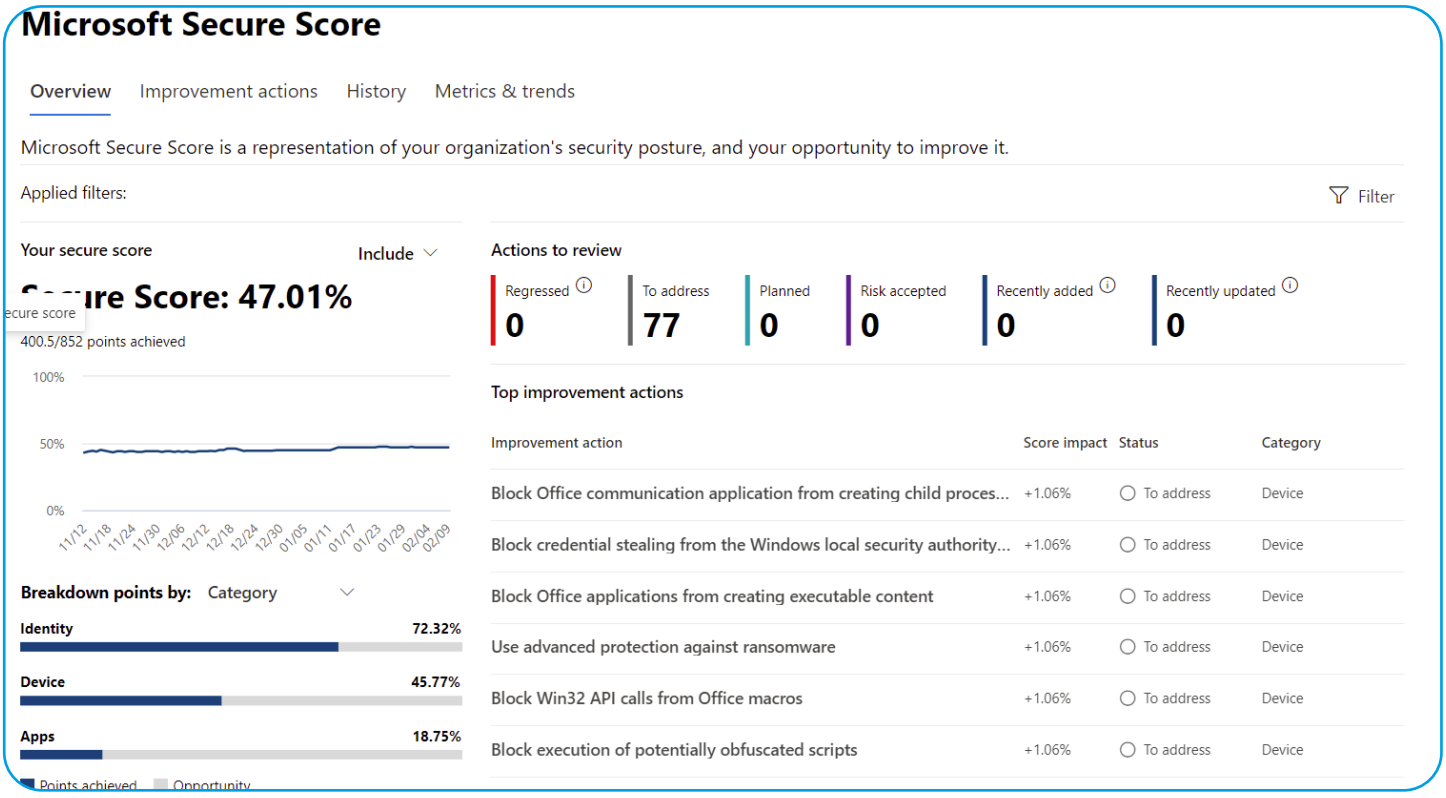


Catálogo SaaS de seguridad de aplicaciones en la nube

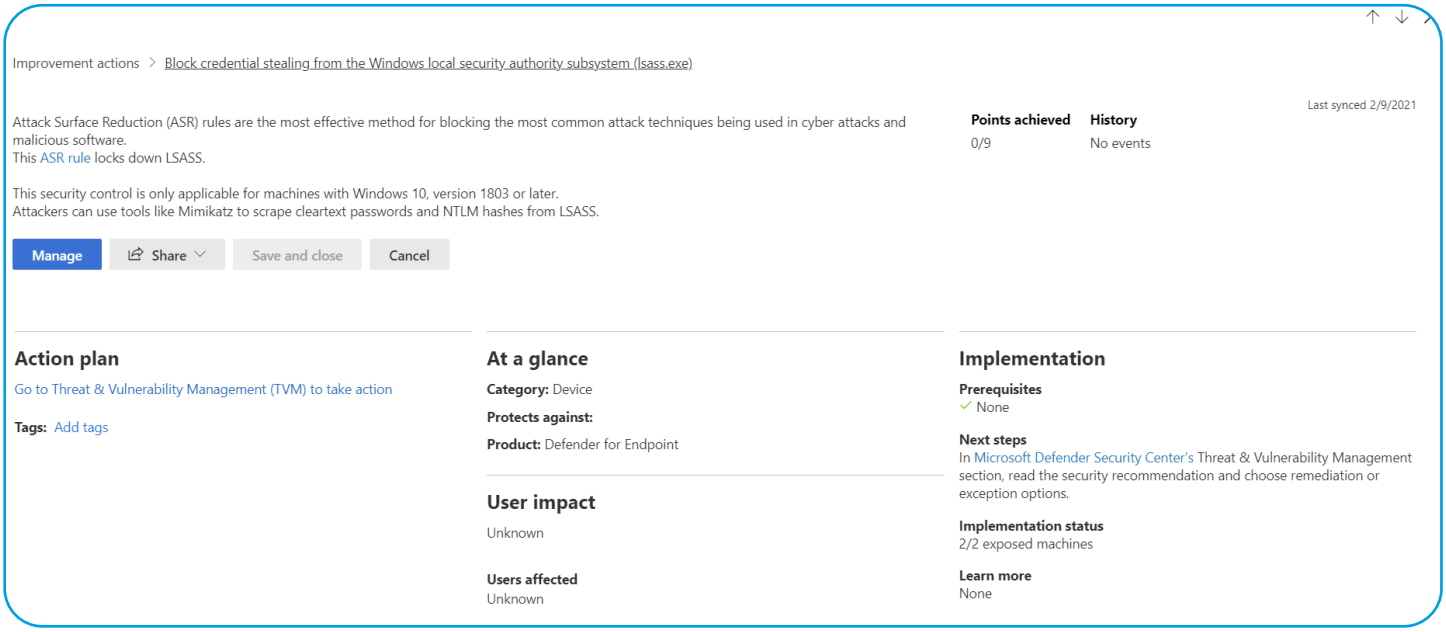
15.5: PUNTUACIÓN DE SEGURIDAD

En el último capítulo y en este hemos visto muchos de los controles de seguridad que puedes utilizar. Pero ¿por dónde se empieza? ¿Cómo puedes saber qué es lo más importante a tener en cuenta? ¿Y dónde hay que ir en los distintos portales (o PowerShell) para configurar cada ajuste?

Las respuestas a estas preguntas se encuentran en Puntuación de seguridad, que ahora forma parte del **portal Seguridad**, donde puedes ver una puntuación global de tu tenant (referente a controles de Identidad / Datos / Dispositivos / Aplicaciones e Infraestructura) y compararla con la media global de M365, la media de tu sector y la de empresas del mismo tamaño. En la segunda pestaña están las acciones que debes emprender para mejorar la puntuación, cuántos puntos te dará cada acción y el impacto en el usuario y el esfuerzo administrativo que requiere.



Visión general de la Puntuación de seguridad



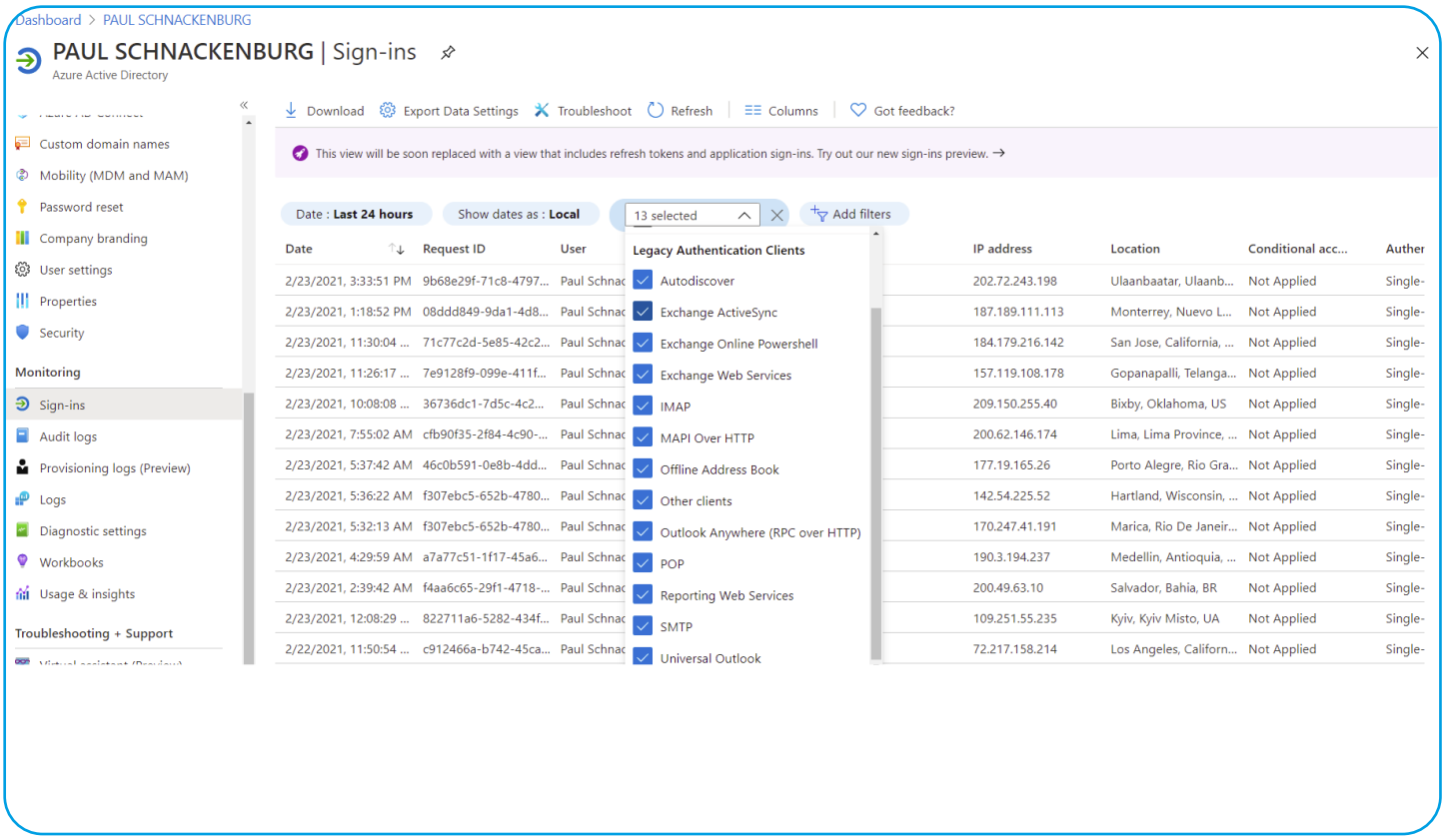
Ejemplo de acción para mejorar la seguridad

Al hacer clic en una acción se obtienen detalles sobre qué riesgos mitiga el control, a qué normativa de cumplimiento se ajusta, la posibilidad de hacer clic en un botón para ir directamente a la zona adecuada para configurarlo y la opción de indicar al sistema que ya ha mitigado este riesgo con un servicio de terceros.

A medida que implementas más controles, tu puntuación aumenta (puede tardar entre 24 y 48 horas), y puedes hacer un seguimiento de tu progreso en la pestaña Historial. Puntuación de seguridad es el MEJOR lugar para empezar a mejorar el nivel de seguridad de tu tenant.

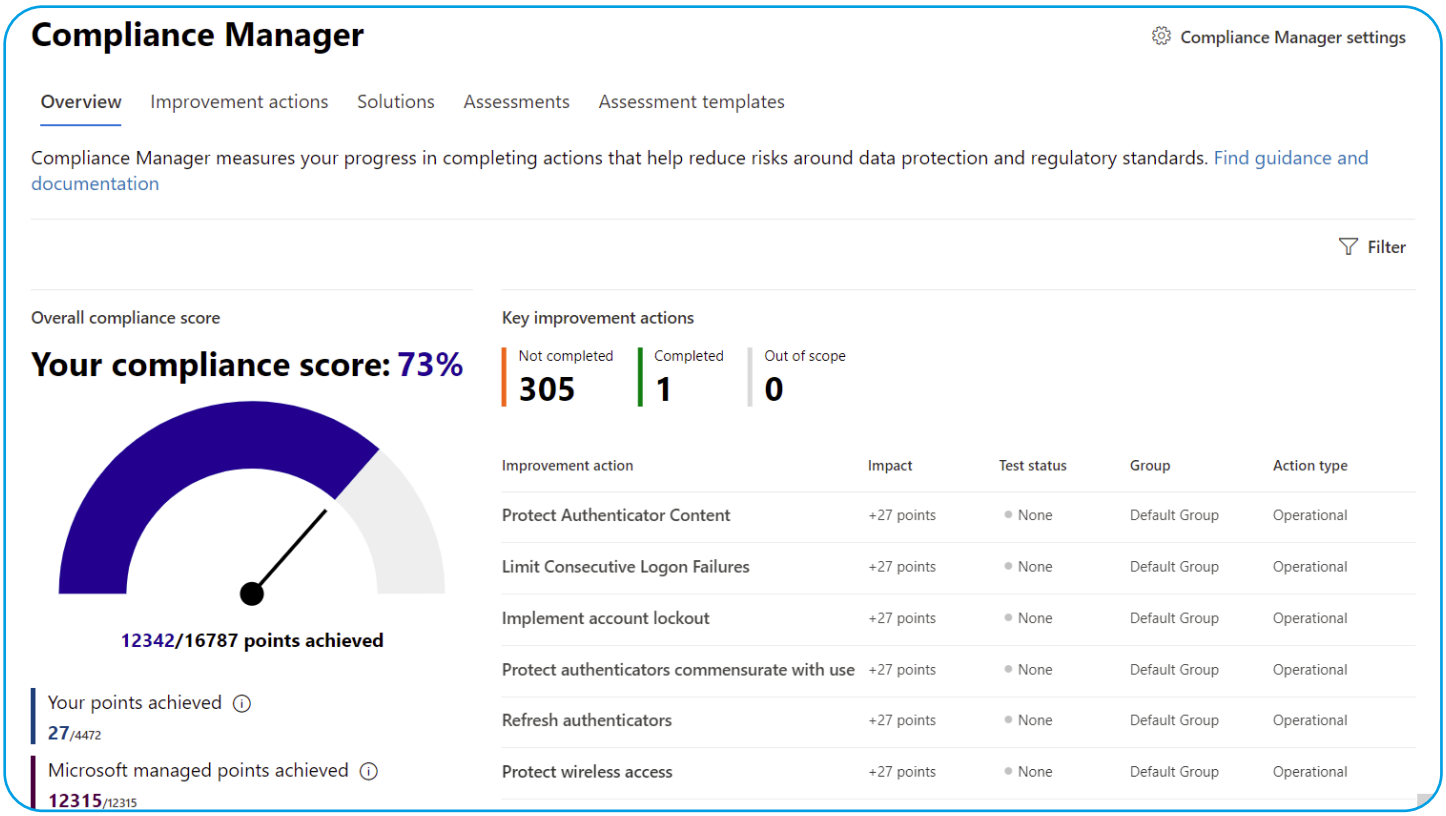
Me gustaría destacar otro control (aparte de la MFA) que te permitirá mejorar rápidamente la seguridad general: el **bloqueo de la autenticación heredada**. Esto se debe a que, incluso si has activado la MFA, los atacantes pueden seguir accediendo a las cuentas de tus usuarios con solo un nombre de usuario y una contraseña a través de protocolos más antiguos incompatibles con la MFA. Para investigar si existen conexiones legítimas que utilicen estos protocolos antiguos (que deberán actualizarse o quedar exentas de tu directiva de bloqueo de autenticación heredada), ve al portal de Azure AD, haz clic en Inicios de sesión en supervisión, haz clic en Añadir filtros y elige Aplicación cliente. A continuación, haz clic en «No seleccionar ninguno» y añade las 13 opciones de conexión heredada.
Aquí se puede ver un tenant con la MFA activada y la autenticación heredada aún activa con numerosos intentos de acceso fallidos.

Si estás seguro de que no hay necesidades legítimas de autenticación heredada, usa **directivas de CA para bloquearla.**



Intentos de inicio de sesión en Entra ID mediante autenticación heredada

El concepto de la Puntuación de seguridad se ha extendido a otras partes de M365, en el **Administrador de cumplimiento** existe la Puntuación de cumplimiento para indicar el grado de cumplimiento de tu empresa con los marcos normativos que debes cumplir. Hace poco que Microsoft ha añadido cientos de normativas adicionales de todo el mundo para ayudarte a realizar un seguimiento de tu cumplimiento y asignar tareas a los usuarios para lograr y mantener el cumplimiento.



Puntuación de cumplimiento en el Administrador de cumplimiento

La gestión del cumplimiento de tus sitios de SharePoint y OneDrive y tu nivel de seguridad/configuración de uso compartido utilizando las herramientas integradas es una fuente de desesperación, ya que están repartidas por varios portales. En cambio, **365 Permission Manager** de Hornetsecurity proporciona un único panel para ver la configuración de cada sitio de tu tenant, aplicar políticas, corregir infracciones de cumplimiento, ver todos los accesos que tiene un usuario concreto, elaborar informes y mucho más.

15.6: LA SEGURIDAD ES RESPONSABILIDAD DE TODOS

Los dos últimos capítulos te han dado una visión general de alto nivel de las muchas características de seguridad disponibles en M365. La triste realidad es que la mayoría de las pequeñas y medianas empresas no implementan ni de lejos las funciones que ya han pagado, e incluso las grandes empresas tienen dificultades para implantar estas protecciones para todos sus usuarios.

Esto se debe en parte a la complejidad inherente de muchas de las funciones de seguridad nativas de Microsoft. Recuerda el dicho: «la complejidad es enemiga de la seguridad». Es por eso que muchas organizaciones recurren a soluciones de seguridad de terceros, como Hornetsecurity, para que les ayuden a hacer más accesibles las principales funciones de seguridad y a reducir la complejidad.

Por otra parte, descuidar la seguridad también se debe a una cierta dejadez, que se deriva del hecho de que en muchas empresas todavía prevalece una mentalidad de la era local (on-premise), en la que se pensaba que (casi) todo contaba con un cortafuegos y las tiendas de informática se encargaban de ello.

Hoy en día el mundo es distinto: debemos comprender que la responsabilidad de la seguridad está en manos de cada uno de nosotros y que nuestra cadena de ciberdefensa solo puede ser tan fuerte como su eslabón más débil.

Estudia la posibilidad de impartir formación sobre concienciación en seguridad a los empleados, ya que es esencial para reducir el riesgo de ciberataques, evitar la filtración de datos y garantizar EstEstudia la posibilidad de impartir formación sobre concienciación en seguridad a los empleados, ya que es esencial para reducir el riesgo de ciberataques, evitar la filtración de datos y garantizar el cumplimiento de la normativa. Capacita a los empleados para reconocer y afrontar amenazas a la seguridad fomentando una sólida cultura de ciberseguridad y protegiendo tanto los activos como la reputación de la empresa. En última instancia, invertir en formación de concienciación supone un ahorro de costes y un entorno digital más seguro.

15.7: PRESERVAMOS LA HONRADEZ DE MICROSOFT

Si la idea de pagar la propia plataforma de Microsoft y luego tener que pagar las funciones de seguridad adicionales no te satisface, considera una solución de terceros para tus necesidades de seguridad y cumplimiento de M365. Hornetsecurity ofrece **distintos planes** con una potente protección avanzada contra amenazas para tu correo electrónico, prevención de pérdida de datos (DLP), servicio de concienciación en seguridad (simulación y formación de phishing para usuarios finales), cifrado de correo electrónico, archivo de correo electrónico y mucho más.

Hornetsecurity también ofrece un libro electrónico gratuito completo centrado en la seguridad de un tenant de Microsoft 365, **The Microsoft 365 Security Checklist.** Trata de todos los ajustes de seguridad y configuraciones que debes conocer para cada licencia de M365 para asegurar adecuadamente tu entorno y profundiza más en las configuraciones concretas que este libro.

CAPÍTULO 16:

COPIA DE SEGURIDAD EN MICROSOFT 365

EN ESTE CAPÍTULO ANALIZAMOS LA NECESIDAD DE PROTECCIÓN DE DATOS EN MICROSOFT 365: DE QUÉ ES RESPONSABLE MICROSOFT Y DE QUÉ ES RESPONSABLE TU ORGANIZACIÓN.

16.1: RESILIENCIA DE DATOS NATIVA

Como cualquier servicio en la nube, Microsoft se toma muy en serio la disponibilidad de los datos de los clientes en M365. Como ya se ha dicho, **los buzones de Exchange tienen cuatro copias**, tres actualizadas y una cuarta retrasada (24 horas). Esta última copia se usa en caso de corrupción sistémica de las otras tres copias. Estas cuatro copias se distribuyen en, al menos, dos centros de datos. Todo esto lo gestiona automáticamente el sistema y los usuarios finales no se percatan de ello.

Del mismo modo, **el almacenamiento de SharePoint y OneDrive para Empresas depende de que los datos se almacenen en dos regiones de Azure separadas**: una escritura solo se considerará completada si se escribe correctamente en ambas regiones. Y el almacenamiento subyacente utiliza Solo anexar, lo que garantiza que los datos anteriores no puedan ser corrompidos o cifrados por un atacante. Esta creación de versiones también permite restaurar versiones anteriores de los archivos.

Suena bien, ¿no? Como es obvio que Microsoft hace cosas para proteger mis datos, ¿no tengo que preocuparme? No tan rápido: todo lo descrito anteriormente tiene que ver con la resiliencia de los datos y su alta disponibilidad. Lo que no proporciona, aparte de algunas opciones limitadas, son copias de seguridad de tus datos.

Las copias de seguridad son copias de los datos de producción, en un sistema independiente, que se copian regularmente (cada hora, cada día) de los datos de producción a la ubicación de la copia de seguridad. Esto proporciona las funciones siguientes:

- La capacidad de «retroceder en el tiempo» y restaurar correos electrónicos/documentos/buzones/sitios a un punto anterior en el tiempo, ya sea a una ubicación de producción o a una ubicación de exportación independiente.

- La capacidad de acceder a tus datos de producción en caso de fallo catastrófico o interrupción de los servicios en Microsoft 365.

En otras palabras, la resiliencia de datos o la alta disponibilidad no son lo mismo que las copias de seguridad. Guardan relación, pero tienen fines distintos. Dependiendo de las necesidades de tu empresa o de la normativa que debas cumplir, es posible que necesites ambas cosas.

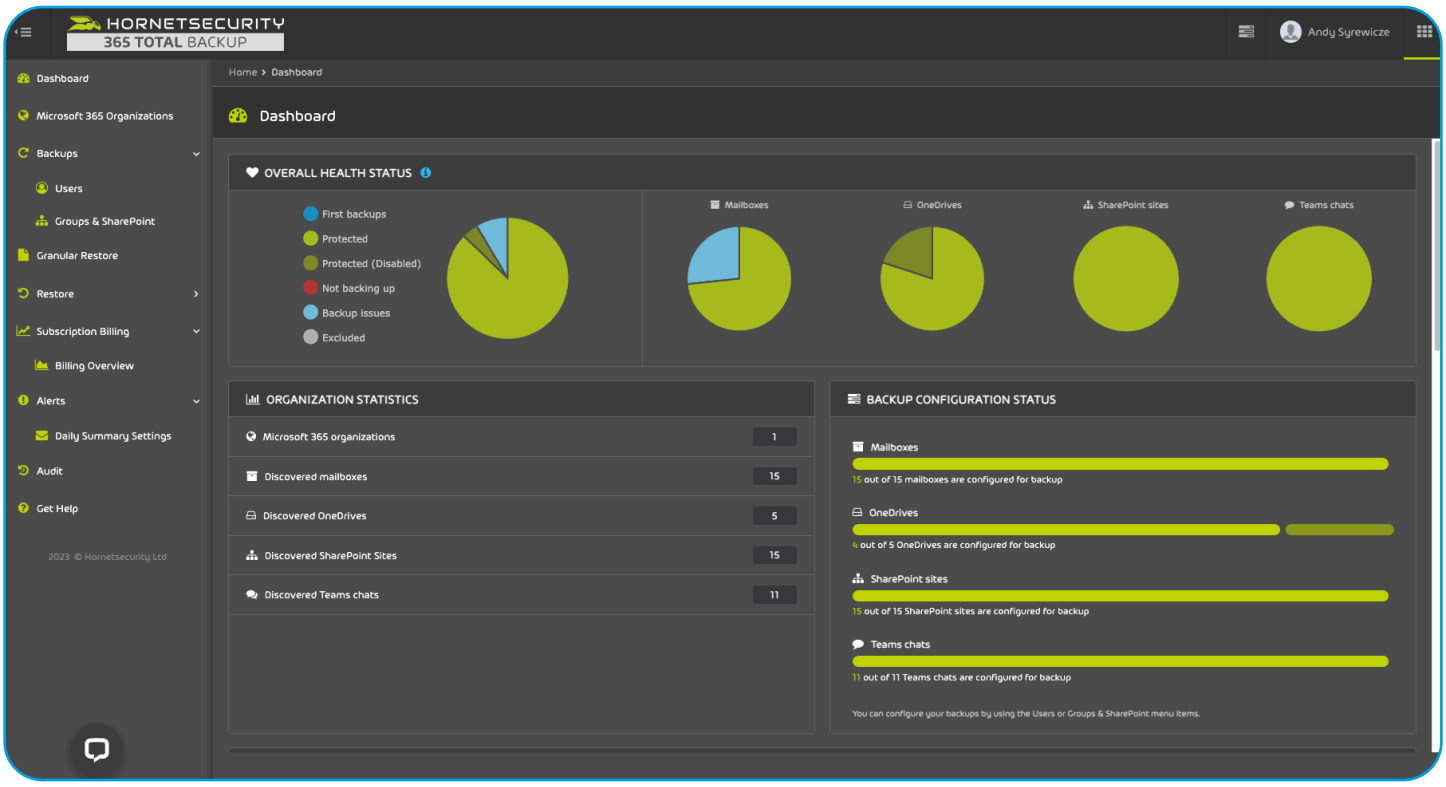
Veamos las opciones nativas para restaurar versiones anteriores de los datos. Los **elementos de Exchange** (correos electrónicos, contactos, citas del calendario) eliminados pueden recuperarse de la carpeta Elementos eliminados de Outlook. Permanecen **allí indefinidamente** a menos que cambies la política de tu tenant. Si se eliminan de la carpeta Elementos eliminados, puedes recuperarlos durante un máximo de 14 días desde la carpeta oculta Elementos recuperables. Tendrás que enseñar a los usuarios a hacerlo por sí mismos o asegurarte de que tu equipo de asistencia esté preparado para ayudarles con regularidad, ya que la interfaz de usuario no es precisamente intuitiva.

En SharePoint/OneDrive para Empresas, los **documentos eliminados** se guardan por defecto durante 93 días, primero en una papelera de reciclaje accesible para el usuario y, si se purgan de ahí, en una papelera de reciclaje accesible para el administrador. Una vez más, el proceso de restauración de un documento eliminado por error no es sencillo, por lo que será necesaria cierta formación.

Para cambiar los valores predeterminados, puedes usar las **Directivas de retención** para conservar los elementos durante más tiempo (están disponibles para su restauración incluso si los usuarios los eliminan de su carpeta Elementos eliminados). Estas directivas pueden aplicarse tanto a los datos de Exchange como a los de SharePoint. En el caso de Exchange, para gestionar la retención también se utilizan las **retenciones locales y por litigio** para determinados buzones de correo.

16.2: 365 TOTAL BACKUP

Si lo que buscas es paliar las dificultades que plantea el uso de las funciones de protección de datos integradas como solución de recuperación, Hornetsecurity ofrece una solución completa de copia de seguridad y recuperación M365 (**365 Total Backup**) o como parte de **365 Total Protection Compliance & Awareness**. Esto protege los buzones de correo, el chat de Teams, el almacenamiento de OneDrive para Empresas, los sitios de SharePoint y los puntos de conexión de Windows. Es fácil de configurar y ofrece una protección completa para todo el tenant.



¡NO DEJES NUNCA DE APRENDER!

Esperamos que este libro y sus enlaces a información técnica más detallada te hayan servido de guía en tu viaje a la nube y, una vez que hayas migrado, en el viaje en curso, ya que la gestión del siempre cambiante panorama de M365 es un viaje sin fin.

Como se mencionó en la Parte 1, estar siempre al tanto de las últimas aplicaciones y características de M365 es una tarea interminable. Consulta con regularidad los recursos oficiales de Microsoft y el **blog de Hornetsecurity** para leer artículos sobre administración y seguridad de M365.

Si prefieres consumir el contenido en formato de audio o vídeo, echa un vistazo a **The Security Swarm Podcast**, una conversación semanal sobre los temas más esenciales a los que se enfrenta el mundo de la ciberseguridad hoy en día, presentada por Andy Syrewicze, Security Evangelist de Hornetsecurity. Desde el uso malicioso de herramientas de IA hasta las estafas de ingeniería social, cada episodio se centra en un tema pertinente analizado por un experto del sector y respaldado por datos reales obtenidos directamente de nuestro Laboratorio de seguridad.

¡Buena suerte!

SOBRE EL HORNETSECURITY GROUP

HORNETSECURITY

Hornetsecurity is a leading global provider of next-generation cloud-based security, compliance, backup, and security awareness solutions that help companies and organizations of all sizes around the world. Its flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market. Driven by innovation and cybersecurity excellence, Hornetsecurity is building a safer digital future and sustainable security cultures with its award-winning portfolio.

Hornetsecurity operates in more than 30 countries through its international distribution network of 8,000+ channel partners and MSPs. Its premium services are used by more than 50,000 customers.

For more information, visit **www.hornetsecurity.com.**

SOBRE EL AUTOR

PAUL SCHNACKENBURG
MICROSOFT CERTIFIED TRAINER

Paul empezó en el mundo de la informática cuando DOS y los procesadores 286 eran lo último. Dirige Expert IT Solutions, una consultora informática para pequeñas empresas en Sunshine Coast (Australia). También trabaja como profesor de informática en una Microsoft IT Academy. Paul es un autor de tecnología muy respetado y activo en la comunidad. Escribe artículos técnicos detallados acerca de Hyper-V, System Center, cloud privada e híbrida y tecnologías de cloud pública de Office 365 y Azure. Cuenta con las certificaciones MCSE, MCSA y MCT.

HORNETSECURITY

365 TOTAL PROTECTION

PLAN 4 - COMPLIANCE & AWARENESS

PROTECCIÓN DE ÚLTIMA GENERACIÓN PARA MICROSOFT 365:
SEGURIDAD DEL CORREO ELECTRÓNICO, BACKUP, CUMPLIMIENTO Y CONCIENCIACIÓN EN SEGURIDAD

PLAN 1 | PLAN 2 | PLAN 3 | PLAN 4

BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS		
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT	PHISHING & ATTACK SIMULATION	COMMUNICATION PATTERN ANALYSIS
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS	SECURITY AWARENESS	AI RECIPIENT VALIDATION
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT	ESI® REPORTING	SENSITIVE DATA CHECK

365 Total Protection cubre todos los aspectos de seguridad y protección de datos de Microsoft 365 de una organización: seguridad del correo electrónico, backup y recuperación, cumplimiento normativo, gestión de permisos y concienciación en seguridad. La solución se integra a la perfección con Microsoft 365, proporcionando capas muy necesarias de seguridad adicional y protección de datos frente a spam, malware y amenazas avanzadas.

PRUEBA GRATUITA