

# CONCEPTOS BÁSICOS

# MICROSOFT 365

# Contenido

MODULO 0 - Introducción	7
Bienvenido a Conceptos básicos	7
Soluciones de productividad y trabajo en equipo de Microsoft 365	9
Introducción	9
Explorar formas de mejorar la productividad personal	9
Explorar formas de involucrar a los empleados	10
Explorar el chat en Microsoft Teams	12
<b>Hospedar reuniones en línea con Microsoft Teams</b>	12
Explorar el correo electrónico y el calendario	14
Explorar Office en todos los dispositivos	15
Explorar el almacenamiento y el uso compartido de archivos en Microsoft 365	16
Describir las inversiones en accesibilidad en Microsoft 365	17
<b>Prueba de conocimientos</b>	19
Involucrar a los empleados con Microsoft Teams, Viva y Yammer	20
Introducción	20
Chat y colaboración con Microsoft Teams	21
Reuniones en línea con Microsoft Teams	24
Grandes experiencias de los empleados con Microsoft Viva	26
Conectar empleados con Yammer	30
Utilizar Microsoft Stream para interactuar	33
Ampliar Teams con Power Platform y aplicaciones	36
Prueba de conocimientos	40
Almacenamiento y uso compartido de archivos con OneDrive y SharePoint	41
Introducción	41
OneDrive en Microsoft 365	41
SharePoint en Microsoft 365	46
Prueba de conocimientos	48
Module 2 - Demostrar conocimientos fundamentales de las capacidades de administración empresarial de Microsoft 365	49
Administristrar su negocio con Microsoft 365	49
Introducción	49
Productividad en la organización	49
Administración simplificada	51
Automatización de procesos de negocio	52
Extensibilidad	57

Administración de formularios y flujos de trabajo	59
Inteligencia empresarial	61
Administración del trabajo	64
Prueba de conocimientos	66
Simplifique la administración de dispositivos con Microsoft Endpoint Manager	67
Introducción	67
Administración moderna	67
Soluciones integradas en Microsoft Endpoint Manager	70
Intune	73
Configuration Manager	75
AutoPilot e implementación sin interacción	77
Prueba de conocimientos	79
Más tareas y garantía de la seguridad con Windows 10	80
Introducción	80
Describir Windows como servicio	80
Explorar los métodos de implementación para Windows 10	82
Explicar cómo Windows se mantiene seguro y actualizado	83
Describir las opciones de mantenimiento para Windows 10	84
Describir Azure Virtual Desktop (AVD)	84
Prueba de conocimientos	86
Aproveche la inteligencia empresarial con análisis e informes de Microsoft 365	87
Introducción	87
Descubrir cómo Workplace Analytics puede ayudar a las organizaciones a mejorar la productividad	87
Centro de administración de Microsoft 365	90
Describir los centros de administración adicionales en Microsoft 365	92
Prueba de conocimientos	93
Module 3 - Demostrar conocimientos fundamentales de las licencias, el servicio y el soporte técnico de Microsoft 365	94
¿Qué es Microsoft 365?	94
Introducción	94
Explore las ventajas de productividad de Microsoft 365	96
Explorar las opciones de suscripción de Microsoft 365	97
Explorar el inquilino de Microsoft 365	98
Explorar las áreas de examen	100
Prueba de conocimientos	101

Identificar las opciones de licencia disponibles en Microsoft 365	102
Introducción	102
<b>Comparar las opciones para el hogar, el negocio y la empresa</b>	102
Describir las capacidades adicionales disponibles con Azure	105
Describir el modelo de proveedor de soluciones en la nube	106
Explorar las opciones de administración de facturas	106
Explicar las formas en que Microsoft 365 ayuda a optimizar los costes	107
Prueba de conocimientos	108
Describir los beneficios de los servicios de Microsoft 365	109
Introducción	109
Explorar las opciones de soporte técnico de servicios para Microsoft 365	109
Explicar los acuerdos de nivel de servicio	110
Describir cómo realizar un seguimiento del estado de mantenimiento del servicio	112
Comunicar y compartir ideas con UserVoice	115
Prueba de conocimientos	117
Seleccionar una implementación en la nube	117
Introducción	117
Modelo de nube híbrida	118
¿Qué modelo de nube deberían elegir las organizaciones?	119
Migración frente a coexistencia: planificación de su traslado a Microsoft 365	120
Prueba de conocimientos	122
Module 4 - Demostrar conocimientos fundamentales de las funcionalidades de seguridad y cumplimiento de Microsoft 365	123
Describir los principios de seguridad y cumplimiento de Microsoft	123
Introducción	123
Descripción de la metodología de Confianza cero	123
Describir el modelo de responsabilidad compartida	125
Descripción de la defensa en profundidad	127
Descripción de las amenazas comunes	129
Describir Cloud Adoption Framework	130
Prueba de conocimientos	132
Describir las capacidades de administración de identidad y acceso de Microsoft 365	133
Introducción	133
Describir el modelo de Confianza cero de Microsoft y los conceptos de administración de identidad y acceso	133
Administrar identidades y acceso en Microsoft 365 con Azure Active Directory	137

Reducir el riesgo de infracciones de seguridad con una autenticación segura	140
Prueba de conocimientos	144
Describir las funcionalidades de protección contra amenazas de Microsoft 365	145
Introducción	145
Identificar las amenazas de seguridad más comunes	145
Descubrir cómo las empresas pueden prevenir y detectar amenazas y responder a ellas	146
Definir la posición de seguridad con el Centro de seguridad y la Puntuación de seguridad de Microsoft	151
Describir Microsoft Intelligent Security Graph y Azure Sentinel	154
Prueba de conocimientos	156
Describir las nuevas funcionalidades de seguridad en la nube de Microsoft 365	157
Introducción	157
Tome el control de su entorno en la nube con Microsoft Cloud App Security	157
Explore las capacidades de integración de Microsoft Cloud App Security	158
Prueba de conocimientos	160
Describir las funcionalidades de gobernanza y protección de la información de Microsoft 365	161
Introducción	161
Detectar e identificar información importante en su entorno	162
Proteger los datos confidenciales durante todo su ciclo de vida	164
Controlar los datos mediante Microsoft 365	167
Prueba de conocimientos	168
Describir las funcionalidades de administración de cumplimiento de Microsoft	169
Introducción	169
Describir las necesidades de cumplimiento comunes	169
Describir las ofertas del Portal de confianza de servicios	170
Describir los principios de privacidad de Microsoft	171
Describir el Centro de cumplimiento	171
Describir el Administrador de cumplimiento	175
Describir el uso y las ventajas de la puntuación de cumplimiento	178
Prueba de conocimientos	180
Reducir el riesgo y simplificar el proceso de detección y auditoría	182
Introducción	182
Administrar el riesgo interno	182
Administrar el cumplimiento de comunicaciones	185
Restringir las comunicaciones con barreras de información	186

Controlar el acceso de administrador privilegiado	187
Aumentar el control con Caja de seguridad del cliente	188
Investigar con Auditoría avanzada	189
Administrar el cumplimiento y las investigaciones legales con eDiscovery avanzado	190
Prueba de conocimientos	191

# MODULO 0 - Introducción

## Bienvenido a Conceptos básicos

### **Bienvenido al curso de Conceptos básicos de Microsoft 365**

Este curso está diseñado para ayudar a los alumnos a prepararse para Microsoft 365 Certified: Para el examen de conceptos básicos se le aportan materiales para ayudarle a entender las opciones disponibles en Microsoft 365 y las ventajas de adoptar servicios en la nube, el modelo de la nube de software como servicio (SaaS) y la implementación del servicio en la nube de Microsoft 365.

### **Demostrar conocimientos fundamentales de las capacidades de productividad y trabajo en equipo de Microsoft 365**

Conocer las soluciones de productividad y trabajo en equipo en Microsoft 365 y las capacidades que ayudan a las personas a ser más productivas con Microsoft 365: la nube de productividad del mundo.

Temas cubiertos:

- Soluciones de productividad y trabajo en equipo de Microsoft 365
- Involucrar a los empleados con Microsoft Teams, Viva y Yammer
- Hacer más con Office en todos los dispositivos
- Almacenamiento y uso compartido de archivos con OneDrive y SharePoint

### **Demostrar conocimientos fundamentales de las capacidades de administración empresarial de Microsoft 365**

Conocer las soluciones de administración empresarial en Microsoft 365 y las capacidades que ayudan a las organizaciones a ser más productivas con Microsoft 365: la nube de productividad del mundo.

Temas cubiertos:

- Administrar su negocio con Microsoft 365
- Simplifique la administración de dispositivos con Microsoft Endpoint Manager
- Haga más y manténgase seguro con Windows 10
- Aproveche la inteligencia empresarial con análisis e informes de Microsoft 365

### **Demostrar conocimientos fundamentales de las licencias, el servicio y el soporte técnico de Microsoft 365**

Aprender sobre las opciones de licencia, servicio y soporte técnico de Microsoft 365.

Temas cubiertos:

- Identificar las opciones de licencia disponibles en Microsoft 365
- Describir las ofertas de servicio técnico para los servicios de Microsoft 365
- Describir el ciclo de vida del servicio en Microsoft 365
- Seleccionar un modelo de implementación en la nube

## **Demostrar conocimientos fundamentales de las funcionalidades de seguridad y cumplimiento de Microsoft 365**

Conocer las áreas de soluciones de seguridad y cumplimiento de Microsoft 365 y las capacidades disponibles para ayudar a las empresas a protegerse y cumplir con los requisitos normativos.

Temas cubiertos:

- Describir las capacidades de administración de identidad y acceso de Microsoft 365
- Describir las funcionalidades de protección contra amenazas de Microsoft 365
- Describir las nuevas funcionalidades de seguridad en la nube de Microsoft 365
- Describir las capacidades de protección de la información y gobernanza de Microsoft 365
- Reducir el riesgo y simplificar el proceso de detección y auditoría

# Module 1 - Demostrar conocimientos fundamentales de las capacidades de productividad y trabajo en equipo de Microsoft 365

Soluciones de productividad y trabajo en equipo de Microsoft 365

## Introducción

En este módulo, aprenderá las soluciones de Microsoft 365 que pueden mejorar la productividad personal. Además de la solución Aplicaciones Microsoft 365, con la que ya está familiarizado, existen varias aplicaciones de colaboración y productividad que lo ayudan a trabajar bien en conjunto. Desde el correo electrónico y el chat hasta el almacenamiento y el uso compartido de archivos, Microsoft 365 ayuda a las personas y organizaciones a hacer más.

Al final de este módulo, podrá hacer lo siguiente:

- Describir cómo Microsoft 365 aporta a los usuarios herramientas para ayudarlos a mejorar su productividad personal.
- Explicar las capacidades de productividad y trabajo en equipo en Microsoft 365, y en qué productos se incluyen.
- Explicar cómo Microsoft incluye un diseño accesible en todos sus productos y servicios.

## Explorar formas de mejorar la productividad personal

En el mundo actual, la productividad personal significa trabajar cuando y donde sea conveniente. Microsoft 365 ofrece herramientas de productividad líderes en la industria e impulsadas por IA que le ayudan a dar rienda suelta a su creatividad y potencial. Produzca su mejor trabajo y manténgase en contacto, dondequiera que se encuentre; todo con la ayuda de la inteligencia y las capacidades integradas para:

- **Mejorar la productividad.** Use la integración de Power Platform para automatizar procesos, analizar datos y crear agentes virtuales.
- **Involucrar a los empleados.** Puede involucrar e informar a los empleados y clientes con transmisiones de vídeo envolventes y debates interactivos. Las herramientas de Microsoft 365 le ayudan a comunicar la visión de la organización y aportan un foro para el debate abierto.

- **Comunicarse con mensajería instantánea y chat.** Comuníquese con sus compañeros a través del chat o una reunión, ya sea de manera informal mientras trabaja o para reuniones regulares de equipo. Teams le da el poder de trabajar a su manera y mantenerse siempre en contacto.
- **Organizar reuniones en línea.** Trabaje de manera remota, segura y eficaz con sus compañeros. Las reuniones en línea le mantienen en contacto con su equipo y le ofrecen flexibilidad para trabajar en cualquier lugar. Puede organizar reuniones individuales, reuniones de equipo, así como importantes eventos en vivo; todo con audio, vídeo y pantalla compartida de alta calidad. Y todo con la misma seguridad y cumplimiento de Microsoft 365.
- **Manténgase en contacto a través del correo electrónico y el calendario.** Su calendario, contactos y tareas están todos en un solo lugar en Outlook. Y Outlook va donde usted vaya. Mantenga sus prioridades a la vista y comparta su calendario con los demás.
- **Sea productivo desde cualquier lugar.** Instale sus aplicaciones Microsoft 365 hasta en cinco dispositivos. Todas sus aplicaciones se mantienen actualizadas con las correcciones más recientes, lo que le ofrece más tiempo para concentrarse en su trabajo. La IA está integrada en sus aplicaciones 365 favoritas para que descubra nueva información, obtenga asistencia personalizada y encuentre lo que necesita más rápidamente.
- **Almacenar y compartir archivos.** Los datos se pueden almacenar y compartir de forma segura en OneDrive o SharePoint, sin tener que preocuparse por las contraseñas.
- **Empoderar a todos.** Todas las aplicaciones y herramientas Microsoft 365 están diseñadas con características de accesibilidad. Sea cual sea su nivel de habilidad, existen funciones de accesibilidad que le ayudarán a trabajar y aumentar su productividad.

## Explorar formas de involucrar a los empleados

La forma en la que trabajamos está cambiando rápidamente y, con ella, la cultura organizativa se está transformando. Cada vez más personas se sienten menos conectadas con su equipo después de pasar a un estilo de trabajo a distancia. Hoy en día, las organizaciones gastan más de **300 000 millones de dólares al año en la experiencia de empleados**, incluido el desarrollo, el aprendizaje, los beneficios y el bienestar, junto con toda una serie de tecnologías para la experiencia de empleados.

Pero, con demasiada frecuencia, estas tecnologías están fragmentadas, son difíciles de encontrar y afectan al flujo de trabajo. A medida que las herramientas digitales se vuelven más cruciales para una gran experiencia de los empleados, los líderes empresariales de todos los sectores están aprovechando la oportunidad de aprender y están revaluando tanto sus gastos como su enfoque.

Nunca se ha necesitado tanto la tecnología, datos e información diseñados para crear una gran experiencia de los empleados, independientemente de su ubicación.

- Los **empleados** quieren sentirse más conectados, más alineados con el propósito y la misión de su empresa. Quieren crecer, generar impacto y marcar la diferencia.

- Los **líderes** necesitan una forma moderna de generar compromiso y desarrollar a sus empleados.
- La **TI** necesita habilitar rápidamente una experiencia de empleado moderna, para el nuevo mundo laboral, sin tener que desechar y reemplazar todos sus sistemas y herramientas existentes.

Para superar estos desafíos, se necesita un nuevo enfoque y una nueva categoría de soluciones tecnológicas llamada **Plataforma de experiencia de empleados (EXP)**.

Una EXP es una plataforma digital que prioriza a las personas al reunir los **sistemas de trabajo** con los **sistemas de apoyo** en una experiencia integrada de empleado. Ofrece a las personas los recursos y el apoyo que necesitan para tener éxito y prosperar, independientemente de su ubicación.



Nuestra visión es una experiencia de empleado integrada llamada **Microsoft Viva**, que reúne todos estos recursos en el flujo natural del trabajo diario.

Microsoft Viva reúne comunicaciones, conocimiento, aprendizaje, recursos e información en una experiencia integrada que permite a personas y equipos dar lo mejor de sí en cualquier lugar. Con todo el apoyo de la amplitud y profundidad de Microsoft 365, Microsoft Viva se utiliza a través de Microsoft Teams y otras aplicaciones de Microsoft 365 que los usuarios usan a diario.

Obtenga más información sobre cómo [Viva ofrece a todos los empleados las herramientas que necesitan para la nueva era digital](#).

Para obtener más información sobre la disponibilidad de Viva, consulte [Experiencia y compromiso del empleado | Microsoft Viva](#).

## Explorar el chat en Microsoft Teams

Cuando necesite hacer algo, el chat y la mensajería instantánea le ayudarán a trabajar de forma más eficaz. La mensajería instantánea o el chat son ideales si necesita consultar algo con un compañero o hacer una pregunta rápida. También puede tener una conversación grupal para conocer la opinión de todos.

El chat y la mensajería instantánea les permiten trabajar juntos sin saturar su correo electrónico.

**Microsoft Teams** es su núcleo central para la colaboración dentro de la organización y proporciona un espacio de trabajo basado en un chat para ayudar a todos a trabajar de manera eficiente. Estas son algunas de las ventajas de usar el chat:

- Chatear en privado o en grupos: **Mantener a la gente informada y obtener aportaciones.**
- Eliminar el correo electrónico a Otros correos, incluidos las confirmaciones y poner a mucha gente en copia. Mantener **las bandejas de entrada limpias** para mensajes importantes.
- Fomentar los **intercambios abiertos**, hacer preguntas y promover el **debate reflexivo**.
- Inicie una **llamada** o **comparta pantallas** para hacer las cosas de manera más rápida.
- Los mensajes son en tiempo real, pero no interrumpen el trabajo de sus compañeros. Para que **todos puedan ser productivos**.
- Puede chatear desde su **dispositivo móvil** para mantenerse en contacto donde quiera que esté.
- Los **archivos útiles se pueden compartir** utilizando Teams para tener todo a mano.

Teams tiene todo lo que necesita para colaborar de forma eficaz, incluido chat, reuniones y llamadas. Puede organizar conferencias de audio, vídeo y web, y chatear con personas pertenecientes o ajenas a su organización

Leer más sobre [Mensajería instantánea con Teams](#). Mejore la comunicación de su equipo y haga más colectivamente.

## Hospedar reuniones en línea con Microsoft Teams

Reunir a su equipo para una reunión en línea es más fácil que nunca. Reúnase con cualquier persona, en cualquier lugar con inteligencia y confianza.

### Ciclo de vida de la reunión

Microsoft **Teams** le ayuda a reinventar el ciclo de vida de la reunión y a trabajar de forma más eficiente en cada paso. Desde la programación hasta el seguimiento, cuando está ocupado, puede ser difícil administrar todo. Teams le ahorra tiempo y le permite aumentar la productividad.

Teams le ofrece funciones avanzadas en cada etapa del ciclo de vida de la reunión:

Antes	Durante	Después
Comparta la agenda, invite a compañeros e invitados externos y aporte notas y grabaciones de reuniones anteriores.	Utilice el vídeo para personalizar, compartir contenidos y crear una grabación con transcripción automática.	Comparta grabaciones y notas, hable con sus compañeros y programe su próxima reunión.

## Reuniones en línea

Organice conferencias de audio, vídeo y web con cualquier usuario. Obtenga características, como asistencia de programación, toma de notas de la reunión, pantalla compartida, grabación de la reunión y mensajería instantánea.



- **Reuniones en línea** Las reuniones pueden ser 1:1 o grupales.
- **Uso compartido y de calidad de vídeo, audio y pantalla** El uso compartido de vídeo, audio y pantalla de alta calidad le permite concentrarse en su trabajo y en lo que se está hablando en lugar de en la tecnología.
- **Seguridad** Reúñase con confianza, sabiendo que cuenta con la misma seguridad y cumplimiento que Microsoft 365.
- **Programación y toma de notas** Invite a sus contactos a reuniones y use la pestaña de toma de notas para mantener un registro de lo expuesto en la reunión.

## Eventos en directo

Involucre e informe a sus empleados y clientes con transmisiones de vídeo inmersivo y debates interactivos en Microsoft Stream, Microsoft Teams y Yammer.

- Organice **eventos en directo** con hasta 10 000 usuarios y ofrezca una experiencia coherente en la web y en los dispositivos móviles.
- **Comparta su pantalla** durante eventos en directo.
- Monte **eventos de alto perfil** con cámaras profesionales, varias fuentes de contenido y mucho más.

Obtenga más información sobre [Microsoft Teams para reuniones en línea](#) y [Microsoft Teams para eventos en directo](#). Teams mantiene a todo el mundo en contacto, aunque no puedan estar en el mismo cuarto.

## Audioconferencia

La audioconferencia de Microsoft 365 permite que los usuarios entren en reuniones desde sus teléfonos. Dondequiera que estén, pueden unirse a una reunión mediante Teams. Hasta 250 usuarios pueden asistir a una audioconferencia. Los contactos se unen a las reuniones utilizando un número de acceso telefónico global, ya sea gratuito o de pago.

Aunque los usuarios tengan acceso a un equipo, la audioconferencia puede ser una buena opción si:

- La conectividad a Internet es limitada.
- La reunión es solo de audio.
- La calidad de la llamada es mejor cuando se marca por acceso telefónico.
- Alguien quiere acceso “manos libres” mediante un dispositivo Bluetooth.

Cuando configure una audioconferencia en Teams, obtendrá un puente de audioconferencia. Un puente de conferencia puede contener uno o más números de teléfono. El número de teléfono que establezca se incluirá en las invitaciones a la reunión para la aplicación Microsoft Teams.

Pero solo debe configurar la audioconferencia para los usuarios que vayan a programar o dirigir las reuniones. Los asistentes a la reunión que marquen para acceder no necesitan tener asignada ninguna licencia ni otra configuración.

## Dispositivos para reunión

Use dispositivos de un toque para unirse a las Salas de Microsoft Teams. Elija entre los socios certificados Logitech, Crestron, Polycom, Lenovo, HP o Yealink. Obtenga más información sobre los dispositivos para reuniones y las Salas de Microsoft Teams en [Sistemas de sala](#).

Obtenga más información sobre reuniones en línea:

- [Soluciones para reuniones en línea](#).
- [Audioconferencia en Microsoft 365](#)
- [Preguntas frecuentes sobre Audioconferencia](#)
- [Tutorial sobre Audioconferencia](#).

## Explorar el correo electrónico y el calendario

Con el correo electrónico empresarial y el calendario de Microsoft, puede estar al tanto de su trabajo con una vista clara y unificada de las cosas importantes. Su correo electrónico, calendario y contactos están todos en un solo lugar y lo acompañan a donde quiera que vaya.

- **Manténgase conectado.** Microsoft 365 sincroniza correos electrónicos, calendarios e información de contacto en todos sus dispositivos, manteniéndolo actualizado dondequiera que esté. Todo lo que necesita es una conexión a Internet para mantenerse en contacto sin problemas. Si pierde su teléfono, puede eliminar datos de forma remota para que su información personal permanezca segura.
- **Personalice su correo electrónico.** Cree un formato personalizado, incluya imágenes y, según su país o región, use su propio nombre de dominio. Puede conservar los correos electrónicos que necesite, incluidas las imágenes.
- **Administración simplificada.** Configure nuevos usuarios, restaure cuentas eliminadas y cree scripts personalizados, y más. El correo electrónico de Microsoft 365 también le proporciona el beneficio de una protección antimalware y un filtrado antispam líderes en la industria para proteger a la organización contra amenazas omnipresentes. Algunos planes también ofrecen archivado para detección y cumplimiento legal, y eDiscovery.
- **Conéctese.** Obtenga información valiosa sobre las personas con las que trabaja, dentro y fuera de su organización, conectando sus perfiles de LinkedIn y Microsoft 365.

Obtenga más información sobre el [correo electrónico empresarial de Microsoft 365](#). Encontrará artículos y sugerencias sobre cómo aprovechar al máximo el correo electrónico de Microsoft 365.

## Explorar Office en todos los dispositivos

Quiere trabajar cuando y donde más le convenga. Microsoft 365 le ofrece las aplicaciones con las que está familiarizado, además de todos los beneficios de la nube. Eso significa que puede trabajar desde cualquier lugar y ser productivo.



Microsoft 365 tiene las herramientas que necesita para trabajar en cualquier momento, en cualquier lugar y en cualquier dispositivo. Tiene las mismas aplicaciones de Microsoft Office que ha usado durante años, además de todos los beneficios de la nube.

- **En todos los dispositivos.** Dependiendo del plan, puede instalar aplicaciones Microsoft 365 hasta en cinco PC o Mac y cinco tabletas (iPad, Windows o Android). Si cambia de dispositivo, puede transferir la instalación. También puede ver y editar archivos en dispositivos Apple y Android con las aplicaciones móviles de Microsoft 365.

- **Siempre al día.** Sus aplicaciones familiares están ahora siempre actualizadas. No necesita perder tiempo instalando actualizaciones o preocuparse por cuándo se lanzarán las funciones porque todo está listo. Por lo tanto, siempre está trabajando con las características más actualizadas, al igual que todos sus compañeros.
- **Trabajo inteligente.** Las aplicaciones Microsoft 365 incluyen capacidades inteligentes para ayudarle a obtener mejores resultados. Los servicios inteligentes están integrados en aplicaciones, como Investigador y Editor en Word, Diseñador en PowerPoint e Insight Services para analizar datos. Estas herramientas inteligentes le ayudan a trabajar mejor, independientemente de en lo que esté trabajando.

Obtenga más información sobre cómo trabajar sin problemas en todos los dispositivos en [Microsoft 365 en todos los dispositivos](#).

## Explorar el almacenamiento y el uso compartido de archivos en Microsoft 365

En lo relativo al almacenamiento de archivos, desea que su trabajo sea accesible y esté seguro. Quiere poder colaborar con otros, trabajar en coautoría y compartir archivos, tanto dentro como fuera de su organización.

Los productos de almacenamiento y uso compartido de archivos de Microsoft están diseñados para ayudarle a almacenar, acceder, ser coautor y actualizar archivos de forma segura y desde cualquier lugar. Y puede compartir archivos tanto dentro como fuera de su organización.

Microsoft OneDrive ofrece acceso seguro y almacenamiento de archivos desde cualquier lugar. Microsoft SharePoint permite colaborar, compartir contenido y coordinar el trabajo dentro de la organización.

- **Trabaje desde cualquier lugar.** Use OneDrive para almacenar y acceder a sus archivos. OneDrive funciona a la perfección con Microsoft 365 y viene preinstalado con Windows. Cuando sincroniza sus archivos con su escritorio, puede trabajar sin conexión. Y puede acceder a sus archivos en Windows, Mac o dispositivos móviles.
- **Compartir de forma segura.** Microsoft 365 proporciona una seguridad perfecta para que pueda tener la confianza de que solo los destinatarios previstos pueden ver sus datos, tanto dentro como fuera de la organización. Use OneDrive para compartir archivos de forma segura dentro o fuera de su organización.
- **Colaborar.** Cuando guarde su trabajo en OneDrive o SharePoint, todos sus cambios se actualizarán automáticamente. Si comienza a realizar cambios en un dispositivo y termina en otro, todos los cambios se guardarán. Al ser coautor de un documento, puede anotar, resaltar y comentar en él.

Más información sobre [Almacenamiento y uso compartido de archivos de Microsoft](#). Las capacidades de almacenamiento y el uso compartido de archivos en Microsoft 365

permiten trabajar desde cualquier lugar, compartir con cualquier persona y colaborar de manera efectiva.

## Describir las inversiones en accesibilidad en Microsoft 365

Microsoft 365 ofrece las mejores aplicaciones de su clase y potentes servicios en la nube con accesibilidad integrada. Microsoft diseña todos sus productos para satisfacer las necesidades de personas con diferentes aptitudes, asegurando que todos puedan crear, comunicarse y colaborar en cualquier dispositivo.

No hay ningún límite en lo que los usuarios pueden lograr cuando la tecnología refleja la diversidad de todos. Con más de mil millones de personas en el mundo con discapacidades, la accesibilidad es una parte importante de las aplicaciones de Microsoft 365.

Microsoft 365 se ha diseñado con características accesibles para ayudar a las organizaciones a ser más inclusivas y que las personas sean más independientes. Con el enfoque firmemente en las *habilidades*, las funciones de accesibilidad de Microsoft se rigen por las normas de accesibilidad EN 301 549, la Sección 508 de EE. UU., WCAG 2.0 e ISO/IEC 40500.

### Visión

Para las personas ciegas, daltónicas o con deficiencia visual, estas son algunas características de Microsoft 365 que mejoran la visibilidad.

- Filtros de color: Aumentar el contraste o eliminar el color por completo. Tanto si experimenta daltonismo, sensibilidad a la luz o alguna preferencia visual, con los filtros de color puede personalizar la paleta de colores de su pantalla.
- Información: Acceder rápidamente a los comandos de varias aplicaciones de Microsoft 365 sin tener que navegar por la cinta de comandos. Puede utilizar Información para ayudar con el formato, descubrir las capacidades difíciles de encontrar y obtener ayuda en las aplicaciones de Microsoft 365 utilizando el lenguaje cotidiano.
- Microsoft Soundscape: Use tecnología innovadora basada en audio para permitir que las personas ciegas o con baja visión desarrollen una mayor conciencia de sus alrededores y así se sientan más seguras al navegar en nuevos entornos.
- Leer en voz alta y lector inmersivo: Word y otras aplicaciones de Microsoft 365 tienen la opción de leer el texto en voz alta, a partir de cualquier posición dentro de un documento.

### Audición

Para aquellos que tienen problemas de audición, pérdida de audición o sordera, aquí hay algunas características de Microsoft 365 que ayudan a la audición.

- Microsoft Translator: Muestra subtítulos autogenerados en una presentación en cualquiera de los más de 60 idiomas compatibles con el complemento Traductor de presentaciones para PowerPoint en PC. Además, deje que los miembros de la audiencia sigan la presentación con subtítulos que se muestran en el idioma seleccionado en cualquier dispositivo con Microsoft Translator.
- Generación automática de subtítulos en Microsoft Stream: Comparta vídeos de forma segura en toda su organización en un formato accesible con Microsoft Stream. Seleccione una simple opción y obtendrá leyendas y transcripciones, que se pueden buscar en inglés y en español, y que se generan automáticamente cuando carga vídeos.
- Sonido mono: Si tiene pérdida auditiva parcial o sordera en un oído, Windows 10 le ayuda a escuchar más con su equipo. Solo tiene que activar el sonido mono y los altavoces izquierdo y derecho reproducirán los mismos sonidos.

## Neurodiversidad

Las herramientas innovadoras como el dictado y el inicio de sesión de Windows Hello pueden hacer que el mundo digital sea más accesible para los usuarios que viven con dislexia, ataques, autismo u otras diferencias cognitivas.

- Asistente de concentración: Bloquee alertas y notificaciones para poder terminar las cosas sin distracciones. Si hay algunas personas a las que no desea ignorar, puede agregarlas a una lista especial. Cuando termine la concentración, obtendrá un resumen de lo que se ha perdido.
- Vista de lectura: Use la vista de lectura para eliminar el contenido molesto de las páginas web, de modo que pueda concentrarse en lo que desea leer. Y con las herramientas de aprendizaje de Microsoft Edge, puede hacer que los documentos se lean en voz alta.

## Aprendizaje

Las personas con dificultades de aprendizaje pueden aumentar la atención, la concentración, mejorar las aptitudes de lectura y escritura y mejorar la comprensión con estas características de Microsoft 365.

- Lector inmersivo: Lea con mayor eficacia con las herramientas de aprendizaje que leen el texto en voz alta, dividen las palabras en sílabas e identifican partes del discurso. Mantenga la atención con el modo Focalizado y el espaciado ajustable entre líneas, letras y palabras. Disponible para OneNote, Word y Outlook en varios dispositivos.
- Editor en Word: Con el editor, vea errores ortográficos, gramaticales y problemas de estilo a medida que escribe en Word y Outlook para PC. Obtenga sugerencias sobre errores ortográficos, vea sinónimos junto a sugerencias y haga que se lean las sugerencias en voz alta para evitar errores comunes en las elecciones de palabras.
- Sugerencias de texto: Obtenga ayuda para construir oraciones con sugerencias. Aparecen sugerencias de palabras y se pueden insertar mientras

escribe. Es una característica estupenda para los estudiantes de inglés y para cualquier persona que desee un poco de ayuda con su escritura.

## Movilidad

- Dictar en las aplicaciones de Microsoft 365: Convierta su voz en texto con Dictar, en las aplicaciones de Microsoft 365 como Word, PowerPoint y Outlook para PC. También puede obtener el complemento Dictar para Word, Outlook y PowerPoint para equipos PC, lo que permite el dictado en más de 20 idiomas y traducción en tiempo real a más de 60 idiomas.
- Información: Busque la bombilla y el mensaje *Dígame qué desea hacer*. Escriba en qué necesita ayuda y la búsqueda inteligente le mostrará opciones que incluyen definiciones, personas y acciones que puede realizar.

## Salud mental

Se trata de tecnologías de asistencia para personas que viven con problemas como el trastorno bipolar, ansiedad, TEPT, depresión o TDAH. Los productos de Microsoft 365 pueden ayudar con los problemas de distracción, lectura y concentración.

- Minimizar las distracciones visuales: Reducir las animaciones y desactivar las imágenes de fondo y las transparencias. También puede eliminar elementos de la barra de tareas y simplificar el menú de inicio.
- Asistente de concentración: Bloquee alertas y notificaciones para poder terminar las cosas sin distracciones. Si hay personas a las que no desea ignorar, puede agregarlas a una lista especial. Cuando termine la concentración, obtendrá un resumen de lo que se ha perdido.
- Tareas pendientes: OneNote y Outlook trabajan en conjunto para ayudarlo a mantenerse organizado. A medida que tome notas y planee proyectos en OneNote, puede administrar fechas límite y recordar las cosas en su lista de tareas pendientes creando tareas de Outlook. A continuación, puede ver y seguir esas tareas en Outlook y recibir recordatorios.

Para información detallada sobre las funciones de accesibilidad de los productos de Microsoft, consulte [Accesibilidad de Microsoft](#). Todas las características tratadas en esta unidad pueden ayudarle a mejorar su productividad, tenga o no una discapacidad reconocida.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

Desea tener una reunión semanal con los jefes de su equipo, que se encuentran en lugares distintos. ¿Cuál es el producto de Microsoft más adecuado?

- A. PowerPoint
- B. Teams
- C. SharePoint

Recientemente, se le pidió que administrara un proyecto que incluye personas de dentro y fuera de su organización. Necesita compartir archivos con todos en el proyecto. ¿Cuál es el producto de Microsoft más adecuado?

- A. Correo electrónico
- B. Yammer
- C. OneDrive

Está administrando un proyecto con personas que trabajan en diferentes ubicaciones. Para mejorar la colaboración y el trabajo en equipo, está fomentando una comunicación más frecuente e informal. ¿Cuál es el producto de Microsoft más adecuado?

- A. Word
- B. Teams
- C. OneDrive

Su organización está lanzando un producto nuevo importante. Desea organizar un importante evento en línea para anunciarlo en su sector. Tendrá varias personas hablando, además de vídeos. ¿Qué combinación de productos de Microsoft debería utilizar para organizar el evento?

- A. PowerPoint, SharePoint y Stream.
- B. Yammer, Teams y Stream.
- C. Teams, SharePoint y Stream.

## Involucrar a los empleados con Microsoft Teams, Viva y Yammer

### Introducción

Las personas trabajan periódicamente en proyectos, departamentos y con usuarios de socios externos, lo que puede dificultar la colaboración de manera efectiva y segura. Microsoft Teams, Yammer y Microsoft Stream pueden ayudar a su organización a mejorar la forma en que las personas trabajan juntas. Aprenderá cómo estas herramientas pueden ayudar a mejorar la productividad en toda su organización.

Al final de este módulo, debería ser capaz de hacer lo siguiente:

- Describir cómo herramientas como Microsoft Stream, Microsoft Teams y Yammer pueden ayudar a las personas de su organización a trabajar juntas.
- Explicar cómo funcionan las soluciones de mensajería instantánea y chat en Microsoft 365 para conseguir la implicación de los empleados
- Describir las soluciones para reuniones en línea en Microsoft 365
- Detallar cómo se puede usar Yammer para fomentar conexiones en todos los niveles de una organización

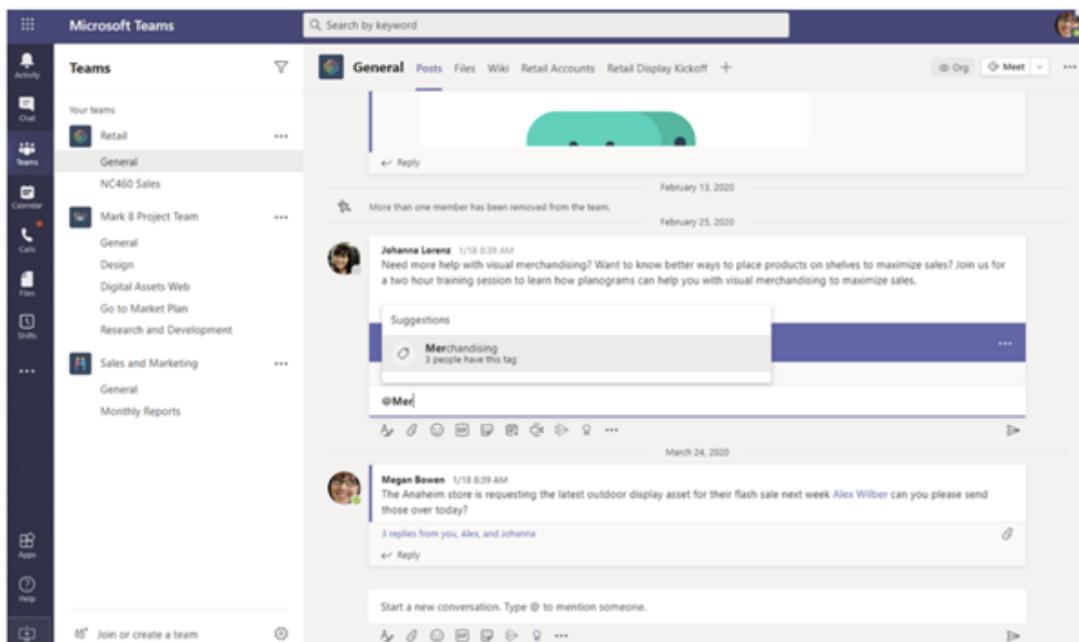
- Describir cómo Microsoft Stream puede mejorar el compromiso con el contenido de vídeo en toda la organización
- Explicar cómo Microsoft Teams se puede ampliar con Power Platform y aplicaciones

## Chat y colaboración con Microsoft Teams

Las personas de su organización tienen que colaborar de forma regular en proyectos como equipos. Desea comprender cómo los equipos de su organización pueden colaborar de manera más productiva cuando trabajan juntos en proyectos.

### ¿Qué es Microsoft Teams?

Microsoft Teams proporciona un punto de acceso central que los equipos pueden usar para colaborar en sus proyectos a través de áreas de trabajo basadas en chat.



Microsoft Teams ayuda a los equipos a compartir continuamente documentos, actualizaciones de estado y más para que todos se mantengan conectados y con información actualizada, ya sea que estén en su escritorio o de viaje con su dispositivo móvil. La colaboración no se limita a su organización, Teams le permite trabajar de la misma manera junto con cualquier persona fuera de su organización. Los usuarios pueden acceder a Microsoft Teams a través de su explorador de Internet o instalando Microsoft Teams en su equipo o dispositivo móvil. Microsoft Teams incluye muchas características y funcionalidades para ayudar a sus usuarios a conectarse y colaborar, incluidas las siguientes:

### Equipos y canales

Microsoft Teams anima a sus usuarios a organizarse y colaborar en proyectos y cargas de trabajo. Para ello, presenta los siguientes conceptos para ayudar al trabajo en equipo:

- **Equipos de trabajo.** Un equipo de trabajo es una colección de personas, contenidos y las herramientas necesarias para trabajar en proyectos. Los equipos pueden ser privados, solo para los usuarios invitados. Los equipos también pueden ser públicos y estar abiertos a cualquier persona que quiera unirse. Un equipo de trabajo tiene un límite de hasta 10 000 miembros a la vez.
- **Canales.** Los canales son lugares donde los usuarios pueden mantener conversaciones y en los que se lleva a cabo el trabajo. Los canales ofrecen características como las pestañas. Las pestañas permiten que los usuarios accedan y trabajen en el mismo contenido. Por ejemplo, los usuarios de un equipo podrían tener un canal con una pestaña para un informe específico al que todos se dedican y en el que están trabajando juntos.

## Chat

Microsoft Teams incluye funciones de chat y uso compartido para facilitar la colaboración entre los usuarios a través de la conversación, para que puedan participar en debates y mantenerse al día. Entre ellas, se incluyen las siguientes:

- **Chat privado.** Los usuarios pueden charlar con otros usuarios individuales para formular preguntas rápidas y tener conversaciones privadas. También se pueden agregar usuarios adicionales directamente a una conversación.
- **Chat de grupo.** Los usuarios pueden charlar con otros usuarios como parte de un grupo, para una mayor discusión y colaboración.
- **Acceso de los invitados.** Los usuarios pueden chatear y trabajar con usuarios externos fuera de la organización.
- **Uso compartido de archivos.** Los usuarios pueden compartir archivos y documentos con compañeros de trabajo y colegas externos.
- **Seguridad.** Todos los datos se cifran en reposo y en tránsito.
- **Integración con otras aplicaciones.** Microsoft Teams puede conectarse con otras aplicaciones y servicios que sus usuarios ya usan para colaborar. De esta manera, pueden colaborar mediante esas aplicaciones y servicios desde una ubicación central. Por ejemplo, los usuarios pueden trabajar en el mismo archivo de Excel para crear un informe juntos.

## Llamadas de voz y vídeo

Microsoft Teams incluye diferentes características y capacidades diseñadas para permitir que los usuarios colaboren a través de llamadas de voz o vídeo y reuniones.

- **Reúñase con cualquiera.** Los usuarios pueden organizar llamadas de voz y vídeo individuales, llamadas y conferencias con todos los miembros de un equipo y eventos en directo para hasta 10 000 personas.
- **Pantalla compartida.** Los usuarios pueden decidir qué quieren mostrar en un chat o reunión. Por ejemplo, el escritorio completo, una pantalla específica o una aplicación específica.
- **Fondos personalizados.** Los usuarios pueden difuminar sus fondos o utilizar fondos personalizados durante las reuniones para evitar distracciones, establecer el tono y garantizar la privacidad.

- Compartir notas de reuniones. Los usuarios pueden compartir grabaciones de reuniones y notas de audio o llamadas de voz en la conversación de la reunión para una reunión.

## Seguridad y cumplimiento

Microsoft Teams está basado en Microsoft 365 y ofrece capacidades de cumplimiento y seguridad de nivel empresarial con una capacidad de administración completa y controles granulares:

- Cifrado para Teams: todos los datos de Teams se cifran en tránsito y en reposo.
- Protección de datos integrada: Teams proporciona de forma nativa funciones críticas para la empresa, como la prevención de pérdida de datos y las directivas de retención, sin necesidad de un servicio de terceros como Zoom o Slack.
- Administre fácilmente reuniones e invitados: control total sobre las directivas que garantizan que los invitados estén completamente controlados y que las reuniones se limiten solo a los usuarios esperados
- Administración centralizada: el Centro de administración de Microsoft 365 permite al departamento de TI simplificar la administración de los controles de seguridad, cumplimiento e identidad que rigen su organización.
- Líder del sector: Teams admite más de 90 estándares y leyes regulatorias, incluidas FedRAMP, SOC, HIPAA y la Ley de privacidad y derechos educativos de la familia (FERPA).

## Colaboración remota y aprendizaje a distancia

Cada vez más organizaciones están pasándose al trabajo remoto. Un equipo puede estar formado por miembros que se encuentran en diferentes ubicaciones geográficas y zonas horarias. El trabajo remoto puede ayudar a las organizaciones a ahorrar costes, mejorar la productividad e incluso salvar vidas en las pandemias globales. Microsoft Teams facilita el trabajo remoto animando a los usuarios a conectarse y permitiéndoles compartir fácilmente ideas y cargas de trabajo. Microsoft Teams está diseñado para ayudar a los equipos a trabajar juntos y mantenerse conectados como si estuvieran en la misma oficina. Por ejemplo, un usuario puede compartir su pantalla y otros usuarios pueden solicitar el control de su equipo para ayudar a su compañero a resolver problemas en su dispositivo.

Microsoft Teams también está diseñado para mejorar el aprendizaje a través de experiencias tipo aula. Microsoft Teams hace posible que los usuarios aprendan a distancia a través de aulas virtuales. Los usuarios pueden participar en conferencias, sesiones uno a uno o discusiones grupales y compartir tareas y materiales.

## Apoye las conversaciones productivas a través de Microsoft Teams

Use el tutorial interactivo a continuación para aprender cómo Microsoft Teams ayuda a los equipos a ser más productivos y eficientes a través de características que están diseñadas para mejorar sus conversaciones de chat y mensajería instantánea. Incluye

características como audio y vídeo enriquecidos, intercambio de archivos, canales de equipo e integración con otras aplicaciones como Microsoft Planner, Microsoft Whiteboard, Power BI y más.

## Reuniones en línea con Microsoft Teams

En el pasado, a los participantes de las reuniones les resultaba difícil configurar las reuniones, y reunirse a ellas, con las herramientas anteriores. Desea comprender cómo Microsoft Teams puede ayudar a los equipos de su organización a tener reuniones más productivas en el futuro.

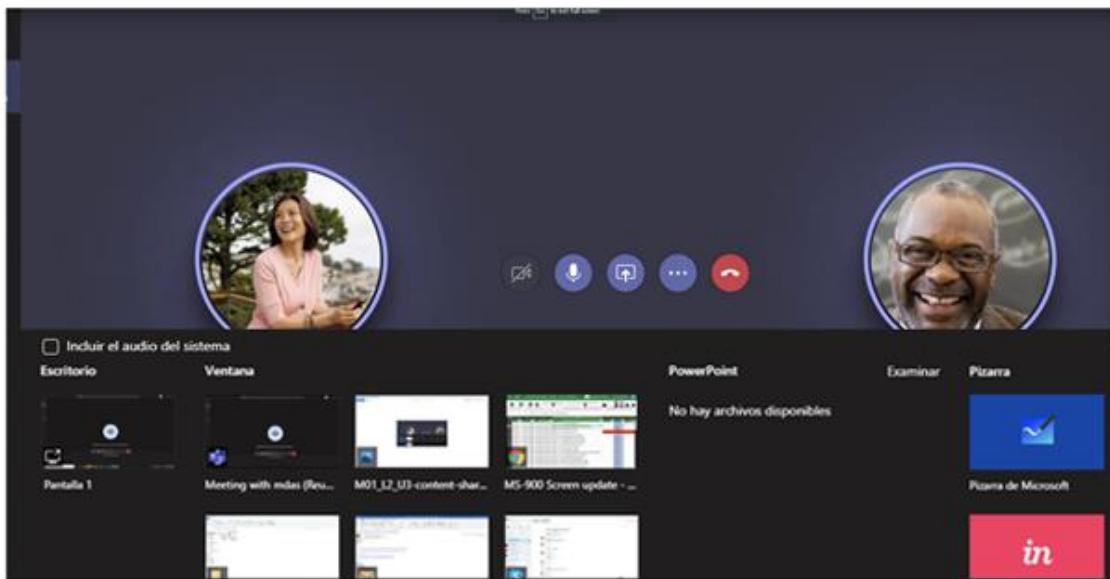
### Características y funcionalidades de Microsoft Teams para reuniones

Las reuniones ayudan a los equipos a compartir actualizaciones de estado, intercambiar ideas y resolver problemas juntos. Los equipos de su organización necesitarán colaborar en proyectos mediante reuniones con regularidad.

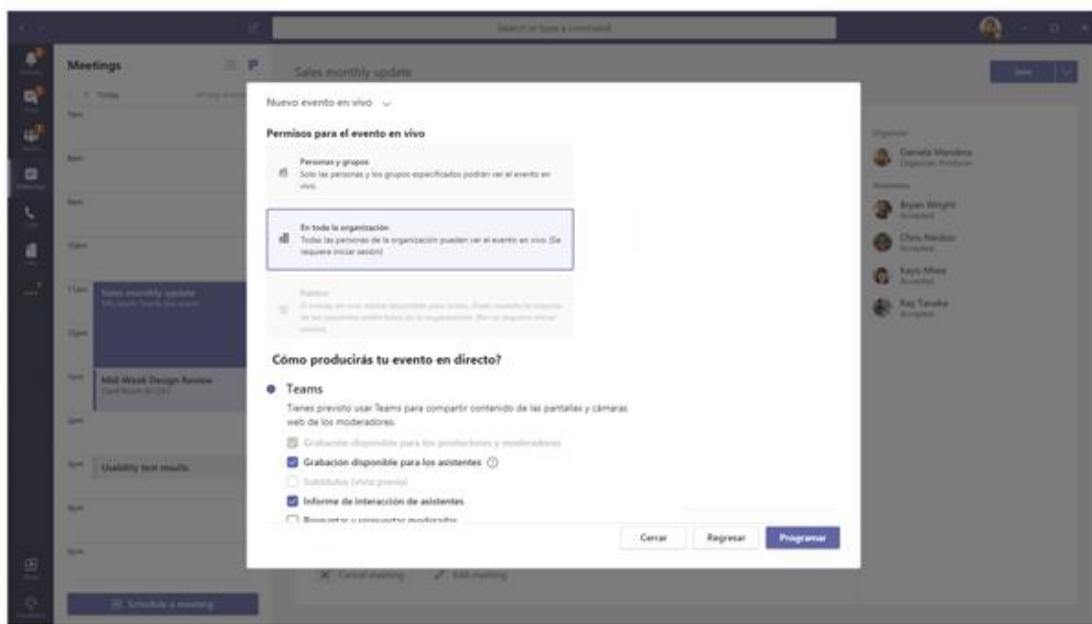
Microsoft Teams está diseñado para ayudarle a tener reuniones más productivas. Microsoft Teams viene con muchas características y capacidades diferentes que puede usar para ayudar a sus equipos a participar rápidamente y mejorar la forma en que trabajan juntos a través de reuniones:

- **Programar y participar en reuniones:** Los usuarios pueden unirse a las reuniones a través de vínculos, sus calendarios o llamar a las reuniones utilizando sus teléfonos. El calendario de Teams de un usuario está conectado a su calendario de Exchange. De forma que, cuando los usuarios programan una reunión en Outlook, su reunión es automáticamente visible y accesible desde Teams, y viceversa. Los usuarios también pueden iniciar reuniones cuando lo deseen, sin programarlas.
- **Reuniones de varias personas:** Varias personas pueden unirse a una sola reunión. Por ejemplo, un equipo interno puede unirse a una reunión con un equipo externo de usuarios. Microsoft Teams aporta una vista de galería para reuniones que mostrará a todos los participantes, hasta cuarenta y nueve a la vez.
- **Dispositivos de reunión:** Los usuarios pueden iniciar reuniones y unirse a ellas con dispositivos especializados que utilizan a diario. Por ejemplo, los miembros del equipo en el terreno en un sitio de construcción pueden acceder desde un dispositivo móvil para compartir actualizaciones en vivo sobre el progreso y los problemas.
- **Compartir contenido en reuniones:** Los usuarios pueden compartir pantallas, ventanas y archivos individuales durante una reunión. También

pueden usar pizarras para esbozar ideas y compartir notas:



- **Grabar y publicar con Microsoft Stream:** Los usuarios pueden grabar reuniones y publicarlas en Microsoft Stream para su archivo y utilización más amplia.
- **Transcripción automática de videos:** Microsoft Teams puede transcribir automáticamente sus reuniones grabadas mediante traducción basada en inteligencia artificial.
- **Eventos en vivo:** Microsoft Teams funciona con Microsoft Stream para permitir a sus usuarios organizar fácilmente eventos en vivo para miles de asistentes:



- **Subtítulos en tiempo real.** Microsoft Teams puede detectar qué se dice en una reunión y presentar subtítulos en tiempo real atribuidos a la persona que habla.

**Nota:** Por ahora, los subtítulos solo están disponibles en inglés (EE. UU.).

## Administrar reuniones con Microsoft Teams

Utilice el tutorial interactivo a continuación para aprender cómo los usuarios configuran y administran reuniones y cómo administrar configuraciones como las directivas de reuniones para controlar qué funciones están disponibles para los usuarios en las reuniones.

## Grandes experiencias de los empleados con Microsoft Viva

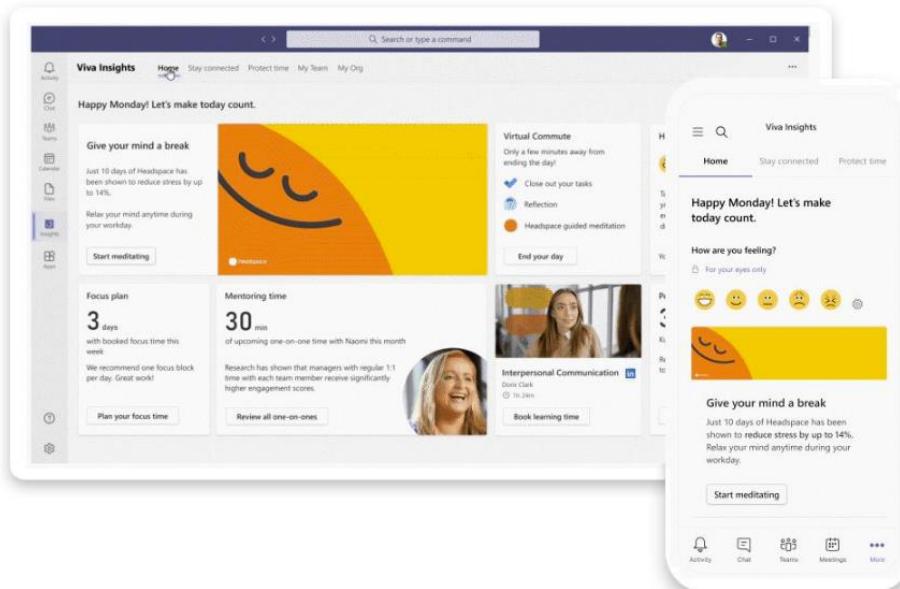
Microsoft Viva reúne comunicaciones, conocimiento, aprendizaje, recursos e información en una experiencia integrada que permite a personas y equipos dar lo mejor de sí en cualquier lugar. Con todo el apoyo de la amplitud y profundidad de Microsoft 365, Microsoft Viva se utiliza a través de Microsoft Teams y otras aplicaciones de Microsoft 365 que los usuarios usan a diario.

### Una nueva clase de experiencia de empleado

Para comenzar, Microsoft Viva incluirá cuatro módulos: Ideas Microsoft Viva, Temas Microsoft Viva, Aprendizaje Microsoft Viva y Conexiones Microsoft Viva, además de otras que llegarán.

### Insights

**Microsoft Viva Insights** es una nueva aplicación unificada en Teams que reúne Workplace Analytics, MyAnalytics y Glint. Aporta datos cuantitativos y cualitativos e información para permitir a los usuarios, administradores y líderes mejorar la productividad y el bienestar de la organización.



Con acceso en Microsoft Teams, Ideas Microsoft Viva para **usuarios** ayuda a los empleados a mantenerse conectados con sus compañeros y a reservar tiempo para los descansos regulares, el trabajo concentrado y el aprendizaje.

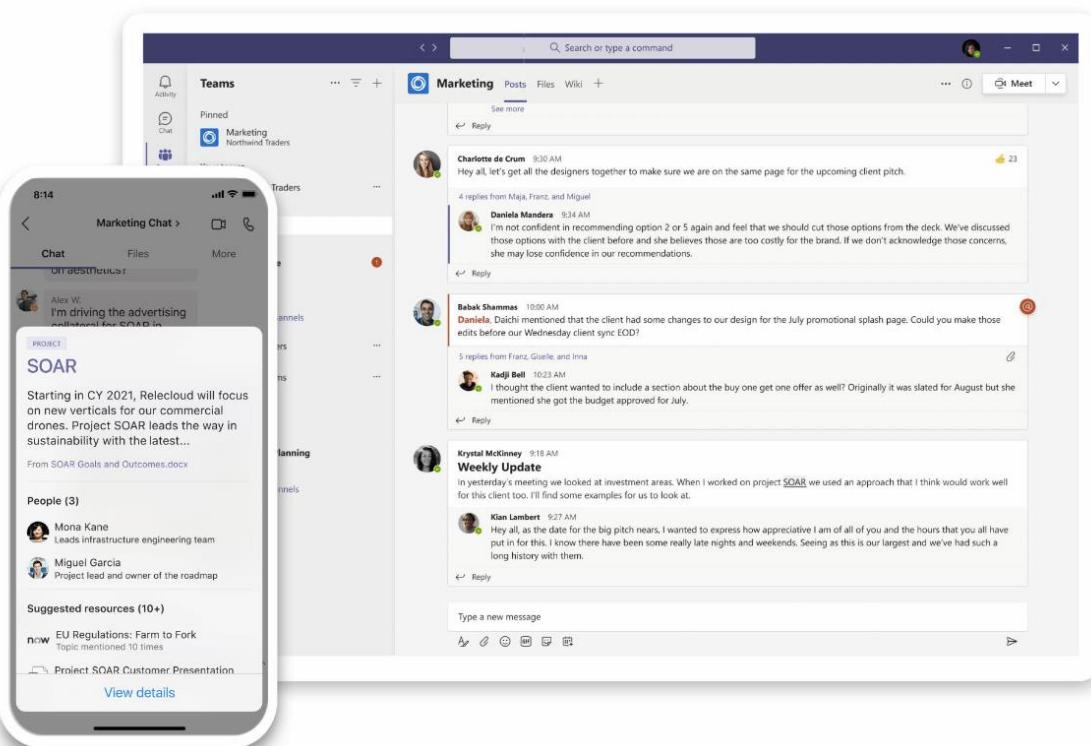
Para los **administradores**, Viva Insights puede dar información y recomendaciones basadas en datos y protegidas por la privacidad para fomentar equipos saludables y exitosos. Por ejemplo, Viva Insights puede ayudar a un administrador a ver si su equipo está en riesgo de agotamiento y aportar recomendaciones como animar a su equipo a apagar las notificaciones, establecer límites en su calendario y establecer prioridades diarias para centrarse en lo que más importa..

Para los **Líderes empresariales**, Viva Insights puede ayudar a abordar desafíos complejos y a responder a los cambios dando información sobre los patrones y tendencias de trabajo de la organización. Esto podría incluir oportunidades de bienestar, pero también aspectos como la planificación del espacio, a medida que las empresas reimaginan sus oficinas para el trabajo híbrido.

Para ayudar a garantizar la **privacidad y la seguridad**, Microsoft Viva utiliza la agregación, la desidentificación y la privacidad diferencial. Esto significa que la información personal es visible solo para el empleado, mientras que la información de los administradores y líderes se agrega y desidentifica por defecto para proteger la privacidad individual..

## Topics

**Microsoft Viva Topics** se centra en el conocimiento y la experiencia. Utiliza inteligencia artificial (IA) para identificar conocimientos y expertos y organizarlos en temas compartidos. Las páginas de temas aparecen como tarjetas justo en el flujo de trabajo en Office y Teams.



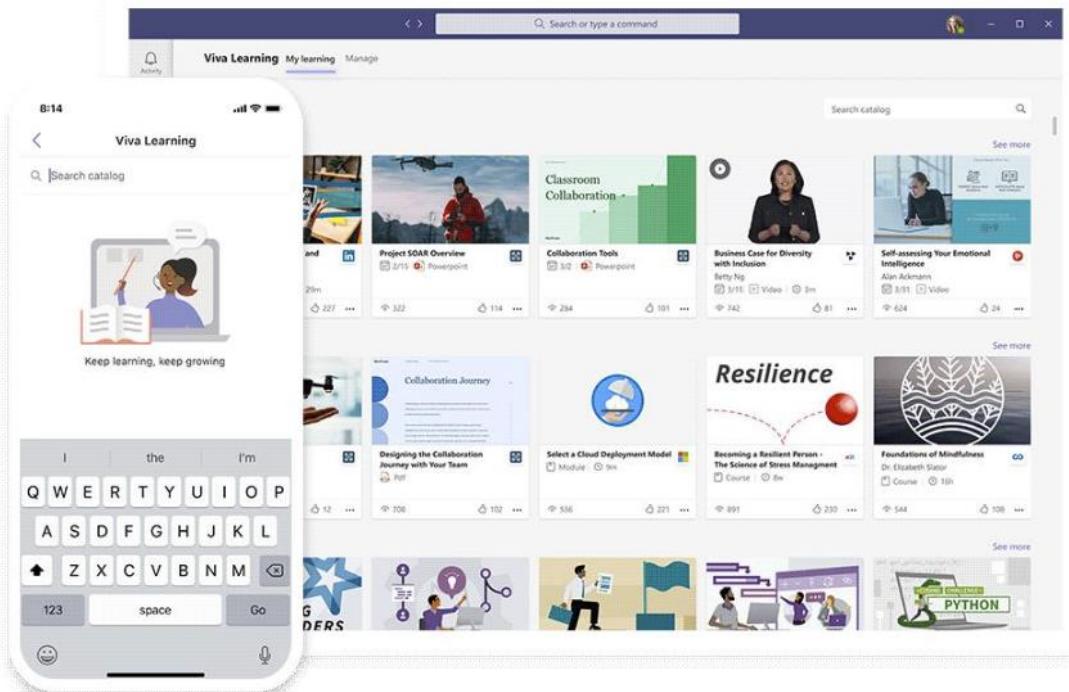
Temas Microsoft Viva revela automáticamente las tarjetas de temas a medida que la gente trabaja en aplicaciones como Office, SharePoint y Microsoft Teams. Cuando los empleados hacen clic en una tarjeta, aparece una página de temas con documentos, vídeos y personas relacionadas. Los expertos de la empresa también pueden ayudar a recopilar la información que se muestra en Viva Topics compartiendo conocimientos a través de sitios web sencillos y altamente personalizables denominados Páginas de temas.

Además del contenido de Microsoft Cloud, Viva Topics también ofrece información de servicios de terceros como ServiceNow y Salesforce y se basa en las integraciones realizadas por socios como Accenture, Avanade, BA Insight, Raytion y ClearPeople. Y los conectores de Graph facilitan la conexión a todavía más contenido que puede ser de utilidad para los empleados.

Para obtener información más detallada sobre Viva Topics, consulte [Introducción a Temas Viva - Learn | Microsoft Docs](#).

## Aprendizaje

**Aprendizaje Microsoft Viva** permite a los empleados descubrir fácilmente el aprendizaje informal y formal en el flujo de trabajo. Agrega contenido de LinkedIn Learning, Microsoft Learn, contenido de aprendizaje de terceros y contenido interno propio. Además de aportar agregación y recomendaciones, también permite a los administradores asignar, seguir e informar sobre el aprendizaje dentro y entre varios equipos.



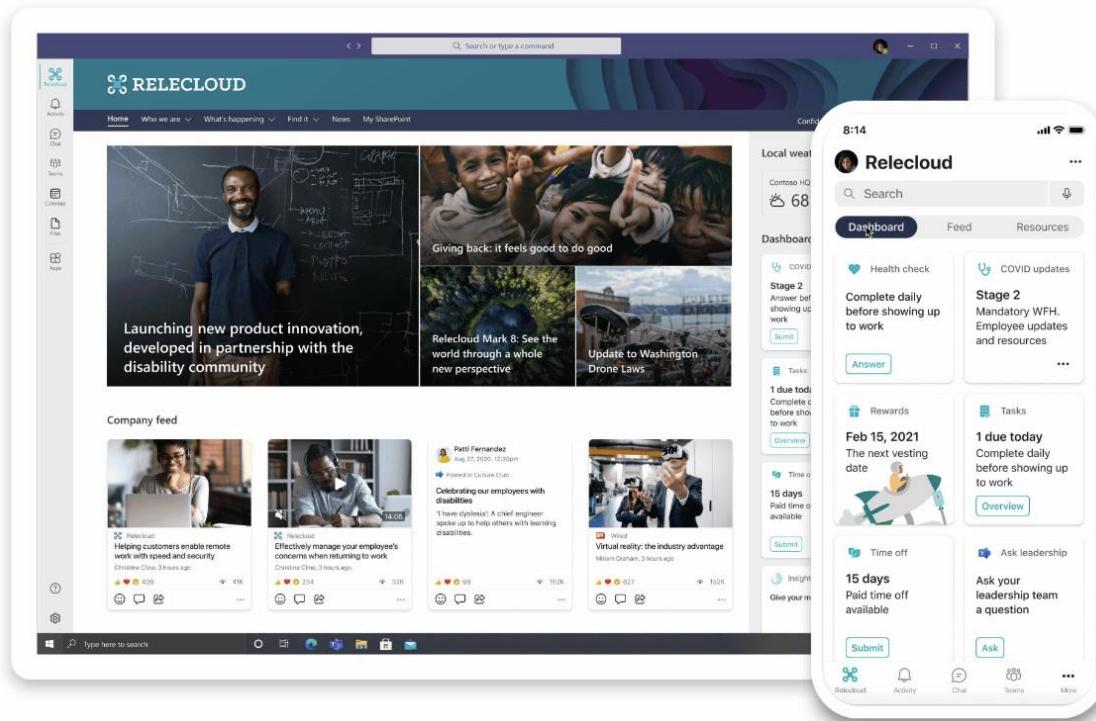
Con Aprendizaje Microsoft Viva, los empleados pueden descubrir y compartir fácilmente desde cursos de aprendizaje hasta contenidos de microaprendizaje. Y los administradores obtienen las herramientas necesarias para asignar el aprendizaje y hacer un seguimiento de la finalización de los cursos para ayudar a fomentar una cultura de

aprendizaje. Viva Learning crea un punto central para el aprendizaje en Teams, con una IA que recomienda el contenido adecuado en el momento adecuado.

Agrega contenido de LinkedIn Learning, Microsoft Learn, el contenido propio personalizado de su organización y los cursos de aprendizaje de los principales proveedores de contenidos, como Skillsoft, Coursera, Pluralsight y edX. Viva Learning también funciona con los principales sistemas de administración del aprendizaje

## Conexiones

**Conexiones Microsoft Viva** reúne todas estas experiencias en una aplicación para empleados de la marca de la empresa en Teams. Se basa en las capacidades existentes de SharePoint y Yammer y aporta un destino para empleados personalizado y protegido. Permite a las organizaciones comunicarse e involucrar a los empleados y habilita un fácil acceso a todos los recursos que un empleado necesita para tener éxito.



## Abierta, extensible y con novedades por delante

Microsoft Viva está diseñada para ser una plataforma abierta y extensible, fácil de integrar con los sistemas y herramientas que ya tiene la empresa. Las integraciones con Microsoft 365, Microsoft Power Platform, Microsoft Dynamics 365, productos y servicios de terceros ofrecerán una experiencia completa a los empleados en el flujo de trabajo.

Todos sabemos que los empleados comprometidos y sanos que tienen un sentido de propiedad, propósito y pertenencia tienen un mayor impacto en nuestras organizaciones. Con Microsoft Viva, queremos hacer que sea más fácil y natural para todo el mundo estar conectado, acceder a los conocimientos, aprender en el trabajo y utilizar información protegida por la privacidad. Permitir a las personas priorizar el bienestar,

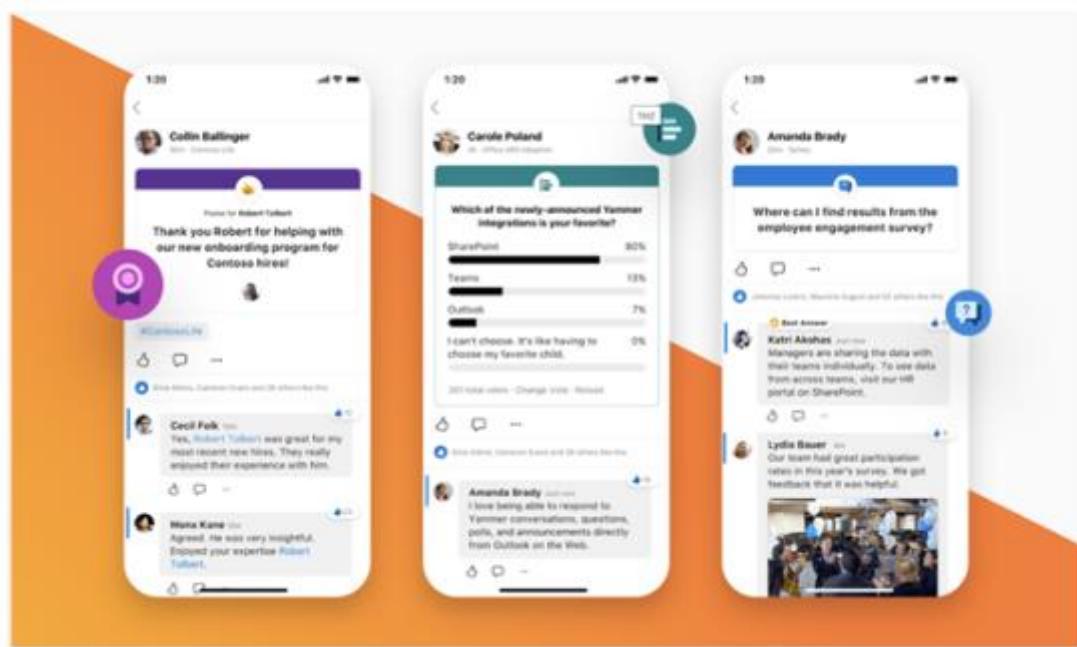
formar a los administradores para dirigir con mayor eficacia y ayudar a los líderes a impulsar una mejor toma de decisiones en toda la organización. Se trata de una oportunidad única para crear experiencias centradas en las personas que ayuden a obtener resultados extraordinarios.

## Conectar empleados con Yammer

Quiere que las personas de distintas partes de su organización puedan compartir y explorar ideas juntas. Desea que su organización mejore la colaboración entre equipos y departamentos.

### Qué es Yammer

Si bien Microsoft Teams está ahí para ayudarle a trabajar con los compañeros de equipo en proyectos, Yammer está diseñado para ayudarle a conectarse con personas de su organización con las que es posible que no trabaje directamente de forma regular. Yammer ayuda a facilitar la colaboración comunitaria y el intercambio de ideas para su organización. Puede usar Yammer a través de su explorador o puede instalarlo en su escritorio o dispositivo móvil.



### Qué es una red de Yammer

Una red de Yammer se usa para representar a personas que forman parte de una sola organización y que colaboran con regularidad. Todos los usuarios que forman parte del mismo espacio empresarial de Microsoft 365 (con una suscripción válida de Yammer) pueden usar Yammer para trabajar juntos.

Su organización puede configurar un dominio en Microsoft 365 para comenzar a usar Yammer. Por ejemplo, si el dominio de su organización es contoso.com, los usuarios de

su organización pueden acceder a la red de Yammer yendo a <https://www.yammer.com/contoso.com>.

Las redes de Yammer vienen con muchas configuraciones que su organización puede establecer para ayudar a decidir cómo los usuarios deben tener acceso a Yammer, entre otros:

- Establecer un nombre para su red de Yammer
- Decidir quién puede cargar archivos y hacer cumplir las limitaciones de formato de archivo
- Permitir o restringir qué aplicaciones de terceros se pueden usar
- Decidir si Yammer debe obtener detalles sobre vínculos en mensajes
- Elegir si dar a los usuarios la opción de que Yammer traduzca automáticamente los mensajes
- Configurar un idioma predeterminado para los mensajes de todo el sistema

Su organización puede tener más de una red de Yammer.

## Funciones y capacidades de Yammer

Yammer aporta a sus usuarios características y capacidades para ayudarles a comunicarse, con un enfoque particular en:

- **Comunicación abierta:** Yammer ayuda a los usuarios de toda la organización a comunicarse con otras personas con las que no tendrían la oportunidad de comunicarse de otra manera. Por ejemplo, usuarios de diferentes partes del mundo y con roles laborales distintos pueden unirse para trabajar en un proyecto apasionante o responder preguntas y resolver problemas juntos.
- **Integración perfecta con aplicaciones:** Yammer se conecta con las aplicaciones Microsoft 365 y otras aplicaciones. Por ejemplo, un grupo de usuarios pueden trabajar juntos y editar un documento de sus conversaciones de Yammer.
- **Seguridad:** Yammer le ayuda a aprovechar las características de seguridad de nivel empresarial que Microsoft 365 usa para proteger sus datos.
- **Cumplimiento:** Yammer viene con herramientas como eDiscovery para consultar y administrar datos, diseñadas para ayudarle a cumplir con los requisitos legales y reglamentarios.

Estas son solo algunas de las características disponibles en Yammer:

	<b>Descripción</b>
Organigramas	Yammer puede ayudar a crear organigramas para que los usuarios puedan ver su lugar en la organización.
Directorios de miembros	Los usuarios pueden encontrar personas en su equipo y en toda la organización.

Elogio	Permite a los usuarios compartir insignias y logros por el gran trabajo que realizan.
Sondeos	Los usuarios pueden crear encuestas y recopilar comentarios para ayudar a tomar decisiones.
Fuentes	Permite a sus usuarios mantenerse al día con los proyectos y las conversaciones en toda la organización.
Etiquetas	Los usuarios pueden etiquetar el contenido para encontrar fácilmente archivos y mensajes en toda la organización.
Compartir archivos	Los usuarios pueden compartir archivos en toda la organización y marcarlos como de solo lectura. Los usuarios también pueden ver quién ha accedido por última vez a un archivo o ha realizado cambios.
Anuncios	Permite a los usuarios hacer anuncios para notificar a los usuarios de un grupo.

## Supervisar el uso de Yammer

Yammer permite supervisar cómo se usa para que su organización pueda comprender mejor cómo mejorar la productividad. Yammer aporta diferentes tipos de informes para usar, incluidos los siguientes:

Tipo de informe	Descripción
Informes de actividad de Yammer	Para ayudarle a entender el nivel de compromiso de su organización en Yammer. Aportan información útil sobre las publicaciones de los usuarios, sus actividades de lectura, etc.
Informes de actividad de grupo de Yammer	Obtenga una mejor comprensión de las actividades de los grupos de Yammer en su empresa. Dan información sobre las publicaciones, lecturas y la actividad de los miembros de los grupos.
Informes de utilización de dispositivos de Yammer	Da información sobre los dispositivos que los usuarios utilizan para acceder a Yammer. Encuentre información sobre los tipos de dispositivos, el número de dispositivos, el tipo de sistema operativo y más en toda la organización o en un nivel de usuario individual.

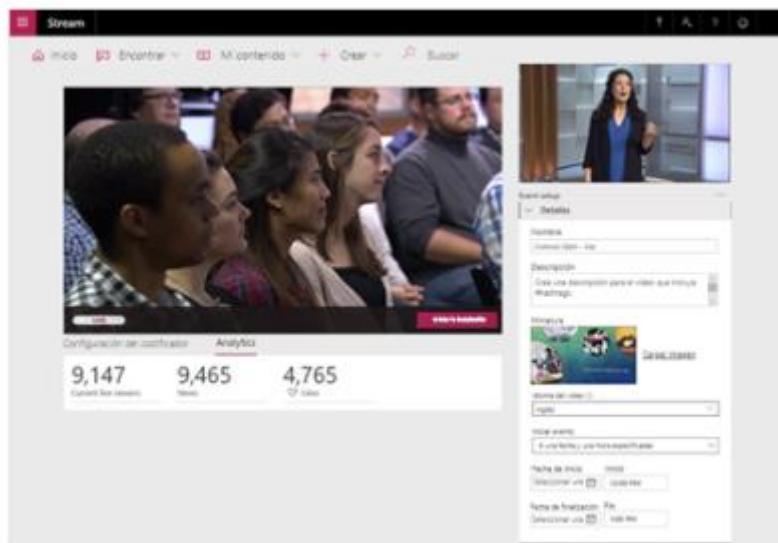
Su organización puede usar el panel de Informes de Microsoft 365 para ver los informes de Yammer. También puede exportar informes a archivo .csv para un análisis más detallado.

# Utilizar Microsoft Stream para interactuar

Su organización crea regularmente contenido audiovisual para mejorar el aprendizaje y la comunicación en toda la organización. Quiere ayudar a su organización a mejorar la forma en que los usuarios interactúan con este contenido.

## Qué es Microsoft Stream

Microsoft Stream es un servicio de vídeo que permite a los miembros de su organización cargar, ver y compartir vídeos de manera segura. Microsoft Stream le permite compartir contenido de vídeo de reuniones, sesiones de entrenamiento, clases y eventos en vivo para facilitar la colaboración de los equipos de su organización.



Para habilitar Microsoft Stream para sus usuarios, su organización puede asignarles licencias de Microsoft Stream desde el centro de administración de Microsoft 365. De esta forma, no tendrán que suscribirse manualmente al servicio.

## Crear y administrar contenido

Hay diferentes formas para que los usuarios creen contenido en Microsoft Stream. Por ejemplo:

- Crear eventos en vivo para hasta 10 000 personas.
- Crear presentaciones.
- Crear encuestas, cuestionarios o sondeos para vídeos.
- Agregar automáticamente subtítulos a los vídeos.

Microsoft Stream también facilita compartir contenido con otros. Los usuarios pueden compartir contenido por correo electrónico, copiando y pegando un vínculo directo al contenido o mediante Yammer, para que los usuarios puedan ver el contenido directamente en Yammer.

## Control del acceso

Microsoft Stream ofrece a su organización un control detallado sobre cómo se ve o se accede al contenido.

Por ejemplo, los usuarios pueden crear canales y grupos para categorizar y organizar el contenido. Microsoft Stream da permisos detallados para personalizar quién puede ver el contenido, a nivel de usuario individual, de grupo o de canal. Puede aprovechar otras medidas de control que incluyen:

- Agregar instrucciones de utilización.
- Bloquear suscripciones.
- Restringir los usuarios de carga.
- Restringir la creación de canales.

## Usar registros de auditoría

Microsoft Stream ayuda a realizar un seguimiento de cómo los usuarios interactúan con el servicio. Aporta registros de auditoría que su organización puede usar para investigar y supervisar actividades en Microsoft Stream. Por ejemplo, para ayudar a cumplir con los requisitos de administración de datos y cumplimiento normativo, su organización puede encontrar información sobre quién ha realizado una acción en particular sobre un elemento determinado en un momento específico.

Los registros de auditoría de Microsoft Stream se pueden encontrar en los registros de auditoría de Microsoft 365. Para acceder a los registros, su organización debe tener:

- El rol de administrador global de Microsoft 365 o de Exchange.
- Una licencia válida de Exchange Online.
- Una licencia válida de buzón de correo de Exchange.

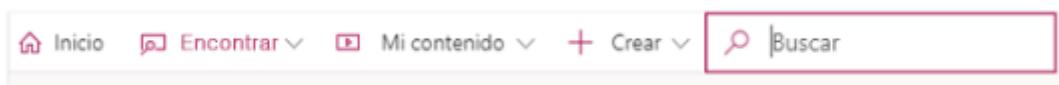
## Usar Microsoft Stream con otras aplicaciones

Microsoft Stream se integra a la perfección con otras aplicaciones Microsoft 365 como Yammer, SharePoint, Microsoft Teams y más. Sus usuarios pueden usar el inicio de sesión único para trabajar fácilmente en Microsoft Stream y estas otras aplicaciones.

## Descubrir contenido

Microsoft Stream está diseñado para ayudar a los usuarios a encontrar y realizar un seguimiento del contenido de su organización.

Los usuarios pueden buscar y encontrar videos introduciendo términos de búsqueda en el campo de búsqueda.



Los resultados se clasifican para los usuarios en vídeos, canales, personas y grupos.

Microsoft Stream no solo verá la descripción o el título de un vídeo cuando busque contenido. Buscará activamente a través de lo que realmente se dice en un vídeo para ver si coincide con los términos de búsqueda de un usuario.

Microsoft Stream mostrará un vídeo coincidente y los códigos de tiempo para cuando los términos de búsqueda coincidan en un vídeo. Los usuarios pueden seleccionar partes coincidentes del vídeo para comenzar a reproducirlo desde ese punto:

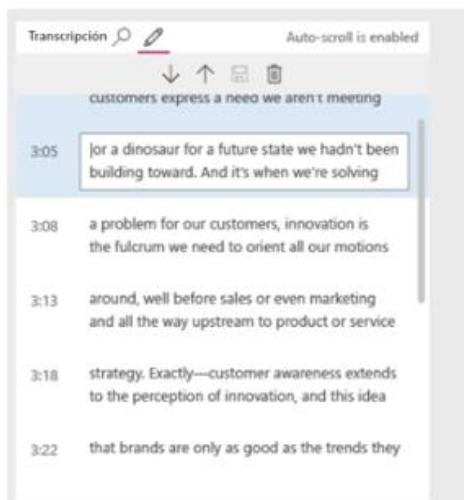


## Retransmitir con inteligencia integrada

Microsoft Stream utiliza el poder de las tecnologías de inteligencia artificial de Microsoft para ayudar a sus usuarios a aprovechar al máximo el contenido. Los usuarios pueden aprovechar las siguientes capacidades:

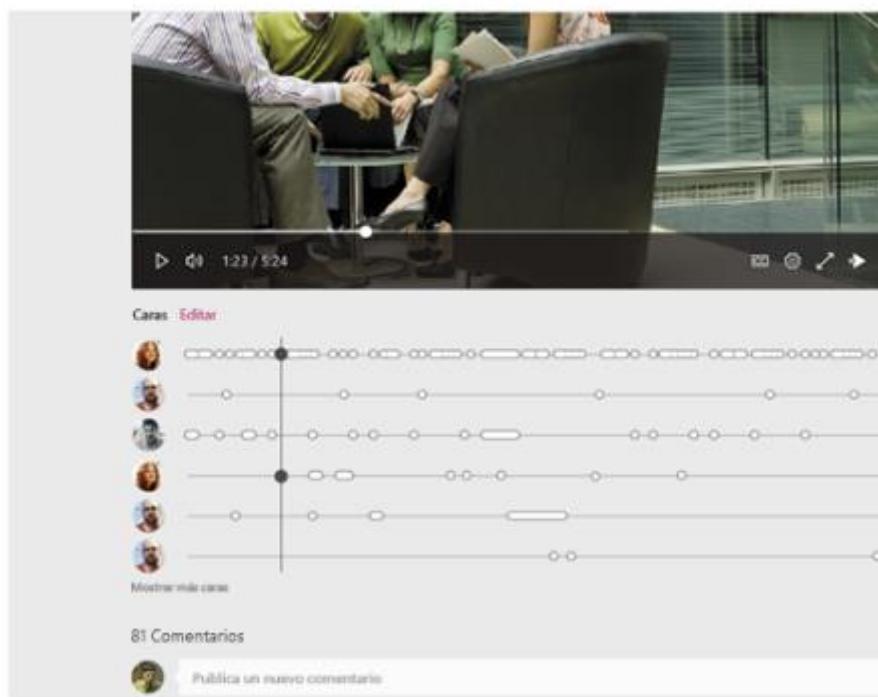
### Subtítulos y modo de transcripción generados automáticamente

Microsoft Stream usa la tecnología de reconocimiento automático de voz para generar subtítulos en vídeos si los usuarios configuran el campo de idioma del vídeo en uno de los idiomas admitidos. Microsoft Stream también puede generar una transcripción deslizante que los usuarios pueden usar para seguir el contenido hablado en un vídeo. Los usuarios también pueden revisar la transcripción una vez que el vídeo haya terminado.



## Detección de personas

Si está habilitado, Microsoft Stream también puede detectar quién está en un vídeo y aporta una línea de tiempo que muestra dónde está activa una persona en particular en un vídeo. De esta manera, los usuarios pueden seguir la contribución de una persona o equipo en particular en un vídeo.



## Ampliar Teams con Power Platform y aplicaciones

Sus equipos pueden utilizar muchas herramientas diferentes al colaborar. Microsoft Teams puede ayudar a sus equipos a utilizar sus herramientas existentes de forma más eficaz.

### Aplicaciones de Microsoft Teams

Su organización puede ampliar las capacidades de Microsoft Teams para ayudar a sus equipos a mejorar la forma en que trabajan. Las aplicaciones de Microsoft Teams amplían las capacidades de Microsoft Teams. Una aplicación de Microsoft Teams es un paquete de servicios y puede constar de extensiones de mensajería, webhooks, bots y pestañas.

Existen diferentes formas para que su organización cree aplicaciones de Microsoft Teams. Por ejemplo, sus desarrolladores pueden usar Node.js. para crear aplicaciones basadas en bots. La forma preferida es usar [App Studio](#) para crear e integrar fácilmente aplicaciones de Microsoft Teams, ya sean aplicaciones personalizadas o aplicaciones de software como servicio que su organización ya usa.

## Pestañas para Microsoft Teams

Las pestañas son páginas web que los usuarios pueden insertar en Microsoft Teams, ya sea en el ámbito de un canal de Teams o a nivel de usuario personal. Los usuarios pueden crear pestañas personalizadas para incluir contenido web para agregar la funcionalidad de Microsoft Teams a las páginas web.

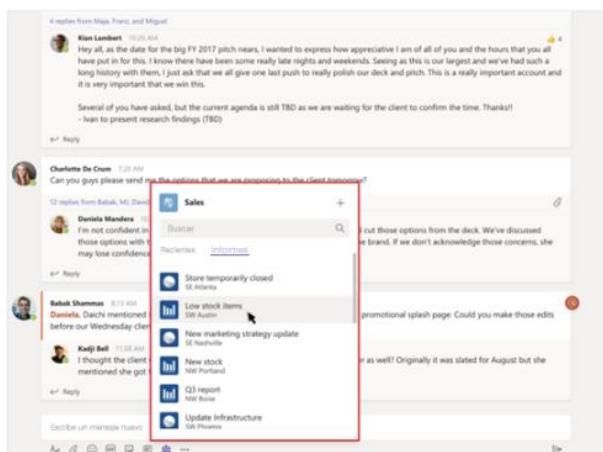
Las pestañas también se pueden usar para integrar Microsoft Teams con aplicaciones como Power BI. Por ejemplo, los usuarios pueden usar pestañas para insertar informes interactivos de Power BI en sus canales y chats de Microsoft Teams:



Las pestañas también se pueden usar como páginas de soporte técnico para extensiones de mensajería y bots de Microsoft Teams.

## Extensiones de mensajes y bots

Las extensiones de mensajes permiten a los usuarios de su organización interactuar con los servicios web de Microsoft Teams. Esto hace posible que los usuarios activen acciones y ejecuten consultas en un sistema externo, directamente desde Microsoft Teams. Por ejemplo, un usuario puede activar un comando de búsqueda desde el cuadro de mensaje para buscar artículos con pocas existencias en un inventario de ventas:

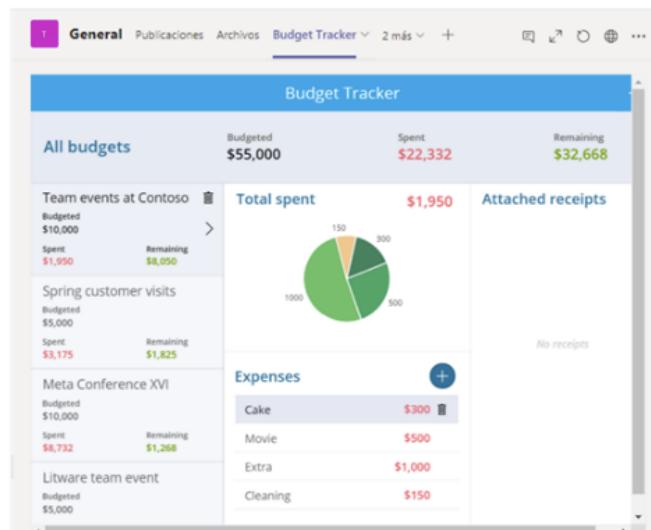


Sus usuarios también pueden aprovechar los bots con Microsoft Teams. Los bots permiten a sus usuarios interactuar con otros servicios de una manera sofisticada enviando mensajes y recibiendo respuestas del bot. Los bots se pueden usar en un canal de Teams o en conversaciones individuales.

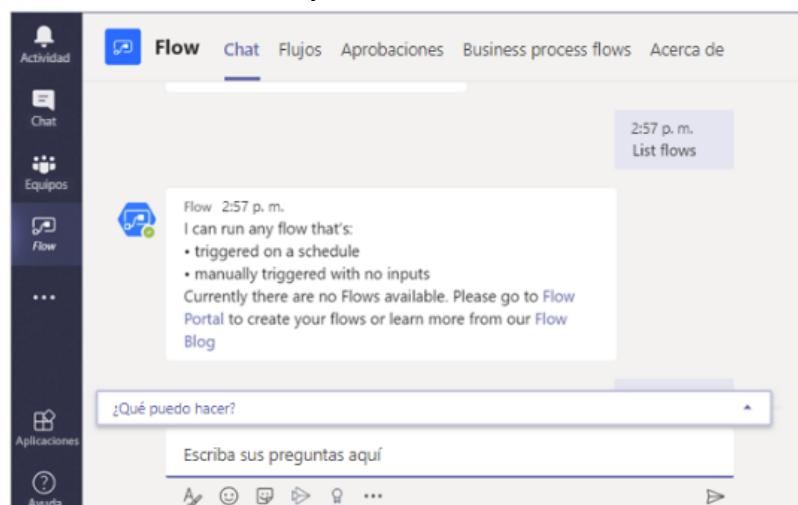
## Integración de Power Platform

Si sus equipos utilizan Power Platform, Microsoft Teams puede integrarse con las soluciones de Power Platform para ayudar a sus equipos a colaborar y sacar el máximo partido de sus soluciones. Hay diferentes formas de hacer esto, por ejemplo:

- **Power Virtual Agents:** Los usuarios pueden crear chatbots utilizando Power Virtual Agents sin escribir ningún código. Los usuarios pueden integrar esos bots en Microsoft Teams publicando los bots y haciéndolos accesibles a Microsoft Teams desde el portal de Power Virtual Agents.
- **PowerApps:** Los usuarios pueden crear aplicaciones en PowerApps. Luego, esas aplicaciones se pueden agregar directamente a Microsoft Teams creando pestañas para esas aplicaciones. Se puede acceder a las aplicaciones desde esas pestañas:



- **Power Automate:** Los usuarios pueden crear flujos para automatizar tareas en Power Automate. Se pueden activar desde Microsoft Teams:



## Aplicaciones y servicios de terceros

Su organización puede integrar Microsoft Teams con aplicaciones y servicios de terceros a través de webhooks y conectores. Los webhooks y conectores ayudan a simplificar la conexión de servicios web a canales y equipos dentro de Microsoft Teams.

### Webhooks

Microsoft Teams habilita a sus usuarios con webhooks salientes y entrantes.

Los webhooks salientes permiten a sus usuarios enviar mensajes de texto a los servicios web de su organización. Luego, sus servicios pueden responder con un mensaje que consta de texto o una tarjeta que incluye contenido de texto e imagen.

Los webhooks entrantes también están disponibles. Los webhooks entrantes permiten que sus servicios externos envíen mensajes a sus canales de Teams a través de un punto de conexión HTTP. Esto es útil para las herramientas de notificación y seguimiento.

### Conectores

Los conectores son una forma de que sus usuarios se suscriban para recibir alertas e información de sus servicios web.

Los usuarios pueden encontrar conectores haciendo clic derecho en el canal de un equipo y seleccionando **Conectores**. Luego, pueden agregar conectores de la lista de conectores disponibles para agregar a un canal:

The screenshot shows the 'Connectors' page for the 'General' channel in the 'Contoso' team. The page title is 'Conectores del canal "General" del equipo "Contoso"'. It includes a search bar, a 'Todos' filter, and an 'Ordenar por: Popularidad' dropdown. On the left, there's a sidebar with 'ADMINISTRAR' sections for 'Configurado' (Mis Cuentas) and 'CATEGORÍA' (Todos, Análisis, CRM, Asistencia Al Cliente, Herramientas Del Desarrollador, RR. HH., Marketing, Noticias Y Redes Sociales, Administración De Proyectos). The main area displays a list of connectors under 'Conectores para su equipo':

Conector	Descripción	Opciones
Formularios	Cree fácilmente encuestas, cuestionarios y sondeos.	Configurar
Azure DevOps	Realice el seguimiento de las tareas pendientes y colabore en proyectos.	Agregar
RSS	Obtenga fuentes RSS para su grupo.	Agregar
Webhook entrante	Envíe datos de un servicio a su grupo de Office 365 en tiempo real.	Agregar
Jira Cloud	Recopile, organice y asigne los problemas detectados en el software.	Agregar
Yammer	Recibir actualizaciones de la red de Yammer	Agregar

Además de las aplicaciones y los servicios de Microsoft, los usuarios pueden encontrar conectores para aplicaciones de terceros como GitHub, Bitbucket, Salesforce y muchas más.

Por último, los usuarios pueden usar los conectores de Office 365. Los conectores Office 365 permiten a los usuarios crear páginas de configuración personalizadas para webhooks entrantes y empaquetarlas como parte de una aplicación de Microsoft Teams. Pueden utilizar este tipo de conector para trabajar con otras aplicaciones, como Outlook. Su organización puede publicar este tipo de conector internamente y también en la App Store de Microsoft.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Cómo se puede agregar una aplicación de PowerApps al canal de Microsoft Teams?

- A. Creando un webhook.
- B. Creando una pestaña.
- C. Creando un bot.

¿Dónde se agregan las salas de reuniones de Microsoft Teams al crear una nueva reunión de Teams?

- A. Las salas estarán disponibles en el menú desplegable Sala en el nuevo formulario de reunión.
- B. Las salas no estarán disponibles en el nuevo formulario de reunión en Microsoft Teams.
- C. Las salas estarán disponibles en el menú desplegable Ubicación del nuevo formulario de reunión.

¿Qué informe contiene el número de usuarios que acceden a Yammer desde un teléfono móvil?

- A. Informes de actividad de Yammer.
- B. Informes de actividad de grupo de Yammer.
- C. Informes de utilización de dispositivos de Yammer.

¿Qué servicios de Microsoft 365 reúne Ideas Microsoft Viva para permitir a los usuarios, administradores y líderes mejorar la productividad y el bienestar de la organización?

- A. MyAnalytics, SharePoint, Yammer
- B. Workplace Analytics, MyAnalytics, Delve
- C. MyAnalytics, Workplace Analytics, Glint

# Almacenamiento y uso compartido de archivos con OneDrive y SharePoint

## Introducción

Mover cargas de trabajo a la nube le permite implementar un recurso mundial que sus empleados pueden usar para compartir archivos, administrar proyectos y participar en reuniones en línea. Puede almacenar y acceder a archivos de forma fácil y segura desde todos sus dispositivos. Los empleados pueden trabajar con otros independientemente de si están dentro o fuera de su organización y dejar de compartir cuando lo deseen. Microsoft 365 le ayuda a comunicarse a gran escala para llegar a las personas donde sea que se encuentren con experiencias digitales convincentes para los empleados.

Al final de este módulo, debería ser capaz de hacer lo siguiente:

- Describir las características de OneDrive.
- Describir las características y la funcionalidad de SharePoint.

## Requisitos previos

- Ninguno

## OneDrive en Microsoft 365

### OneDrive

OneDrive es un servicio en la nube que le permite almacenar y proteger archivos, compartirlos con otros usuarios, acceder a ellos desde cualquier lugar utilizando una aplicación o explorador web y restaurarlos todos a una fecha y hora anteriores. Puede almacenar y acceder a sus archivos de forma fácil y segura desde todos sus dispositivos. Puede trabajar con otras personas independientemente de si están dentro o fuera de su organización y dejar de compartir cuando lo deseé. OneDrive ayuda a proteger su trabajo a través del cifrado avanzado mientras los datos están en tránsito y en reposo en los centros de datos.

### Por qué implementar OneDrive

La mayoría de las funciones avanzadas centradas en la empresa en OneDrive están disponibles para cada tipo de suscripción, lo que permite a las empresas usar OneDrive de la manera que más beneficie a su negocio, ya sea simplemente un recurso compartido de archivos basado en la nube para una pequeña empresa o un sistema de almacenamiento muy utilizado que da la base para toda la colaboración dentro de una empresa. Pero en esencia, OneDrive le permite compartir de forma segura y trabajar juntos en todos sus archivos. Con OneDrive, puede:

- **Acceda a archivos desde todos sus dispositivos.** Acceda a todos sus archivos personales y a los archivos que otros comparten con usted en todos sus dispositivos, incluidos dispositivos móviles, Mac, PC y un explorador web.
- **Compartir dentro o fuera de su organización.** Comparta archivos de forma segura con personas dentro o fuera de su organización utilizando su dirección de correo electrónico, incluso si no tienen una cuenta de servicios de Microsoft. Esta experiencia de uso compartido común está disponible en las versiones web, móvil y de escritorio de OneDrive.
- **Colaborar con la integración profunda de Microsoft Office.** La coautoría de documentos está disponible en Web Apps de Office, Mobile Apps de Office y las aplicaciones de escritorio de Office, lo que le ayuda a mantener una única versión funcional de cualquier archivo. Solo OneDrive aporta capacidades de coautoría en aplicaciones de Office en todos sus dispositivos.
- **Encuentre rápidamente los archivos más importantes.** La búsqueda de contenido en su OneDrive se simplifica gracias a la inteligencia de la interfaz de programación de aplicaciones de Microsoft Graph. Esta tecnología simplifica la búsqueda de lo que es importante al dar recomendaciones de archivos basadas en su relación con otras personas, cómo recibió varios archivos y cuándo accedió a ellos por última vez.
- **Proteja sus archivos con seguridad de nivel empresarial.** OneDrive tiene muchas características de seguridad y cumplimiento, lo que le permite satisfacer algunos de los requisitos de cumplimiento más estrictos que existen.

## Funciones clave de OneDrive

Las funciones enumeradas en esta sección abordan las preocupaciones comunes de los clientes o los requisitos de cumplimiento específicos, o aportan una funcionalidad única disponible solo en OneDrive:

- **Movimiento de carpeta conocido.** Hace que sea más fácil mover archivos en las carpetas Escritorio, Documentos e Imágenes de sus usuarios a OneDrive. Esto permite a los usuarios seguir trabajando en las carpetas con las que están familiarizados y acceder a sus archivos desde cualquier dispositivo.
- **Archivos a petición de OneDrive.** Permite a los usuarios ver, buscar e interactuar con archivos almacenados en OneDrive desde el Explorador de archivos, sin descargarlos todos en su dispositivo. Esta característica da una apariencia perfecta tanto para OneDrive como para archivos locales, sin ocupar espacio en el disco duro local.
- **Archivos adjuntos modernos.** OneDrive se integra con Outlook para permitir un intercambio fluido de archivos de OneDrive que aparecen como archivos adjuntos de correo electrónico. Esta característica da una experiencia de uso compartido familiar, pero centraliza el almacenamiento de archivos adjuntos en OneDrive. Aporta beneficios de colaboración, como el control de versiones que normalmente se pierde cuando los usuarios envían y reciben documentos por correo electrónico.

- **Colaboración en equipo en tiempo real.** Coautoría en versiones completas de Microsoft Word, Excel y PowerPoint.
- **Restauración de archivos de OneDrive.** Permite a los usuarios restaurar archivos a cualquier estado de los últimos 30 días. Para seleccionar el tiempo de recuperación deseado, OneDrive presenta a los usuarios un histograma que muestra la actividad del archivo para que puedan determinar qué tiempo de recuperación satisface sus necesidades. A partir de ahí, los usuarios simplemente seleccionan la entrada del historial de archivos que desean restaurar, y todos los cambios posteriores a ese punto se revertirán.
- **Papelera de reciclaje.** Una papelera de reciclaje similar a la disponible en el escritorio de Windows. Los archivos eliminados se mueven a la papelera de reciclaje y se guardan durante un tiempo designado antes de ser eliminados permanentemente. En las cuentas laborales o educativas, los archivos eliminados se purgan después de 93 días, a menos que se configure de otra manera.
- **Auditoría y elaboración de informes.** Capacidades detalladas de informes y auditoría para los archivos que almacena OneDrive, así como para los archivos almacenados a través de otros servicios, como Microsoft SharePoint. También puede auditar acciones individuales de archivos, como las descargas, cambios de nombre y visualizaciones.
- **Cifrado de datos en tránsito y en reposo.** OneDrive utiliza métodos avanzados de cifrado de datos entre su cliente y el centro de datos, entre los servidores en el centro de datos y en reposo. En reposo, OneDrive usa el cifrado de disco a través del cifrado de unidad BitLocker y el cifrado de archivos para proteger sus datos. Cada archivo está cifrado con su propia clave de cifrado. Todo lo que supere los 64 KB se divide en fragmentos individuales, cada uno de los cuales tiene su propia clave de cifrado bloqueada en un almacén de claves.
- **Claves de cifrado controladas por el cliente.** Al usar una característica de Office 365 llamada cifrado de servicio con clave de cliente, puede cargar sus propias claves de cifrado en Azure Key Vault. Utilice estas claves para cifrar sus datos en reposo en los centros de datos de Azure. Aunque este cifrado se realiza de forma nativa a través de BitLocker, los clientes pueden requerir el uso de su propia clave para cumplir con los requisitos de seguridad. Si los usuarios pierden su clave, pueden recuperar la clave eliminada de la papelera de reciclaje hasta por 90 días (según su configuración).
- **Caja de seguridad del cliente de Microsoft 365.** Si un ingeniero de soporte técnico de Microsoft necesita acceder a sus datos para resolver un problema, primero debe obtener la aprobación de un administrador de Microsoft. La función caja de seguridad del cliente de Office 365 agrega un requisito a ese proceso: debe aprobar o rechazar ese acceso antes de que el ingeniero de soporte técnico pueda acceder a sus datos. Con la caja de seguridad del cliente, también establece límites sobre cuánto tiempo el ingeniero puede acceder a sus datos, y toda la actividad durante ese tiempo se registra con fines de auditoría.
- **Ubicaciones de almacenamiento de OneDrive Multi-Geo.** Multi-Geo es una característica de Office 365 que permite a las organizaciones distribuir su almacenamiento en varias ubicaciones geográficas de Office 365 y especificar en cuál de ellas almacenar los datos de los usuarios. Podrá

establecer geografías de almacenamiento para cada usuario. Para los clientes multinacionales con requisitos de residencia de datos, puede utilizar esta característica para garantizar que los datos de cada usuario se almacenen en la ubicación geográfica necesaria para el cumplimiento.

- **Nube de administración pública.** OneDrive está disponible en los planes de Office 365 Administración Pública para Estados Unidos. Para obtener información sobre estos planes, consulte [Office 365 Administración Pública de EE. UU..](#)

## Opciones de implementación y administración

Puede implementar y administrar OneDrive de muchas maneras, pero ciertas opciones tienen más sentido en organizaciones más grandes que en empresas más pequeñas y viceversa. Por ejemplo, probablemente no tendría sentido tener una solución de administración empresarial como Microsoft Endpoint Configuration Manager para una empresa que tiene solo 10 empleados. La Tabla 1 describe las herramientas de implementación y administración que normalmente se utilizan para pequeñas y medianas empresas.

**Nota:** Tenga en cuenta que una organización de una determinada categoría de tamaño probablemente incorporará opciones adicionales de otras categorías de tamaño. Esta tabla no pretende identificar exclusivamente una tecnología con un tamaño de negocios específico.

Tamaño de la organización	Herramientas de implementación utilizadas	Administración
Empresa pequeña	Instalación local	Centro de administración de OneDrive
Empresa mediana	Instalación generada por script o administración de dispositivos móviles (MDM) de Microsoft Intune	Office 365 con MDM, centro de administración de OneDrive, administración de aplicaciones móviles de Intune (MAM) o MDM
Empresa	Microsoft Endpoint Manager con Intune o Windows Autopilot	Microsoft Endpoint Configuration Manager, objetos de directiva de grupo (GPO), etc.

Dependiendo de dónde encaja su organización en esta tabla y las tecnologías disponibles para usted, puede elegir qué parte de esta guía utilizar. Por ejemplo, si tiene un pequeño negocio, es posible que desee mantener la implementación simple de OneDrive instalando la aplicación de sincronización manualmente en los equipos de sus empleados y utilizando el centro de administración de OneDrive para administrar algunas configuraciones para sus usuarios. Alternativamente, si está ejecutando una empresa, puede optar por implementar y administrar OneDrive mediante el uso de herramientas avanzadas como Microsoft Endpoint Configuration Manager y la Directiva de grupo, y podría usar las secciones que corresponden a esas herramientas, en su lugar. Para adaptarse a diversas situaciones, las partes de implementación y

administración de esta guía tienen un formato modular para que pueda consultar el documento de la manera que mejor se adapte a sus necesidades y capacidades de implementación. Este formato también aporta visibilidad de tecnologías alternativas para mejorar sus procesos actuales.

## Requisitos previos

- **Requisitos del cliente y de la aplicación.** Aunque puede cargar, descargar e interactuar con sus archivos de OneDrive desde un explorador web, la experiencia ideal de OneDrive proviene de las aplicaciones de sincronización de Windows y Mac, y las aplicaciones móviles de iOS y Android. Con eso en mente, OneDrive está disponible para la mayoría de los sistemas operativos y exploradores, y requiere un hardware mínimo.
- **Requisitos de licencia.** Existen varios métodos mediante los cuales puede adquirir una licencia para OneDrive. Pero algunas funciones de OneDrive solo están disponibles en determinados modelos de licencia. Para obtener información sobre los requisitos de licencia de OneDrive, sus funciones avanzadas y cualquier licencia especial necesaria para ellas, consulte [Planes de Office 365](#).

## Preparar su entorno

Antes de implementar OneDrive, prepare su entorno

## Utilización de la red

Una variedad de factores puede afectar la cantidad de ancho de banda de red que usa OneDrive. Para obtener la mejor experiencia, le recomendamos que evalúe este impacto antes de realizar una implementación completa de OneDrive en su organización.

## Multi-Geo

Si tiene requisitos de residencia de datos, considere usar OneDrive Multi-Geo. Con OneDrive Multi-Geo, puede especificar una ubicación de datos preferida (PDL) de entre las ubicaciones disponibles en todo el mundo para el OneDrive de cada usuario. Para obtener información detallada sobre OneDrive Multi-Geo, consulte [Capacidades de Multi-Geo en OneDrive y SharePoint en Microsoft 365](#).

Se ofrece soporte técnico a los usuarios que hayan comenzado a usar OneDrive, ya sea antes o después de configurar OneDrive Multi-Geo.

Las funciones como la sincronización de archivos y la administración de dispositivos móviles funcionan normalmente en un entorno multigeográfico. No hay ninguna configuración o administración especial.

Decisiones clave:

- ¿Planea utilizar OneDrive Multi-Geo?
- ¿Tendrá OneDrive Multi-Geo completamente configurado antes de que sus usuarios comiencen a usar OneDrive?

## Híbrida

Si actualmente usa OneDrive o MySites en SharePoint Server local, le recomendamos que implemente OneDrive híbrido. Con OneDrive híbrido, los usuarios son redirigidos desde su OneDrive local a OneDrive en Microsoft 365. OneDrive híbrido permite una navegación fluida a OneDrive en la nube desde SharePoint local y Microsoft 365.

Si no usa OneDrive en SharePoint Server, pero tiene un entorno de SharePoint local, es posible que desee considerar la implementación de OneDrive híbrido. Al hacerlo, se actualizarán los vínculos de navegación de OneDrive en SharePoint Server para que apunten a OneDrive en Microsoft 365, nuevamente, aportando a sus usuarios una navegación fluida a OneDrive en la nube desde cualquier ubicación.

## SharePoint en Microsoft 365

### SharePoint

SharePoint es la evolución en la nube de Microsoft SharePoint Server. Es un servicio en la nube que le permite almacenar, organizar y agregar aplicaciones de terceros, acceder a información desde casi cualquier dispositivo y permitir el intercambio con personas externas de forma predeterminada, todo desde un explorador web. Ayuda a crear equipos o sitios enfocados a la comunicación para una colaboración y comunicación eficiente. Los usuarios internos con una licencia apropiada de Microsoft 365 o SharePoint pueden utilizar SharePoint. Pueden compartir archivos o carpetas con otras personas dentro o fuera de la organización. El intercambio fuera de la organización puede ser controlado por los administradores del sitio.

Con SharePoint, los usuarios pueden:

- Crear sitios y páginas, bibliotecas de documentos y listas.
- Agregar partes de la web para personalizar sus páginas.
- Compartir objetos visuales, noticias y actualizaciones importantes con un equipo o de forma más amplia.
- Buscar y descubrir sitios, archivos, personas y noticias de toda su organización.
- Administrar sus procesos comerciales con flujos, formularios y listas.
- Trabajar sobre documentos en coautoría con otros usuarios.
- Sincronizar y almacenar sus archivos en la nube para que cualquiera pueda trabajar con ellos de forma segura.
- Ponerse al día con las noticias sobre la marcha con la aplicación móvil SharePoint.

### Colaboración

SharePoint aporta un entorno de colaboración enriquecido donde las personas dentro y fuera de su organización pueden trabajar juntas, elaborando en coautoría documentos. Microsoft 365 ofrece una variedad de opciones para crear un entorno de colaboración de archivos seguro y productivo que satisfaga las necesidades de su organización.

### SharePoint: la intranet inteligente

Aproveche al máximo la potencia de la intranet inteligente para comunicarse de forma efectiva en su organización, involucrar a los empleados y acceder a la información y los conocimientos relevantes. Transforme las comunicaciones y experiencias digitales de los empleados con un enfoque de 4 pasos para que sus equipos estén conectados en línea con Microsoft 365.

## Explorar

Descubra formas de crear una intranet inteligente y atractiva que conecte a sus empleados con compañeros, noticias, conocimientos y aplicaciones. Para crear una intranet potente y atractiva, todo lo que necesita es un poco de inspiración. Eche un vistazo a estos diseños recientes y experiencias modernas con el [Libro de apariencias de SharePoint](#)

## Coordinarse

Coordíñese con su equipo y superen los obstáculos más comunes junto con las demás personas interesadas entendiendo, en primer lugar, los objetivos de su negocio y de las otras partes. Después, identifique las situaciones de intranet que muestren la forma en la que sus empleados utilizan SharePoint y Microsoft 365 para conseguir sus objetivos. Y, por último, determine cuál es el mayor impacto y la situación más sencilla para implementarlo y encontrará el punto de partida que estaba buscando.

## Implementar

Acelere el tiempo de creación de valor con prestaciones y situaciones listas para usar que le ayuden a implementar con facilidad. Microsoft 365 ofrece plantillas que le ayudarán a definir sus objetivos, roles, experiencias y métricas para poder diseñar e implementar la experiencia de su intranet con el mínimo esfuerzo.

## Interactuar

Lance su nueva intranet con un plan de adopción que tenga a su equipo listo para interactuar correctamente. Antes del lanzamiento, deberá tener un plan de adopción para garantizar que los empleados conocen la intranet y cómo pretende aumentar la interacción habitual. Microsoft 365 ha creado los planes aprendizaje, proyecto, cuaderno de estrategias y adopción de SharePoint para ayudar a las organizaciones a realizar una implementación adecuada.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Cuál de los siguientes términos describe la forma en que los datos de OneDrive se almacenan globalmente?

- A. Multigeográfico
- B. Centro de datos geocéntrico
- C. Colocación

¿Cuál de las siguientes afirmaciones describe los tipos de sitios que se pueden crear desde la página de inicio de SharePoint?

- A. Skype
- B. Equipo
- C. OneDrive

# Module 2 - Demostrar conocimientos fundamentales de las capacidades de administración empresarial de Microsoft 365

## Administrar su negocio con Microsoft 365

### Introducción

En el vertiginoso panorama empresarial actual, la capacidad de una organización para adaptarse rápidamente y responder al cambio es vital. Esto significa capacitar a sus empleados para que sean lo más productivos posible, simplificando y automatizando los procesos mientras se mantiene la seguridad y el cumplimiento. Microsoft 365 tiene un conjunto de herramientas y servicios que permitirán que su organización y sus empleados trabajen de manera más eficiente.

Al final de este módulo, será capaz de hacer lo siguiente:

- Describir cómo Microsoft 365 potencia a las organizaciones con herramientas para mejorar la productividad organizativa.
- Identificar las soluciones de administración empresarial y cómo se correlacionan con productos específicos.

### Productividad en la organización

Toda organización busca impulsar el crecimiento, reducir costes y dar un mejor servicio a sus clientes. Microsoft 365 proporciona a las organizaciones la capacidad de optimizar el negocio y cumplir sus objetivos mediante el uso de herramientas como Workplace Analytics. Al mismo tiempo, existen más exigencias para mejorar y mantener la seguridad y garantizar que se satisfagan las regulaciones de cumplimiento y se reduzca el riesgo de privacidad.

Con Microsoft 365 puede alcanzar sus objetivos a través de:

- Administración simplificada: simplifique la administración de todos los dispositivos de su patrimonio a través de Microsoft Endpoint Manager (MEM).
- Automatización de procesos de negocio: proporcione a su organización la capacidad de automatizar tareas que requieren mucho tiempo, optimizar las operaciones y aportar un nuevo nivel de eficiencia a su organización.

- Extensibilidad: permita a los desarrolladores y socios crear aplicaciones personalizadas o ampliar y personalizar las aplicaciones de Office, SharePoint y Microsoft Teams.
- Administración de formularios y flujo de trabajo: capture, realice seguimiento y actúe en función de los datos y las solicitudes con aplicaciones y herramientas integradas diseñadas para simplificar y administrar los procesos del flujo de trabajo
- Inteligencia empresarial: transforme sus datos para crear información valiosa y procesable para su organización.
- Administración del trabajo: administre sus proyectos de forma más eficaz y comparta la información del proyecto con su equipo y las partes interesadas a través de Microsoft Planner y Microsoft 365 Groups.

## Workplace Analytics

Workplace Analytics y MyAnalytics utilizan datos recopilados de las actividades diarias de su organización para identificar patrones de colaboración que afectan la productividad, la eficacia de los recursos y el compromiso de los empleados.

Workplace Analytics le proporcionará conocimientos basados en IA que crean comportamientos procesables que puede aplicar a la forma en que su organización se comporta y reacciona al cambio.

## Ventajas de usar Workplace Analytics

El uso de Workplace Analytics en su organización puede proporcionar contexto a los datos, lo que le ayudará a realizar lo siguiente:

- Solucionar la colaboración improductiva y las referencias culturales de las reuniones.
- Mejorar la eficiencia y la eficacia del proceso
- Impulsar las transformaciones culturales.
- Informar la excelencia y el desarrollo del liderazgo.
- Visualizar datos con paneles e informes de Power BI y otras herramientas de informes.
- Informar iniciativas de liderazgo y desarrollo.
- Desarrollar cuadros de mando ejecutivos y sistemas de informes.

## Puntuación de seguridad de Microsoft

La Puntuación de seguridad de Microsoft es una medida de la posición de seguridad de una organización, según la que un número más alto indica más acciones de mejora tomadas. Seguir las recomendaciones de la puntuación de seguridad puede proteger a su organización de las amenazas. Desde un panel centralizado en el Centro de seguridad de Microsoft 365, las organizaciones pueden supervisar y mejorar la seguridad de sus identidades, datos, aplicaciones, dispositivos e infraestructura de Microsoft 365.

La puntuación de seguridad ayuda a las organizaciones a:

- Informar sobre el estado actual de la posición de seguridad de la organización.

- Mejorar su posición de seguridad al aportar detectabilidad, visibilidad, orientación y control.
- Comparar con puntos de referencia y establecer indicadores clave de rendimiento (KPI).

## Administración simplificada

Hoy en día en el trabajo, los departamentos de TI admiten varios tipos de dispositivos configurados de diferentes formas. Su organización puede tener teléfonos móviles Android e iOS, equipos con Windows 10 y macOS y dispositivos personalizados que sus usuarios llevan al trabajo.

Microsoft proporciona las herramientas y los servicios que le permitirán simplificar la administración de todos estos dispositivos. Microsoft Endpoint Manager (MEM) le ayuda a resolver el desafío de la administración de dispositivos en el entorno actual de trabajo remoto y móvil. MEM es una solución de administración inteligente y segura que mejora la productividad y la colaboración con las experiencias familiares que esperan los usuarios y proporciona al departamento de TI la flexibilidad necesaria para dar soporte a diversos escenarios tanto con dispositivos Bring Your Own Device (BYOD) como con dispositivos corporativos.

Endpoint Manager combina servicios que es posible que conozca y ya esté usando, como Microsoft Intune, Configuration Manager, Análisis de escritorio, administración conjunta, Microsoft Defender y Windows AutoPilot. Estos servicios forman parte de la pila de Microsoft 365 para ayudar a garantizar un acceso seguro, proteger los datos y responder y administrar los riesgos.

Endpoint Manager incluye los siguientes servicios:

- **Microsoft Intune:** Intune es un proveedor totalmente basado en la nube de administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM) para sus aplicaciones y dispositivos. Le permite controlar características y parámetros de configuración en dispositivos Android, Android Enterprise, iOS/iPadOS, macOS y Windows 10. **Configuration Manager:** Configuration Manager es una solución de administración local para administrar escritorios, servidores y equipos portátiles que se encuentren en su red o en Internet. Puede habilitarla en la nube para que se integre con Intune, Azure Active Directory (AD), ATP de Microsoft Defender y otros servicios en la nube. Configuration Manager ofrece un amplio conjunto de funcionalidades que le permiten personalizar las siguientes áreas:
  - Administración de aplicaciones
  - Implementación de sistema operativo
  - Administración de actualización de software
  - Cumplimiento de dispositivos
- **Administración conjunta:** La administración conjunta combina su inversión de Configuration Manager local existente con la nube mediante Intune y otros servicios en la nube de Microsoft 365. Elija si Configuration Manager o Intune es la entidad de administración de los siete grupos de

cargas de trabajo diferentes. Como parte de Endpoint Manager, la administración conjunta utiliza características en la nube, incluido el acceso condicional.

- **Desktop Analytics:** Análisis de escritorio es un servicio basado en la nube que se integra con Configuration Manager. Proporciona información detallada e inteligente para que pueda tomar decisiones más fundamentadas sobre la preparación de actualizaciones de sus clientes Windows. El servicio combina datos de su organización con datos agregados de millones de dispositivos conectados a la nube de Microsoft.
- **Windows Autopilot:** Windows Autopilot prepara y preconfigura nuevos dispositivos y los prepara para su uso. Está diseñado para simplificar el ciclo de vida de los dispositivos Windows, tanto para los usuarios de TI como para los finales, desde la implementación inicial hasta el final de su ciclo de vida. Puede usar Autopilot para preconfigurar dispositivos e inscribirlos automáticamente en Intune. También puede integrar Autopilot con Configuration Manager y la administración conjunta para configuraciones de dispositivo más complejas (en versión preliminar).
- **Azure Active Directory (AD):** Endpoint Manager usa Azure AD para la identidad de dispositivos, usuarios, grupos y la autenticación multifactor (MFA). Azure AD Premium, que puede ser un coste añadido, tiene características adicionales para ayudar a proteger los dispositivos, las aplicaciones y los datos, incluidos los grupos dinámicos, la inscripción automática y el acceso condicional.
- **Centro de administración de Endpoint Manager:** El [centro de administración](#) es un sitio web único para crear directivas y administrar los dispositivos. Se conecta a otros servicios clave de administración de dispositivos, incluidos los grupos, la seguridad, el acceso condicional y los informes. Este centro de administración también muestra los dispositivos administrados por Configuration Manager e Intune (en versión preliminar).

## Automatización de procesos de negocio

Cada negocio tendrá una buen número de tareas repetitivas que requieren mucho tiempo y que deben realizarse para que la compañía funcione. Estas tareas pueden abarcar desde las campañas de marketing por correo electrónico hasta la administración de solicitudes de los empleados. En el vertiginoso mundo empresarial actual, en el que el cliente espera una respuesta inmediata a cada consulta, puede resultar complicado ofrecer un servicio de calidad. La automatización de procesos de negocio le proporciona a su organización la capacidad de automatizar tareas que requieren mucho tiempo, optimizar las operaciones y conseguir un nuevo nivel de eficiencia. La automatización de procesos permite a sus empleados usar sus aptitudes en los trabajos para los que fueron contratados en lugar de en tareas rutinarias que pueden consumir un tiempo valioso.

La automatización de procesos de negocio se puede usar para optimizar una variedad de procesos, entre los que se incluyen:

- Administración de documentos
- Automatización del flujo de trabajo

- Alertas de tareas por correo electrónico
- Campañas de marketing por correo electrónico
- Cartas de agradecimiento
- Recordatorios de pagos
- Revisión y aprobación de documentos
- Administración de solicitudes de los empleados

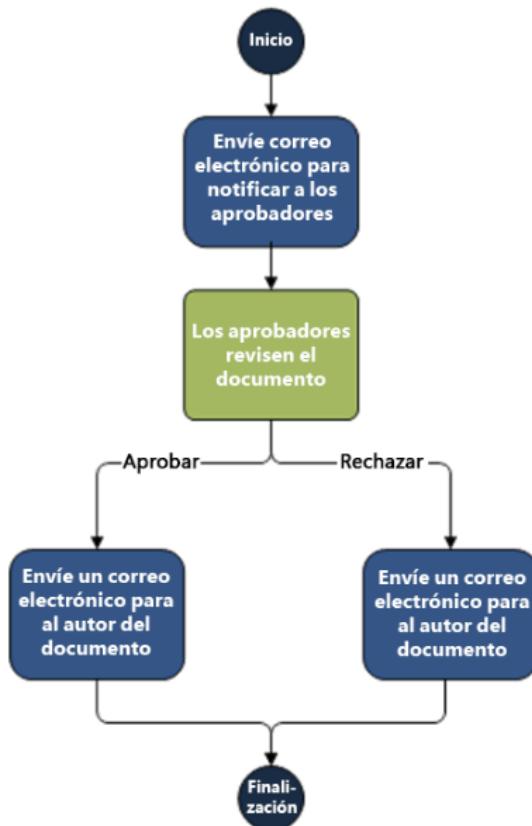
Microsoft 365 ofrece varias herramientas, servicios o aplicaciones para permitir la automatización:

- SharePoint
- Power Automate
- Power Apps

## Usar SharePoint para ofrecer la automatización de procesos de negocio

Los flujos de trabajo de SharePoint son miniaplicaciones preprogramadas que agilizan y automatizan una amplia variedad de procesos de negocio. Los flujos de trabajo pueden incluir la recopilación de firmas, comentarios o aprobaciones para un plan o documento con el fin de realizar un seguimiento del estado actual de un procedimiento de rutina. Los flujos de trabajo de SharePoint están diseñados para ahorrarle tiempo y esfuerzo y para dar coherencia y eficiencia a las tareas que realiza con regularidad.

A continuación, se muestra un ejemplo de un flujo de trabajo típico:



## Aprobación

Este flujo de trabajo dirige un documento o elemento a un grupo de usuarios para su aprobación. De forma predeterminada, el flujo de trabajo de aprobación está asociado al tipo de contenido de documento y, por lo tanto, está disponible automáticamente en las bibliotecas de documentos.

## Recopilar comentarios

Este flujo de trabajo dirige un documento o elemento a un grupo de usuarios para recibir comentarios. Los revisores pueden ofrecer comentarios, que luego se recopilan y envían a la persona que inició el flujo de trabajo. De forma predeterminada, el flujo de trabajo de recopilar comentarios está asociado al tipo de contenido de documento y, por lo tanto, está disponible automáticamente en las bibliotecas de documentos.

## Recopilar firmas

Este flujo de trabajo dirige un documento de Microsoft 365 Office a un grupo de usuarios para recopilar sus firmas digitales. Este flujo de trabajo debe iniciarse en una aplicación de Microsoft 365 Office. Los participantes deben completar sus tareas de firma agregando su firma digital al documento en el programa de Office correspondiente. De forma predeterminada, el flujo de trabajo de recopilar firmas está asociado al tipo de contenido de documento y, por lo tanto, está disponible automáticamente en las bibliotecas de documentos. Sin embargo, el flujo de trabajo de recopilar firmas solo aparece en un documento de la biblioteca de documentos si contiene una o varias líneas de firma de Microsoft Office 365.

## Publicar aprobación

Este flujo de trabajo es similar al flujo de trabajo de aprobación en el sentido de que automatiza el reenvío de contenido a expertos en la materia y partes interesadas para su revisión y aprobación. Lo que hace que el flujo de trabajo de aprobación de publicaciones sea único es que está diseñado específicamente para sitios de publicación en los que la publicación de páginas web nuevas y actualizadas está estrictamente controlada.

## Tres estados

Este flujo de trabajo se puede usar para administrar procesos de negocio que requieran que las organizaciones realicen un seguimiento de un gran volumen de problemas o elementos, como problemas de soporte al cliente, clientes potenciales o tareas de proyecto.

## Personalizar flujos de trabajo

Cada uno de los flujos de trabajo anteriores se puede personalizar para su organización de varias formas. Por ejemplo, cuando agrega un flujo de trabajo a una lista, biblioteca o tipo de contenido para que esté disponible para su uso en documentos o elementos, puede personalizar las listas de tareas y las listas del historial donde se almacena la información sobre el flujo de trabajo.

Cuando un usuario del sitio inicia un flujo de trabajo en un documento o elemento, el usuario puede tener la opción de personalizar aún más el flujo de trabajo especificando la lista de participantes, una fecha de vencimiento e instrucciones de la tarea.

## Usar Power Automate

Power Automate es un servicio de flujo de trabajo en línea que automatiza las acciones en las aplicaciones y servicios más habituales. Por ejemplo, puede crear un flujo que agregue un cliente potencial a Microsoft Dynamics 365 y un registro en MailChimp siempre que un usuario con más de 100 seguidores publique un tweet sobre su compañía. Puede usar Power Automate para automatizar flujos de trabajo entre sus aplicaciones y servicios favoritos, sincronizar archivos, recibir notificaciones, recopilar datos y mucho más.

Por ejemplo, puede automatizar estas tareas:

- Responder al instante a notificaciones o correos electrónicos de prioridad alta.
- Capturar, supervisar y realizar un seguimiento de nuevos clientes potenciales.
- Copiar todos los archivos adjuntos de correo electrónico en su cuenta de OneDrive para la Empresa
- Recopilar datos sobre su negocio y compartir esa información con su equipo.
- Automatizar flujos de trabajo de aprobación

Un uso común de Power Automate es recibir notificaciones. Por ejemplo, puede recibir instantáneamente un correo electrónico o una notificación de inserción en su smartphone cada vez que se agregue un cliente potencial a Dynamics 365 o Salesforce.

Power Automate es uno de los pilares de Power Platform. Proporciona una plataforma con poco código para el flujo de trabajo y la automatización de procesos. A continuación encontrará una lista de los diferentes tipos de flujos:

Tipo de flujo	Caso práctico	Objetivo
<a href="#"><u>Flujos automatizados</u></a>	Cree un flujo que realice una o más tareas automáticamente después de que un evento lo active.	<a href="#"><u>Conectores</u></a> para servicios en la nube o locales.
<a href="#"><u>Flujos de botones</u></a>	Ejecute tareas repetitivas desde cualquier lugar, en cualquier momento, a través de su dispositivo móvil.	
<a href="#"><u>Flujos programados</u></a>	Cree un flujo que realice una o más tareas en una programación.	
<a href="#"><u>Flujo de procesos de negocio</u></a>	Define un conjunto de pasos que se deben seguir para alcanzar el resultado deseado.	Procesos humanos

<u>Flujos de interfaz de usuario</u>	Grabe y automatice la reproducción de pasos manuales en software heredados.	Aplicaciones web y de escritorio que no tienen API disponibles para la automatización.
--------------------------------------	---	--

## Crear Power Apps

Power Apps es un conjunto de aplicaciones, servicios, conectores y plataformas de datos que proporciona un entorno de desarrollo de aplicaciones rápido para compilar aplicaciones personalizadas para las necesidades de su negocio. Al usar Power Apps, puede crear rápidamente aplicaciones empresariales personalizadas que se conectan a los datos almacenados de su empresa, ya sea en la plataforma de datos subyacente Common Data Service o en varios orígenes de datos locales y en línea, por ejemplo, SharePoint, Excel, Microsoft 365, Dynamics 365, SQL Server, etc.

Las aplicaciones creadas con Power Apps ofrecen una lógica de negocios enriquecida y capacidades de flujo de trabajo para transformar los procesos de negocio manuales y convertirlos en procesos digitales y automatizados. Además, las aplicaciones creadas con Power Apps presentan un diseño dinámico y pueden ejecutarse sin problemas en un explorador o en dispositivos móviles (smartphone o tableta). Power Apps “democratiza” la experiencia de creación de aplicaciones empresariales personalizadas, ya que permite a los usuarios compilar aplicaciones empresariales personalizadas con funciones enriquecidas sin escribir código.

Power Apps también aporta una plataforma extensible que permite a los desarrolladores profesionales interactuar mediante programación con datos y metadatos, aplicar lógica empresarial, crear conectores personalizados e integrar datos externos.

Para crear una aplicación, comience con [make.powerapps.com](https://make.powerapps.com).

- **Power Apps Studio** es el diseñador de aplicaciones que se usa para crear aplicaciones de lienzo. Esta aplicación de diseñador hace que la creación de aplicaciones se parezca más a crear una presentación de diapositivas en Microsoft PowerPoint. Más información: Generar una aplicación a partir de datos.
- **Diseñador de aplicaciones** para aplicaciones basadas en modelos le permite definir el mapa del sitio y agregar componentes para compilar una aplicación basada en modelos. Más información: Diseñe aplicaciones basadas en modelos con el diseñador de aplicaciones.

Puede ejecutar aplicaciones que haya creado usted mismo, o que haya creado otra persona y haya compartido con usted, en un explorador o en dispositivos móviles (smartphone o tableta).

## Extensibilidad

Microsoft 365 es una plataforma extensible que permite a los desarrolladores y socios crear aplicaciones personalizadas o ampliar y personalizar las aplicaciones de Office, SharePoint y Microsoft Teams.

### Microsoft Teams

Microsoft Teams es una plataforma extensible en la que se pueden crear aplicaciones personalizadas, lo que hace de la aplicación el centro de la plataforma de colaboración de su organización. Las aplicaciones para Microsoft Teams pueden ser tan simples o complejas como necesite, desde enviar notificaciones a canales o usuarios hasta aplicaciones complejas de múltiples superficies que incorporan bots conversacionales, procesamiento del lenguaje natural y experiencias web integradas. Puede crear aplicaciones para una persona, un equipo, una organización o para todos los usuarios de Microsoft Teams en cualquier lugar.

Algunas situaciones comunes con las que una aplicación personalizada de Microsoft Teams puede ayudar son las siguientes:

- Enviar información de forma proactiva a Teams desde un sistema externo y permitir a los usuarios tomar medidas sobre esa información desde dentro del cliente de Teams.
- Inserte un sitio web o aplicación web directamente en el cliente de Teams.
- Permitir que los usuarios busquen información rápidamente en otro sistema y agreguen los resultados a una conversación en Teams.
- Activar flujos de trabajo y procesos basados en una conversación en Teams, preservando el contexto de la conversación.

Con la plataforma de Microsoft Teams, puede aumentar sus servicios con información específica del contexto de las diversas API de Microsoft Teams, como información sobre el equipo o canal en el que está instalada la aplicación o los mensajes desde los que se activó la aplicación.

La plataforma de Teams proporciona un conjunto rico y flexible de puntos de extensibilidad, construcciones de IU y API que puede aprovechar mientras compila la aplicación. La aplicación puede ser tan simple como incrustar su sitio web actual en una pestaña para su equipo. También puede optar por una aplicación multifacética con todas las funciones que involucre a sus usuarios en todo el espectro del cliente de Teams.

### Ampliar Microsoft Office con complementos de Office

La plataforma de complementos de Office permite ampliar la funcionalidad de las aplicaciones de Office, incluidas Word, Outlook y Excel. Los complementos de Office ofrecen varias opciones sobre cómo su solución puede interactuar con una aplicación de Office. En esta unidad, analizamos dos de esas opciones:

- Panel de tareas
- Contenido

## Complementos del panel de tareas

Los complementos del panel de tareas permiten la interacción del usuario a través de un panel que se muestra dentro de una aplicación de Office. A través de la interfaz del panel de tareas, puede permitir que el usuario modifique documentos o correos electrónicos, vea datos de un origen de datos y más.

## Complementos de contenido

Los complementos de contenido se pueden utilizar para insertar un objeto en una hoja de cálculo de Excel o una presentación de PowerPoint. Ese objeto puede ser una visualización de datos basada en web, medios u otro contenido externo.

La plataforma de complementos de Office le permite mostrar un cuadro de diálogo para que sus usuarios puedan hacer lo siguiente:

- Iniciar sesión en un servicio integrado, por ejemplo, autenticarse con una cuenta Microsoft, de Google o de Facebook.
- Confirmar la acción del usuario.
- Ejecutar una tarea que podría estar demasiado limitada en un panel de tareas, por ejemplo, ver un vídeo.

## Usar SharePoint Framework

SharePoint es una plataforma extensible que puede personalizar y ampliar con SharePoint Framework y las múltiples API disponibles para desarrolladores. El marco de desarrollo del lado del cliente ofrecerá capacidades que ayudarán tanto a los desarrolladores propios como a los de terceros a compilar aplicaciones completas y potentes, y proporcionarán una experiencia web agradable en Microsoft 365 que sean tanto intuitivas como fáciles de consumir para los usuarios finales.

## SharePoint Framework

Los componentes de SharePoint Framework son ligeros y se ejecutan tanto en experiencias web como móviles porque son soluciones del lado del cliente. Todas las personalizaciones que cree y compile se implementan y ejecutan a través del explorador. No hay ningún componente del lado del servidor en un componente de SharePoint Framework. SharePoint Framework es compatible con versiones anteriores, lo que significa que no solo funciona con las páginas modernas, sino también con las páginas clásicas y de publicación. Las herramientas de desarrollo y la plataforma utilizadas en SharePoint Framework se implementan con herramientas de código abierto y marcos web JavaScript comunes como React.

## Microsoft Graph

Microsoft Graph proporciona un modelo de programabilidad unificado que se puede usar para compilar aplicaciones para organizaciones y consumidores que interactúen con los datos de la organización. Las API REST de Microsoft Graph implementan muchos de los parámetros de consulta del protocolo OData. Los parámetros de consulta le ayudarán a lograr múltiples tareas, como limitar la cantidad de datos devueltos por las

solicitudes a Microsoft Graph, controlar cuántos campos se devuelven para cada registro o cuántos registros se devuelven y también filtrar y buscar la información necesaria. Para admitir tantos desarrolladores y plataformas como sea posible, Microsoft Graph tiene dos opciones a elegir para los desarrolladores al integrar Microsoft Graph en sus aplicaciones.

## API REST de Microsoft Graph

En esencia, Microsoft Graph es una API REST. Eso significa que los desarrolladores pueden usar los marcos, plataformas y lenguaje de programación con los que se sientan más cómodos.

## SDK nativos de Microsoft Graph

Microsoft Graph también proporciona varios SDK nativos para los desarrolladores que deseen utilizar un modelo de programación enriquecido dentro de sus aplicaciones. Estos SDK abstraen las tareas de construir, enviar y procesar las solicitudes y respuestas REST con la API REST de Microsoft Graph. Encontrará un SDK existente para la plataforma y el idioma en el que está trabajando, ya que todas las plataformas populares están cubiertas, incluidas .NET, iOS, Android, Java, PHP, Ruby, JavaScript y muchas más.

## Administración de formularios y flujos de trabajo

Microsoft 365 ayuda a que la captura, el seguimiento y la actuación de datos y solicitudes sean más fáciles con aplicaciones y herramientas integradas diseñadas para simplificar y administrar procesos.

## Voz del cliente para Microsoft Dynamics 365

Voz del cliente para Microsoft Dynamics 365 es una capacidad de encuesta empresarial que ayuda a las empresas a obtener los comentarios que necesitan para tomar decisiones más inteligentes. Con tecnología de Microsoft 365 y Dynamics 365, Voz del cliente apoya a las empresas que buscan transformar las experiencias de los clientes, los productos y los empleados. Ofrece nuevas capacidades que hacen que capturar y analizar los comentarios de los clientes y empleados sea más sencillo que nunca. Sus clientes pueden responder a las encuestas utilizando cualquier explorador web o dispositivo móvil. A medida que se envían las respuestas, analícelas con informes de Power BI y tome decisiones efectivas en consecuencia.

Voz del cliente cuenta con sólidas herramientas para apoyar un análisis e información más profundos con integración en sus herramientas, como Common Data Service, Microsoft Power Platform y las aplicaciones basadas en modelos en Dynamics 365. Con Voz del cliente, puede enviar a sus clientes encuestas con la marca e imagen de su empresa. La distribución de encuestas es más sencilla con el redactor de correo electrónico integrado. También puede automatizar el envío de encuestas mediante Microsoft Power Automate y aprovechar las plantillas de flujo preconfiguradas para integrarse con las aplicaciones basadas en modelos en Dynamics 365.

Utilice Voz del cliente para trabajar con formularios y cuestionarios clásicos y crear otros nuevos. Los formularios y cuestionarios clásicos se abren en sus respectivas interfaces dentro del entorno de Forms Pro. Esto le proporciona la posibilidad de trabajar con encuestas y formularios clásicos juntos.

**Nota:** Microsoft Forms Pro es ahora Voz del cliente para Microsoft Dynamics 365.

## Microsoft Bookings

Microsoft Bookings es un sistema de programación de citas basado en la web que se integra con Outlook para proporcionar a sus clientes los medios para reservar una cita con miembros de su personal. Los correos electrónicos de notificación automatizados reducen las ausencias y mejoran la satisfacción del cliente. Bookings se puede diseñar para adaptarse a la situación y a las necesidades de muchas partes diferentes de una organización.

Las reservas se pueden programar y administrar de dos formas diferentes. La primera forma es que el cliente utilice una página de reserva independiente o una página de reserva integrada en su sitio web. La otra forma es que usted o uno de sus empleados escriban Bookings manualmente, como cuando un cliente llama para una cita.

Bookings tiene tres componentes principales:

- Una página de reserva donde sus clientes pueden programar citas con un miembro del personal. Esta página de programación basada en la web se puede compartir a través de un vínculo directo, su página de Facebook e incluso mediante la incorporación de un vínculo en su sitio web.
- Una página web orientada a los negocios donde los propietarios y administradores del calendario de Bookings dentro de una organización pueden definir los tipos y detalles de las citas, administrar los horarios y la disponibilidad del personal, establecer el horario comercial y personalizar cómo se programan las citas.
- Una aplicación móvil para empresas en la que los propietarios y administradores del calendario de Bookings pueden ver todas sus citas, acceder a las listas de clientes y la información de contacto y realizar reservas manuales sobre la marcha.

Microsoft Bookings puede aportar lo siguiente:

- Mayor comodidad para los clientes: la programación de citas en línea les da a los clientes la libertad de encontrar un intervalo de tiempo que les convenga y de reprogramar la cita si fuera necesario.
- Tiempo de almacenaje mejorado entre citas: al programar citas consecutivas para su personal, ahora puede incorporar cualquier actividad previa o posterior requerida.
- Administración mejorada de costes y equipos: los administradores pueden modificar las listas de personal, definir servicios y precios y establecer horas de trabajo.

# Inteligencia empresarial

Todas las organizaciones generan datos, ya sea de ventas, producción, marketing u otros orígenes. Transformar los datos para crear conclusiones valiosas y procesables puede resultar abrumador. Microsoft 365 proporciona una serie de herramientas que pueden ayudarlo a obtener significado de sus datos:

- Microsoft Excel
- Power BI

## Funciones Obtener y transformar de Excel

Excel incluye un sólido conjunto de funciones llamado Obtener y transformar, que ofrece capacidades de recopilación y configuración de datos rápidas y fáciles. Obtener y transformar le permite conectar, combinar y refinar orígenes de datos para satisfacer sus necesidades de análisis. Estas características también se usan en Power BI y en el complemento Power Query disponible para versiones anteriores de Excel.

Obtener y transformar aporta capacidades de recopilación y configuración de datos rápidas y fáciles. Le permite conectar, combinar y refinar orígenes de datos para satisfacer sus necesidades de análisis.

La conexión y la transformación de datos a menudo siguen algunos pasos comunes:



Mirando esos pasos en orden, a menudo ocurren de la siguiente manera:

- Conectar: establezca conexiones a datos que se encuentran en la nube, en servicio o localmente
- Transformar: moldee los datos para satisfacer sus necesidades. La información original permanece sin cambios
- Combinar: cree un modelo de datos a partir de múltiples orígenes de datos y obtenga una vista única de los datos
- Compartir: una vez que su consulta esté completa, puede guardarla, copiarla o usarla para informes

Siempre que se conecta a los datos, los transforma o los combina con otros orígenes de datos, una función de Obtener y transformar llamada Editor de consultas registra cada paso y le permite modificarlo como desee. El Editor de consultas también le permite

deshacer, rehacer, cambiar el orden o modificar cualquier paso, para que pueda dar forma a su vista de los datos conectados de la manera que desee.

Con Obtener y transformar, puede crear consultas que sean tan simples o complejas como necesite. A medida que agrega pasos a una consulta, el Editor de consultas trabaja a la par para crear un conjunto de instrucciones discretas que ejecutan sus comandos. Estas instrucciones se crean en el lenguaje M. Los usuarios que disfrutan del poder y la flexibilidad de las secuencias de comandos de datos pueden crear o cambiar manualmente consultas en lenguaje M utilizando el Editor avanzado.

## Conéctese a los datos

Puede utilizar una consulta para conectarse a un único origen de datos, como una base de datos de Access, o puede conectarse a varios archivos, bases de datos, fuentes OData o sitios web.

## Transforme los datos

Obtener y transformar le permite transformar los datos de sus orígenes de datos de manera que lo ayuden a analizarlos. Transformar datos significa modificarlos para satisfacer sus necesidades. Por ejemplo, puede eliminar una columna, cambiar un tipo de datos o combinar tablas; cada uno de estos procesos se considera una transformación de datos.

## Modele los datos

Después de utilizar las funciones Obtener y transformar de Excel, tendrá un modelo de datos. Un modelo de datos le permite integrar datos de varias tablas, construyendo efectivamente un origen de datos relacionales dentro de un libro de Excel.

## Publique los datos

También puede publicar su libro de trabajo en Power BI y crear informes en línea que se pueden compartir con su grupo, actualizar automáticamente y refinar. Para publicar un libro en Power BI, seleccione Archivo > Publicar> Publicar en Power BI.

## Power BI

Excel es una herramienta poderosa y flexible para cada actividad analítica. Pero si está buscando un análisis de datos profundo y capacidades de visualización mejoradas, necesitará usar Power BI. Power BI es una recopilación de servicios de software, aplicaciones y conectores que funcionan de forma conjunta para convertir los orígenes de datos independientes en información coherente, visualmente inmersiva e interactiva. Sus datos pueden ser una hoja de cálculo de Excel o un conjunto de almacenes de datos híbridos locales y basados en la nube. Power BI le permite conectarse a sus orígenes de datos, visualizar y descubrir nuevas conclusiones y compartirlas con quien desee.

Hay tres tipos distintos de Power BI:

- Una aplicación de escritorio de Windows llamada Power BI Desktop
- Un servicio SaaS (software como servicio) en línea llamado Power BI

- Aplicaciones móviles de Power BI para dispositivos Windows, iOS y Android

Estos tres elementos están diseñados para permitir que las personas creen, compartan y consuman información empresarial de la manera que les sirva a ellos, o a su rol, de la forma más efectiva. La parte final es Power BI Report Server, que le permite publicar informes de Power BI en un servidor de informes local, después de crearlos en Power BI Desktop.

## Licencias de Power BI

Hay varios tipos de licencias por usuario de Power BI: gratuitas, Pro y Premium por usuario. El tipo de licencia que necesita un usuario determina dónde se almacena el contenido y cómo interactuará con ese contenido. Power BI Premium otorga a los usuarios una licencia gratuita para actuar sobre el contenido de las áreas de trabajo asignadas a la capacidad Premium. Fuera de la capacidad Premium, un usuario con una licencia gratuita solo puede usar el servicio Power BI para conectarse a los datos y crear informes y paneles en su área de trabajo. No puede compartir contenido con otros usuarios ni publicarlo en otras áreas de trabajo, salvo que tenga la licencia Power BI Premium por usuario.

Una suscripción estándar de Power BI usa capacidad compartida. Si el contenido se almacena en capacidad compartida, los usuarios a los que se les asigna una licencia de Power BI Pro solo pueden colaborar con otros usuarios de Power BI Pro. Pueden consumir contenido compartido por otros usuarios, publicar contenido en áreas de trabajo de aplicaciones, compartir paneles y suscribirse a paneles e informes. Cuando los espacios de trabajo están en capacidad Premium, los usuarios Pro pueden distribuir contenido a los usuarios que no tienen una licencia de Power BI Pro.

La siguiente tabla resume las capacidades básicas de cada tipo de licencia:

Tipo de licencia	No en la capacidad Premium	Capacidad Premium
Power BI (gratis)	Utilícelo como un espacio aislado personal donde crea contenido para usted mismo e interactúa con ese contenido. Una licencia gratuita es la forma idónea de probar el servicio Power BI. No puede consumir contenidos de otras personas ni compartir su contenido con otros.	Interactúe con los contenidos asignados a la capacidad Premium y compartidos con usted. Los usuarios gratuitos, Premium por usuario y Pro pueden colaborar sin necesidad de que los usuarios gratuitos tengan cuentas Pro.
Power BI Pro	Colabore con usuarios Premium por usuario y Pro creando y compartiendo contenidos.	Colabore con usuarios gratuitos, Premium por usuario y Pro creando y compartiendo contenidos.

## **Analizar en Excel**

Con Analizar en Excel, puede llevar conjuntos de datos de Power BI a Excel y luego verlos e interactuar con ellos utilizando tablas dinámicas, gráficos, segmentaciones y otras características de Excel. Para usar Analizar en Excel, primero debe descargar la característica de Power BI, instalarla y luego seleccionar uno o más conjuntos de datos para usar en Excel.

## **Administración del trabajo**

Todas las organizaciones, independientemente de su tamaño, deben tener un plan sobre cómo evolucionarán y crecerán su negocio, oferta de servicios o productos. Independientemente de la metodología de administración de proyectos que adopte, en última instancia, para que esos proyectos tengan éxito, necesitará un medio para compartir esa información con su equipo y las partes interesadas del proyecto.

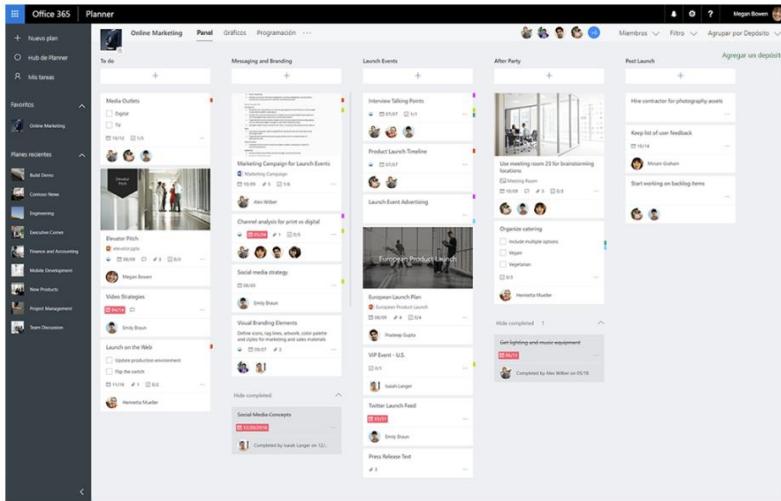
## **Microsoft Planner**

Microsoft proporciona una herramienta de administración de proyectos, llamada Microsoft Planner, para ayudarle a administrar sus proyectos y los equipos que trabajan en ellos.

Planner le permite organizar las actividades en su proyecto, comenzando con el plan general y luego asignando tareas a grupos, conocidos como cubos. A cada tarea se le puede asignar un nombre o etiqueta, asignar a un miembro del equipo y establecer una fecha límite. Microsoft Planner usa grupos de Microsoft 365 para otorgar acceso a los miembros del equipo al plan, de forma que se les puedan asignar tareas. Con los grupos de Microsoft 365, los miembros del equipo pueden colaborar en el plan y recibir notificaciones cuando cambia.

Planner se integra completamente en Teams y Outlook para garantizar que todos los miembros de su equipo estén completamente actualizados sobre las tareas y actividades en las que están trabajando y las actualizaciones de estado del proyecto.

Planner proporciona una forma simple y visual para que los equipos organicen su trabajo. Los clientes pueden usar Planner para crear planes, organizar y asignar tareas, compartir el progreso y colaborar en el contenido. Planner proporciona varias experiencias interactivas, que incluyen un tablero de tareas, una página de gráficos y una vista de programación, así como integraciones en todo el conjunto de herramientas, aplicaciones y servicios de Microsoft 365.



## Tablero

La vista predeterminada es el tablero, que muestra cada cubo y las tareas asociadas. Aquí es donde el miembro del equipo administrará las tareas en las que está trabajando. Pueden mover tareas entre cubos, actualizar el progreso, agregar información adicional a la tarea, incluidos los archivos adjuntos, y marcar una tarea como completada cuando esté lista. El tablero tiene varias herramientas disponibles para filtrar y limpiar la vista:

- Filtro: permite reducir lo que ve. Algunas de las opciones incluyen, tarde, hoy, mañana, esta semana, la próxima semana, futuro y tareas asignadas a miembros específicos del equipo.
- Agrupar por: permite volver a ordenar sus tareas por cubo, asignado a, progreso, fecha de vencimiento y cualquiera de las etiquetas asignadas.

## Gráficos

Permite obtener una representación visual del estado del proyecto y las tareas. Este panel tiene tres componentes, un estado general de todas las tareas, el progreso de los trabajos en cada cubo y la disponibilidad de los miembros del equipo.

## Programación

Use la vista de programación para ver dónde se ubica cada tarea en el calendario. Desde esta vista, tiene la opción de añadir la programación a Outlook. Las tareas también se pueden integrar en Microsoft To-Do, por lo que cada miembro del equipo puede ver las tareas que se le han asignado.

## Grupos de Microsoft 365

Grupos de Microsoft 365 es un servicio que funciona con las herramientas de Microsoft 365 que ya usa para que pueda colaborar con sus compañeros de equipo al escribir documentos, crear hojas de cálculo, trabajar en planes de proyectos, programar reuniones o enviar correos electrónicos.

## Colaboración en equipo

Los grupos en Microsoft 365 permiten elegir un conjunto de personas con las que desee colaborar y configurar fácilmente un conjunto de recursos para que esas personas comparten. Los recursos incluyen una bandeja de entrada de Outlook compartida, un calendario compartido o una biblioteca de documentos para colaborar en archivos.

## Permisos de grupo

No tiene que asignar permisos manualmente a todos esos recursos porque al agregar miembros al grupo se les otorgan automáticamente los permisos que necesitan para las herramientas que proporciona su grupo.

## Creación de grupos

Puede crear Grupos de Microsoft 365 a partir de una variedad de herramientas que incluyen Outlook, Outlook en la Web, Outlook Mobile, SharePoint, Planner, Teams y más. La herramienta desde la que elija comenzar depende del tipo de grupo con el que esté trabajando.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Luego seleccione **Comprobar sus respuestas**.

¿Qué es la puntuación de seguridad de Microsoft?

- A. La puntuación de seguridad es una medida de la posición de seguridad de una organización
- B. La puntuación de seguridad es una medida de la posición del antivirus de una organización
- C. La puntuación de seguridad es una medida de fuerza del firewall de una organización

¿Qué servicios incluye Endpoint Manager?

- A. Microsoft Intune, Configuration Manager, Análisis de escritorio, Security Center, Windows Autopilot, Azure Active Directory, Centro de administración de Endpoint Manager
- B. Microsoft Intune, Configuration Manager, Administración conjunta, Análisis de escritorio, Endpoint Protection, Windows Autopilot, Centro de administración de Endpoint Manager
- C. Microsoft Intune, Configuration Manager, Administración conjunta, Análisis de escritorio, Windows Autopilot, Azure Active Directory, Centro de administración de Endpoint Manager

¿Cuál de estas es la lista correcta de flujos de trabajo integrados de SharePoint?

- A. Aprobación, recopilación de comentarios, recopilación de firmas, aprobación de publicación, tres estados

- B. Aprobación, Recopilar comentarios, Recopilar firmas, Aprobación de publicación, triple estado
- C. Aprobación, Recopilar comentarios, Recopilar firmas, Aprobación de publicación, Triestatal

¿Qué dos opciones están disponibles para los desarrolladores que deseen incorporar o usar Microsoft Graph en sus aplicaciones?

- A. API de SOAP de Microsoft Graph, SDK nativos de Microsoft Graph
- B. API REST de Microsoft Graph, SDK nativos de Microsoft Graph
- C. API REST de Microsoft Graph, SDK de Microsoft Graph para Windows 10

¿Cuál es el tipo mínimo de licencia de Power BI requerido para los usuarios si quieren consumir contenido compartido con ellos?

- A. Power BI Pro
- B. Power BI
- C. Power BI Premium

## Simplifique la administración de dispositivos con Microsoft Endpoint Manager

### Introducción

A medida que su empresa va trasladando una mayor parte de sus cargas de trabajo a la nube, puede hacer que sus empleados trabajen desde cualquier ubicación. Microsoft, en su posición única como proveedor de nube y proveedor de sistema operativo, ha creado aplicaciones de administración integral de equipos en la nube. Esto proporciona una solución a su departamento de TI que permite configuraciones de PC remotas.

Al final de este módulo, debería ser capaz de hacer lo siguiente:

- Explicar los conceptos de administración de aplicaciones y dispositivos modernos.
- Explicar el valor de Microsoft Endpoint Manager (MEM), incluido Microsoft Intune y Configuration Manager.
- Describir cómo Autopilot puede ayudar a agilizar la adquisición y configuración de nuevos dispositivos.

### Administración moderna

#### Ventajas de la administración moderna

Hasta hace poco tiempo, la administración de la infraestructura tecnológica y los equipos de la organización se realizaba con herramientas y métodos diferentes, lo que

implicaba una gran cantidad de tareas prácticas, manuales y largas para los profesionales de TI. Gracias a los nuevos tipos de factores de forma de los dispositivos, los nuevos enfoques en la administración de Windows 10, los avances en la tecnología en la nube y las tendencias Bring Your Own Device (BYOD), el cambio a una administración moderna se ha vuelto más atractivo para muchas organizaciones, y no solo para dispositivos móviles, sino también para equipos.

La administración moderna es un nuevo enfoque para administrar Windows 10 de forma similar a cómo se administran los dispositivos móviles con las soluciones de Enterprise Mobility Management (EMM). Este enfoque le permite simplificar la implementación y administración, mejorar la seguridad, proporcionar mejores experiencias para los usuarios finales y disminuir costes para sus dispositivos Windows. Ahora, con la administración moderna, puede administrar dispositivos con Windows 10 de cualquier tipo, desde equipos de escritorio hasta HoloLens y Surface Hub, ya sean propiedad de la empresa o del empleado, así como dispositivos móviles que usan una plataforma de administración.

La siguiente tabla enumera solo algunos de los muchos beneficios que las organizaciones pueden ver al adoptar metodologías de administración modernas:

Fácil de implementar y administrar	La implementación de sistemas operativos tradicional (OSD), además de ser muy eficaz, suele ser compleja y requiere mucho tiempo. Ahora, hay una forma más sencilla de aprovisionar nuevos dispositivos con Windows 10. Windows Autopilot, que está profundamente integrado en Azure Active Directory (Azure AD) e Intune, simplifica y personaliza la experiencia de configuración rápida (OOBE) para los usuarios, une el dispositivo a Azure AD y lo inscribe en Intune. Intune también aplica automáticamente el correo electrónico de los usuarios, las aplicaciones, los archivos, las preferencias y la configuración de seguridad de la organización sin necesidad de crear imágenes de sistema operativo personalizadas.
Siempre actualizado	Mantenerse al día con las amenazas de seguridad emergentes y mejorar la productividad de los usuarios requiere un cambio en la frecuencia con la que es necesario actualizar Windows 10 y las aplicaciones de Microsoft 365. Con las actualizaciones alineadas, la gran cantidad de información impulsada por la inteligencia de la nube y un enfoque de administración moderno con EMS, ahora hay una forma mejor de mantener actualizados los dispositivos sin la complejidad de mantener una infraestructura local.
Seguridad inteligente integrada	Los atacantes son cada vez más sofisticados y Microsoft 365 se diseñó pensando en la seguridad. Hay muchas características de seguridad nuevas y en evolución integradas en la plataforma de Microsoft 365, entre las que se incluyen Windows Hello, la Protección contra amenazas avanzada (ATP) de Windows Defender, Windows Information Protection, Azure AD Identity Protection, el acceso condicional y mucho más. Las

	características de seguridad cuentan con tecnología de Microsoft Intelligent Security Graph, que usa miles de millones de señales, de forma que mejora constantemente los algoritmos de aprendizaje automático y los conocimientos humanos para ayudarle a proteger los datos de la empresa y responder a ataques sofisticados.
Información proactiva	Con telemetría e inteligencia en la nube enriquecidas, ahora puede detectar proactivamente problemas con los dispositivos y las aplicaciones antes de que afecten a los usuarios finales, tener más confianza al aplicar las actualizaciones del sistema operativo, detectar problemas de seguridad y mucho más. La fusión de la inteligencia basada en el aprendizaje automático con los conocimientos humanos puede dar lugar a una unión única y eficaz.

## Opciones de implementación e inscripción

Con Windows 10, puede seguir usando la implementación tradicional de sistema operativo para implementaciones de escala reducida, pero también puede “administrar de forma rápida” para obtener una experiencia más sencilla tanto para los usuarios como para TI. Para transformar nuevos dispositivos en dispositivos completamente configurados y totalmente administrados, puede:

- Evitar el restablecimiento de la imagen inicial en los servicios de administración de dispositivos basados en la nube, como Microsoft Autopilot para Windows 10 y Microsoft Intune para aprovisionamiento dinámico de suscripciones, aplicaciones, dispositivos y perfiles de usuario.
- Crear paquetes de aprovisionamiento autónomos con el Diseñador de configuración de Windows.
- Usar las técnicas de creación de imágenes tradicionales, como la implementación de imágenes personalizadas con System Center Configuration Manager.

Tiene varias opciones para actualizar a Windows 10. En el caso de los dispositivos existentes que ejecutan Windows 7 o Windows 8.1, se recomienda usar el sólido proceso de actualización local para una transición rápida y confiable a Windows 10, al tiempo que se preservan automáticamente todos los datos, las aplicaciones y las configuraciones existentes. Esto puede reducir de forma significativa los costes de implementación y aumentar la productividad, ya que los usuarios finales pueden ser productivos de forma inmediata porque todo se encuentra justo donde lo dejaron. Por supuesto, puede usar también un enfoque tradicional de borrado y carga si lo prefiere, con las mismas herramientas que usa actualmente con Windows 7.

## Actualizaciones y mantenimiento

Con **Windows como servicio**, el departamento de TI ya no necesita llevar a cabo procesos complejos de creación de imágenes (borrado y carga) con cada nueva versión de Windows. Los dispositivos de las versiones de canal semianual (SAC) de Windows

10 reciben las actualizaciones más recientes de características y calidad a través de procesos de revisión sencillos y a menudo automáticos.

**La administración de dispositivos móviles (MDM)** con Intune ofrece herramientas para aplicar las actualizaciones de Windows a los equipos cliente de su organización. Configuration Manager ofrece excelentes capacidades de administración y seguimiento de las actualizaciones, incluidos los períodos de mantenimiento y las reglas de implementación automáticas.

## Identidad y autenticación

Puede usar Windows 10 y servicios como Azure Active Directory de formas nuevas para identificación, autenticación y administración basadas en la nube. Puede ofrecer a los usuarios la capacidad de “llevar su propio dispositivo” (BYOD) o “elegir su propio dispositivo” (CYOD) de una lista que ponga a su disposición. Al mismo tiempo, es posible que administre equipos y tabletas que deban estar unidos a un dominio, debido a los recursos o las aplicaciones específicos que se usan en ellos.

Puede visualizar la administración de usuarios y dispositivos en estas dos categorías:

- Dispositivos corporativos (CYOD) o personales (BYOD) usados por usuarios móviles para aplicaciones SaaS. Con Windows 10, los empleados podrán aprovisionar sus dispositivos automáticamente.
- Equipos y tabletas unidos a un dominio que se usan para aplicaciones tradicionales y acceso a recursos seguros. Pueden ser aplicaciones y recursos tradicionales que requieran autenticación o acceso a recursos altamente confidenciales o clasificados almacenados de forma local. Con Windows 10, si tiene un dominio de Active Directory local que esté integrado con Azure AD, cuando se unen los dispositivos de los empleados, se registran automáticamente con Azure AD.

Las tabletas y los equipos unidos a un dominio se pueden seguir administrando con la directiva de grupo o el cliente de System Center Configuration Manager.

## Soluciones integradas en Microsoft Endpoint Manager

### Endpoint Manager

Microsoft Endpoint Manager le ayuda a tener un área de trabajo y una administración moderna para mantener sus datos seguros, ya estén almacenados en la nube o de forma local. Endpoint Manager incluye los servicios y las herramientas que utiliza para administrar y supervisar dispositivos móviles, equipos de escritorio, máquinas virtuales, dispositivos integrados y servidores.

Endpoint Manager incluye los siguientes servicios:

- **Microsoft Intune:** Intune es un proveedor totalmente basado en la nube de administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM) para sus aplicaciones y dispositivos. Le permite controlar características y parámetros de configuración en dispositivos Android, Android Enterprise, iOS/iPadOS, macOS y Windows.

10. Se integra con otros servicios, incluidos Azure Active Directory (AD), los defensores de amenazas móviles, las plantillas ADMX, Win32 y las aplicaciones LOB personalizadas, y más. Si tiene una infraestructura local, como Exchange o una instancia de Active Directory, también están disponibles los conectores de Intune:

- El **Conector de Intune para Active Directory** agrega entradas a su dominio de Active Directory local para los equipos que se inscriben mediante Windows Autopilot.
- El **conector de Intune Exchange** permite (o bloquea) el acceso de dispositivos a sus servidores Exchange si los dispositivos están inscritos en Intune y cumplen con sus directivas.
- El **conector de certificado de Intune** procesa solicitudes de certificado provenientes de dispositivos que usan certificados para la autenticación y el cifrado de correo electrónico S/MIME.

Como parte de Endpoint Manager, use Intune para crear y comprobar la compatibilidad e implementar aplicaciones, características y configuraciones en los dispositivos mediante la nube.

- **Configuration Manager:** Configuration Manager es una solución de administración local para administrar escritorios, servidores y equipos portátiles que se encuentren en su red o en Internet. Puede habilitarla en la nube para que se integre con Intune, Azure Active Directory (AD), ATP de Microsoft Defender y otros servicios en la nube. Use Configuration Manager para implementar aplicaciones, actualizaciones de software y sistemas operativos. También puede supervisar el cumplimiento, consultar y actuar sobre clientes en tiempo real y mucho más. Como parte de Endpoint Manager, continúe usando Configuration Manager como siempre lo ha hecho. Si está listo para trasladar algunas tareas a la nube, considere la administración conjunta.
- **Administración conjunta:** La administración conjunta combina su inversión de Configuration Manager local existente con la nube mediante Intune y otros servicios en la nube de Microsoft 365. Elija si Configuration Manager o Intune es la entidad de administración de los siete grupos de cargas de trabajo diferentes.
- **Análisis de escritorio:** Análisis de escritorio es un servicio basado en la nube que se integra con Configuration Manager. Proporciona información detallada e inteligente para que pueda tomar decisiones más fundamentadas sobre la preparación de actualizaciones de sus clientes Windows. El servicio combina datos de su organización con datos agregados de millones de dispositivos conectados a la nube de Microsoft. Proporciona información sobre actualizaciones de seguridad, aplicaciones y dispositivos en su organización e identifica problemas de compatibilidad con aplicaciones y controladores. Cree una prueba piloto para los dispositivos con más probabilidades de proporcionar la mejor información sobre los activos de su organización.
- **Windows Autopilot:** Windows Autopilot prepara y preconfigura nuevos dispositivos y los prepara para su uso. Está diseñado para simplificar las fases del ciclo de vida de los dispositivos Windows, tanto para TI como para los usuarios finales, desde la implementación inicial al final de la vida útil. Como parte de Endpoint Manager, use Autopilot para preconfigurar

dispositivos e inscriba dispositivos automáticamente en Intune. También puede integrar Autopilot con Configuration Manager y la administración conjunta para configuraciones de dispositivo más complejas (en versión preliminar).

- **Azure Active Directory (AD):** Endpoint Manager usa Azure AD para la identidad de dispositivos, usuarios, grupos y la autenticación multifactor (MFA). **Azure AD Premium** puede tener un coste adicional y tiene funciones adicionales para proteger dispositivos, aplicaciones y datos, incluidos grupos dinámicos, inscripción automática y acceso condicional.
- **Centro de administración de Endpoint Manager:** El centro de administración es un sitio web integral para crear políticas y administrar sus dispositivos. Se conecta a otros servicios clave de administración de dispositivos, incluidos los grupos, la seguridad, el acceso condicional y los informes. Este centro de administración también muestra los dispositivos administrados por Configuration Manager e Intune (en versión preliminar).

The screenshot shows the Microsoft Endpoint Manager Admin Center interface. At the top, it displays the title 'Centro de administración de Microsoft Endpoint Manager' and the user 'admin@M365x143776... CONTOSO'. The main content area is titled 'Home page' and shows a summary for the organization 'Contoso'. It includes sections for 'Estado y alertas' (with tabs for 'Estado de inquilino' showing 'Estado de la cuenta: Activo', 'Estado del servicio: Correcto', and 'Estado del conector: Correcto'), 'Alertas de recursos' (listing device compliance, Intune enrollment, device configuration, and client application status), and 'Escenarios guiados' (a section on implementing Microsoft Edge for mobile devices). The left sidebar contains navigation links for various management categories like Device, Application, and User management.

## Elija lo que más le conviene

Hay varias maneras de determinar qué es lo más adecuado para la organización. Los pasos siguientes dependen de lo que hace la organización. Considere lo que está tratando de lograr.

Por ejemplo:

- Si aprovisiona constantemente nuevos dispositivos, comience con Windows Autopilot.
- Si agrega reglas y configuraciones de control para sus usuarios, aplicaciones y dispositivos, comience con Intune.

- Si actualmente usa Configuration Manager para implementar aplicaciones y desea usar el acceso condicional según los requisitos de seguridad, comience con la administración conjunta.
- Si actualmente usa Configuration Manager y es responsable de mantener los dispositivos Windows 10 actualizados, comience con Desktop Analytics.
- Si está comenzando con MDM y MAM, o usa plantillas ADMX para controlar la configuración de Office, Microsoft Edge y Windows, comience con Intune.

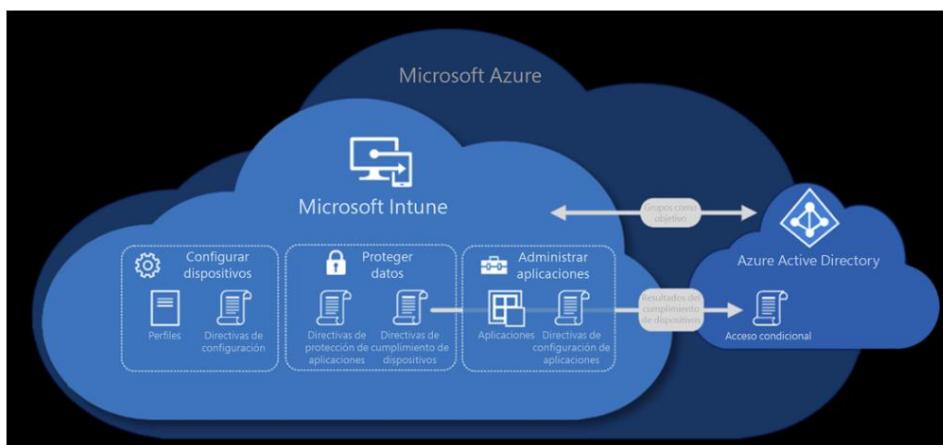
También puede pensar en Endpoint Manager en tres partes: nube, local y nube + local:

- **Nube:** Todos los datos están almacenados en Azure. Y no hay más centros de datos. Este enfoque le ofrece los beneficios de movilidad de la nube y los de seguridad de Azure.
- **Local:** Si tiene una infraestructura local que incluye Configuration Manager o no está listo para usar la nube, puede conservar sus sistemas existentes.
- **Nube + local:** Muchos entornos son mixtos y utilizan un enfoque de conexión a la nube. Lo que significa que usan una combinación de nube y local. Para dispositivos nuevos, utilice los beneficios de Intune para acceder y proteger los datos. Si usa Configuration Manager, conéctese a la nube para obtener funciones y análisis adicionales. Si desea trasladar algunas cargas de trabajo a la nube, la coadministración es una buena opción.

## Intune

Microsoft Intune es un proveedor de MDM y MAM para sus dispositivos

Microsoft Intune es un servicio basado en la nube que se centra en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Intune está integrado como parte de Microsoft Endpoint Manager en Microsoft 365 y permite a los usuarios ser productivos mientras mantienen protegidos los datos de su organización. Se integra con otros servicios, incluidos Microsoft 365 y Azure Active Directory (Azure AD) para controlar quién tiene acceso y a qué tienen acceso, y Azure Information Protection para la protección de datos. Cuando lo usa con Microsoft 365, puede facilitar que sus recursos sean productivos en todos sus dispositivos mientras la información de su organización se mantiene protegida.



Con Intune, puede:

- Elija estar 100 % en la nube con Intune o ser coadministrado con Configuration Manager e Intune.
- Establezca reglas y configure los ajustes en dispositivos personales y propiedad de la organización para acceder a datos y redes.
- Implemente y autentique aplicaciones en dispositivos, locales y móviles.
- Proteja la información de su empresa al controlar la manera en que los usuarios obtienen acceso a ella y la comparten.
- Asegúrese de que los dispositivos y las aplicaciones sean compatibles con los requisitos de seguridad de la empresa.

## Administración de dispositivos

Con Intune, administre los dispositivos con un enfoque adecuado para usted. Para los dispositivos propiedad de la organización, es posible que desee tener un control total sobre los dispositivos, incluida la configuración, las funciones y la seguridad. En este enfoque, los dispositivos y los usuarios de estos dispositivos se “inscriben” en Intune. Una vez inscritos, reciben sus reglas y configuraciones a través de las directivas configuradas en Intune. Por ejemplo, puede establecer requisitos de contraseña y PIN, crear una conexión VPN, configurar la protección contra amenazas y más.

En el caso de los dispositivos personales, o si trae los suyos (BYOD), es posible que los usuarios no deseen que los administradores de su organización tengan el control total. En este enfoque, ofrezca opciones a los usuarios. Por ejemplo, los usuarios inscriben sus dispositivos si desean tener acceso completo a los recursos de su organización. O bien, si estos usuarios solo desean acceder al correo electrónico o Microsoft Teams, utilice las directivas de protección de aplicaciones que requieren autenticación multifactor (MFA) para usar estas aplicaciones.

Con los perfiles de Device Firmware Configuration Interface (DFCI) integrados en Microsoft Intune (ahora disponible en versión preliminar pública), la administración de Surface UEFI extiende la pila de administración moderna hasta el nivel de hardware UEFI. DFCI admite el aprovisionamiento sin intervención, elimina las contraseñas de BIOS, proporciona control de la configuración de seguridad, incluidas las opciones de arranque y los periféricos integrados, y sienta las bases para escenarios de seguridad avanzados en el futuro.

Cuando los dispositivos se inscriben y administran en Intune, los administradores pueden:

- Vea los dispositivos registrados y obtenga un inventario de los dispositivos que acceden a los recursos de la organización.
- Configurar los dispositivos para que cumplan con sus estándares de seguridad y salud. Por ejemplo, probablemente desee bloquear dispositivos con jailbreak.
- Envíe certificados a los dispositivos para que los usuarios puedan acceder fácilmente a su red Wi-Fi o utilizar una VPN para conectarse a su red.
- Vea informes sobre usuarios y dispositivos conformes y no conformes.
- Elimine los datos de la organización si un dispositivo se pierde, es robado o ya no se usa.

## Probar la guía interactiva

La guía interactiva Administre los dispositivos con Microsoft Endpoint Manager le orienta por el centro de administración de Microsoft Endpoint Manager para mostrarle cómo administrar y proteger las aplicaciones móviles y de escritorio.

## Configuration Manager

### Microsoft Endpoint Configuration Manager

Microsoft Endpoint Configuration Manager es un producto local que se utiliza para administrar equipos Windows, macOS y servidores. Configuration Manager ofrece un amplio conjunto de funcionalidades que le permiten personalizar las siguientes áreas:

- Administración de aplicaciones
- Implementación de sistema operativo
- Administración de actualización de software
- Cumplimiento de dispositivos

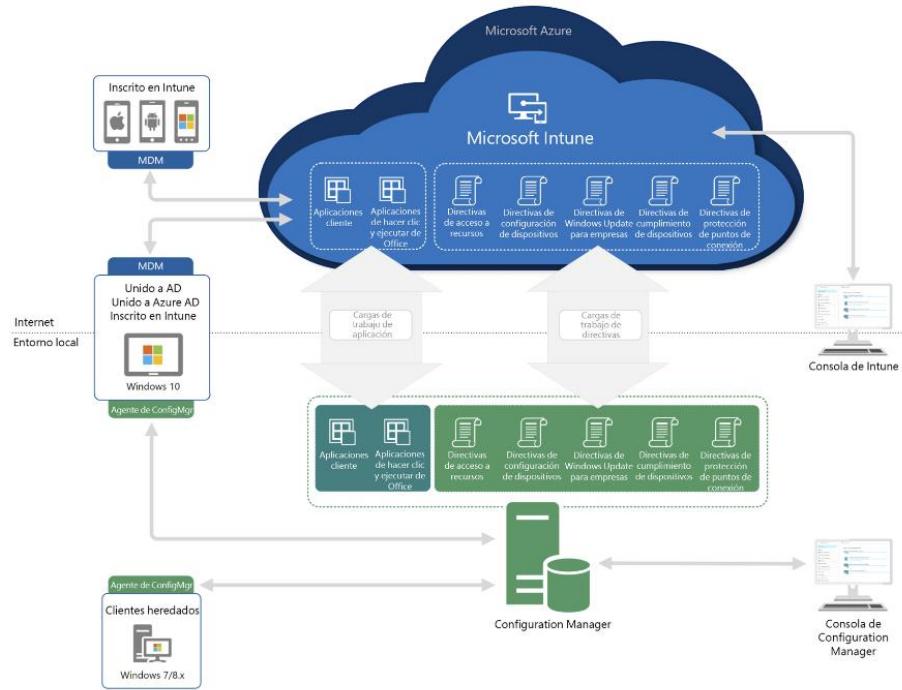
### Administración conjunta: administración de dispositivos conectados a la nube con Microsoft 365

Si tiene una infraestructura de Configuration Manager local existente, puede conectarla a su sistema de administración de Intune basado en la nube con la función de “administración conjunta” de Configuration Manager. Este escenario conectado a la nube le permite administrar dispositivos que ejecutan Windows 10 con Configuration Manager y Microsoft Intune de forma concurrente. Aporta la funcionalidad de Intune a su ecosistema de administración de dispositivos

La administración conjunta es una de las principales formas de conectar la implementación existente de Configuration Manager a la nube de Microsoft 365. Le permite administrar dispositivos con Windows 10 simultáneamente con Configuration Manager y Microsoft Intune. La administración en conjunto permite conectar a la nube su inversión actual en Configuration Manager al agregar nuevas funciones, como el acceso condicional.

Cuando un dispositivo con Windows 10 tiene el cliente de Configuration Manager y se inscribe en Intune, obtiene las ventajas de ambos servicios. Controla qué cargas de trabajo, si procede, cambian la autoridad de Configuration Manager a Intune. Configuration Manager sigue administrando las demás cargas de trabajo, incluidas aquellas que no cambian a Intune, así como las demás características de Configuration Manager que no sean compatibles con la administración conjunta.

También puede probar una carga de trabajo con una colección separada de dispositivos. La prueba piloto le permite probar la funcionalidad de Intune con un subconjunto de dispositivos antes de cambiar a un grupo más grande.



## Caminos para la administración conjunta

El acceso a la administración conjunta tiene dos caminos principales:

- Clientes de Configuration Manager existentes: Tiene dispositivos con Windows 10 que ya son clientes de Configuration Manager. Configure Azure AD híbrido e inscríbalos en Intune.
- Nuevos dispositivos basados en Internet: Tiene nuevos dispositivos Windows 10 que se unen a Azure AD y se inscriben automáticamente en Intune. Instale el cliente de Configuration Manager para llegar a un estado de administración conjunta.

## Beneficios

Cuando inscriba clientes de Configuration Manager existentes en la administración conjunta, obtendrá lo siguiente:

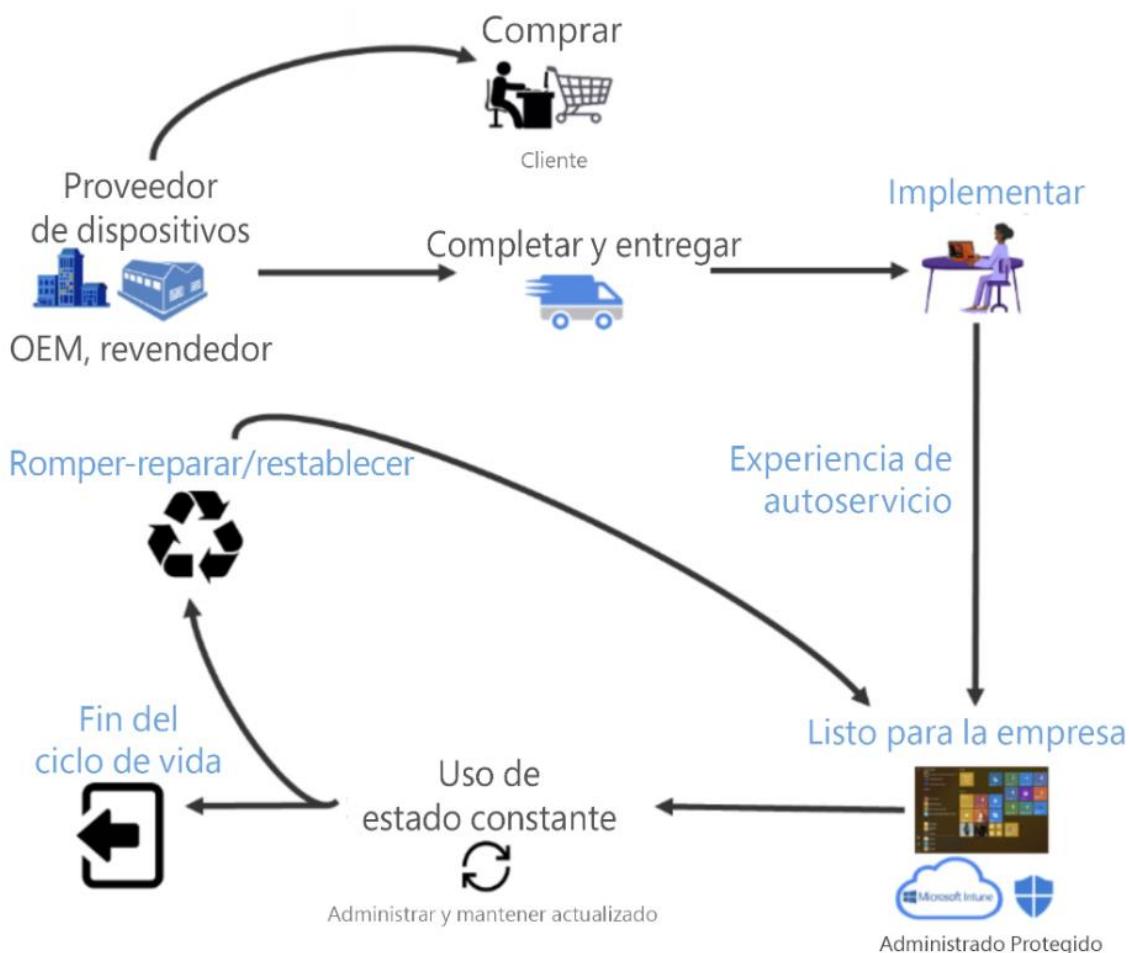
- Acceso condicional con cumplimiento de dispositivos
- Acciones remotas basadas en Intune, por ejemplo: reiniciar, control remoto o restablecimiento de factoría
- Visibilidad centralizada del estado del dispositivo
- Vincular usuarios, dispositivos y aplicaciones con Azure Active Directory (Azure AD)
- Aprovisionamiento moderno con Windows Autopilot
- Acciones remotas

# AutoPilot e implementación sin interacción

## Windows Autopilot

Windows Autopilot es un conjunto de tecnologías que se utilizan para configurar y preconfigurar nuevos dispositivos, preparándolos para un uso productivo. También puede usar Windows Autopilot para restablecer, reasignar y recuperar dispositivos. Esta solución permite a un departamento de TI lograr lo anterior con poca o ninguna infraestructura que administrar, con un proceso fácil y sencillo.

Windows Autopilot está diseñado para simplificar todas las fases del ciclo de vida de los dispositivos Windows, tanto para TI como para los usuarios finales, desde la implementación inicial al final de la vida útil. Al utilizar los servicios basados en la nube, puede reducir los costes totales de implementación, administración y retirada de dispositivos al minimizar la cantidad de tiempo que TI necesita dedicar a estos procesos y la cantidad de infraestructura que se necesita mantener, al tiempo que se garantiza la facilidad de uso para todos los tipos de usuarios finales. Observe el siguiente diagrama:



Al implementar inicialmente nuevos dispositivos Windows, Windows Autopilot aprovecha la versión optimizada del fabricante original de Windows 10 que está preinstalada en el dispositivo, lo que ahorra a las organizaciones el esfuerzo de tener que mantener imágenes y controladores personalizados para cada modelo de dispositivo que se utiliza. En lugar de volver a crear imágenes del dispositivo, su instalación

existente de Windows 10 se puede transformar en un estado “listo para el negocio”, aplicando configuraciones y directivas, instalando aplicaciones e incluso cambiando la edición de Windows 10 que se está utilizando (por ejemplo, desde Windows 10 Pro a Windows 10 Enterprise) para admitir funciones avanzadas.

Una vez implementados, los dispositivos con Windows 10 se pueden administrar mediante herramientas como Microsoft Intune, Windows Update para empresas, Microsoft Endpoint Configuration Manager y otras herramientas similares. Windows Autopilot también se puede usar para reutilizar un dispositivo aprovechando el restablecimiento de Windows Autopilot Reset para preparar rápidamente un dispositivo para un nuevo usuario o, en escenarios de ruptura/reparación, para permitir que un dispositivo vuelva rápidamente a un estado listo para el negocio.

Windows Autopilot permite:

- Unir dispositivos automáticamente a Azure Active Directory (Azure AD) o Active Directory (a través de una unión a Azure AD híbrido).
- Inscribir automáticamente dispositivos en servicios MDM, como Microsoft Intune (requiere una suscripción a Azure AD Premium para la configuración).
- Restringir la creación de cuentas de administrador.
- Crear y asignar automáticamente dispositivos a grupos de configuración en función del perfil de un dispositivo.
- Personalizar el contenido específico de la configuración rápida (OOBE) para la organización.

## Ventajas de Windows Autopilot

Tradicionalmente, los profesionales de TI dedican mucho tiempo a crear y personalizar imágenes que posteriormente se van a implementar en dispositivos. Windows Autopilot presenta un nuevo enfoque.

Desde el punto de vista del usuario, solo se requieren algunas operaciones sencillas para que el dispositivo esté listo para su uso.

Desde la perspectiva del profesional de TI, la única interacción que se requiere por parte del usuario final es conectarse a una red y comprobar sus credenciales. Todo lo demás está automatizado.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Cuáles de las siguientes opciones le permite a las organizaciones crear paquetes de aprovisionamiento autónomos?

- A. Diseñador de configuración de Windows
- B. Microsoft Intune
- C. Microsoft Autopilot

¿Qué medida de seguridad adicional se sugiere para los usuarios que deseen acceder a las aplicaciones corporativas en sus propios dispositivos?

- A. Limitar a los usuarios a aplicaciones basadas en web que requieran HTTPS.
- B. Requerir la implementación de una red privada virtual (VPN)
- C. Implementar la autenticación multifactor (MFA)

¿Cuál de las siguientes afirmaciones es cierta?

- A. Configuration Manager administra tanto la infraestructura local como las funciones basadas en la nube
- B. Configuration Manager administra la infraestructura local e Intune administra las funciones basadas en la nube
- C. Windows Autopilot es el nuevo método para la administración de infraestructura tanto para escenarios locales, como basados en la nube.

Cuando se usa Windows Autopilot para configurar el dispositivo de un usuario, ¿cuál de las siguientes afirmaciones describe la única interacción que se le exige al usuario final?

- A. Conéctese a una red y luego inicie el cliente de Intune.
- B. Conéctese a una red y verifique sus credenciales.
- C. Conéctese a una red y luego ejecute un script de PowerShell (proporcionado por TI) para conectarse al servidor de Autopilot.

# Más tareas y garantía de la seguridad con Windows 10

## Introducción

Windows 10 Enterprise es uno de los componentes principales de la suscripción a Microsoft 365. Windows 10 satisface las necesidades de las organizaciones, ya que proporciona a los usuarios y a las organizaciones las herramientas, los servicios y el soporte necesarios para mejorar su productividad.

En este módulo, aprenderá los fundamentos de Windows 10 y Microsoft 365 como parte de una estrategia de administración empresarial simplificada.

Al finalizar este módulo, podrá:

- Describir las opciones para la implementación y compatibilidad con Windows.
- Describir los modelos de implementación y modelos de versiones para Windows como servicio (WaaS), incluidos los anillos de implementación.
- Describir las capacidades de Azure Virtual Desktop (AVD) y cuándo tiene sentido implementarlo.

## Describir Windows como servicio

Windows 10 es un sistema operativo de escritorio completo que permite trabajar de manera eficiente y segura. Mantener actualizado el sistema operativo de escritorio es importante porque permite que los dispositivos se ejecuten de manera eficiente y permanezcan protegidos.

Windows-as-a-Service (WaaS) es una nueva forma de trabajar con el escritorio de Windows. En el pasado, se lanzaban nuevas funciones cada pocos años y su implementación requería un esfuerzo significativo. Con Windows-as-a-Service, se lanzan nuevas funciones dos veces al año. Al lanzar nuevas funciones en pequeños fragmentos, en lugar de grandes versiones nuevas, se reduce el trabajo requerido por el personal de TI.

El modelo Windows-as-a-Service está diseñado para simplificar la vida tanto de los usuarios como de los profesionales de TI. Hay dos tipos de actualizaciones: funciones y correcciones de calidad.

## Actualizaciones de características

Las actualizaciones de funciones se publican dos veces al año. Debido a que estas actualizaciones son más frecuentes, son más pequeñas. Esto ofrece una serie de beneficios:

- Hay menos interrupciones y se requiere menos esfuerzo para aplicar nuevas funciones.
- Los usuarios son más productivos con un acceso más rápido a las nuevas funciones de Windows.
- Los usuarios tardan menos en adaptarse a cambios más pequeños.
- Se reduce la carga de trabajo y el impacto en los costes de actualizar Windows.

## Actualizaciones de calidad

Las actualizaciones de calidad incluyen correcciones y parches de seguridad. Suelen emitirse una vez al mes. Además, se publica una actualización acumulativa que incluye todas las actualizaciones anteriores. Las actualizaciones de calidad mensuales implican numerosos beneficios:

- Los problemas de seguridad identificados se solucionan y se implementan rápidamente, lo que mantiene los dispositivos seguros.
- Todos reciben correcciones de seguridad con regularidad, manteniendo todos los dispositivos alineados.

## Canales de mantenimiento

Los canales de mantenimiento proporcionan un método para controlar la frecuencia con la que las organizaciones implementan las características de Windows 10. Los canales de mantenimiento permiten controlar cómo y cuándo se aplican las actualizaciones. Windows-as-a-Service ofrece tres canales de mantenimiento, cada uno de los cuales recibe actualizaciones de funciones con diferente frecuencia:

- **Insider preview.** Este canal recibe características de Windows antes del lanzamiento general, a menudo durante el desarrollo. Esto permite a las organizaciones probar y evaluar nuevas características y proporcionar comentarios a Microsoft.
- **Canal semestral.** Las actualizaciones de características para el canal semestral se lanzan dos veces al año.
- **Canal de mantenimiento a largo plazo.** Diseñado para dispositivos especializados que no ejecutan aplicaciones de Office, como equipos médicos o cajeros automáticos. Estos reciben nuevas funciones cada dos o tres años.

## Anillos de implementación

Los anillos de implementación son grupos de dispositivos que se utilizan para probar nuevas funciones antes de implementarlas en el resto de la organización.

Consulte más información sobre Windows-as-a-Service aquí. Para un caso práctico más detallado, consulte [Adoptar Windows-as-a-Service en Microsoft](#).

## Administrar Windows como servicio

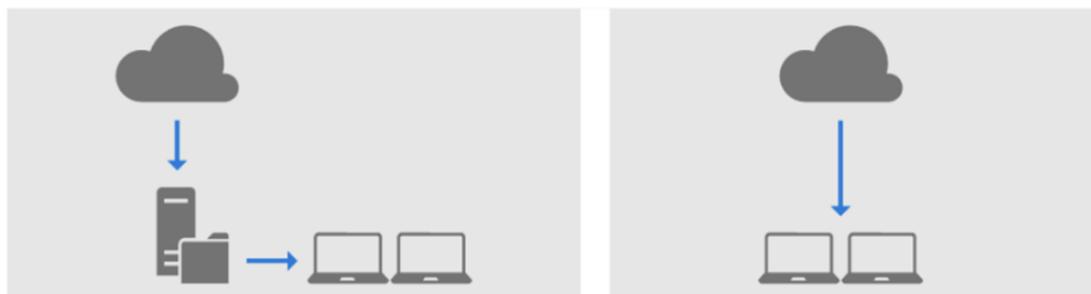
En Configuration Manager, puede ver el estado de Windows-as-a-Service (WaaS) en su entorno. Puede crear planes de mantenimiento para formar anillos de implementación y asegurarse de que los sistemas Windows 10 se mantengan actualizados cuando se lanzan nuevas compilaciones. También puede ver alertas cuando los clientes de Windows 10 están cerca del fin de soporte para su compilación de canal semestral.

## Explorar los métodos de implementación para Windows 10

La implementación de Windows 10 depende de varios factores, como:

- Requisitos comerciales.
- Consideraciones medioambientales.
- Cantidad de control administrativo necesario.
- Capacidad de la red.
- Capacidades de implementación actuales.

Puede elegir entre una variedad de herramientas de implementación nuevas y existentes para Windows 10, como Windows Autopilot y Microsoft Deployment Toolkit para Windows, e Intune y Configuration Manager para Windows. Como parte de la implementación, también puede elegir si desea implementar Windows desde la nube o desde un origen local de su red.



## Opciones de implementación para Windows 10

Windows 10 incluye las siguientes herramientas y métodos de implementación nuevos:

- **Windows Autopilot.** Personalice la experiencia lista para usar (OOBE) para implementar aplicaciones y configuraciones preconfiguradas para su organización. Incluya solo las aplicaciones que necesitan los usuarios. Autopilot es la manera más sencilla de implementar un equipo nuevo con Windows 10. También puede usarlo con Configuration Manager para actualizar Windows 7 o Windows 8.1 a Windows 10.
- **Actualización local.** Actualice el sistema operativo de un dispositivo sin reinstalarlo. Puede migrar aplicaciones, datos de usuario y configuraciones de una versión de Windows a otra (como pasar de Windows 8.1 a Windows 10). También puede actualizar de una versión de Windows 10 a la siguiente (como pasar de la versión 1803 a la versión 1809 de Windows 10).

- **Aprovisionamiento dinámico.** Cree un paquete de aprovisionamiento para configurar rápidamente uno o más dispositivos, incluso aquellos que no dispongan de conectividad de red. Los paquetes de aprovisionamiento se crean con el Diseñador de configuración de Windows y se pueden instalar mediante una red, desde un medio extraíble (como una unidad USB) o en códigos de barras o etiquetas de transmisión de datos en proximidad (NFC).
- **Activación de suscripción.** Use una suscripción para cambiar de una edición de Windows 10 a otra. Por ejemplo, puede cambiar de Windows 10 Pro a Windows 10 Enterprise. Cuando un usuario con licencia inicia sesión en un dispositivo (y tiene credenciales asociadas a una licencia de Windows 10 E3 o E5), el sistema operativo cambia de Windows 10 Pro a Windows 10 Enterprise y todas las funciones de Windows 10 Enterprise adecuadas se desbloquean. Si la suscripción expira (o se transfiere a otro usuario), el dispositivo se revierte sin problemas a la edición de Windows 10 Pro tras un período de gracia de hasta 90 días.

**Nota:** Utilice Windows Autopilot para implementar y configurar de forma remota dispositivos Surface en un proceso sin intervención, de forma inmediata. Los dispositivos se inscribirán y configurarán automáticamente cuando se enciendan por primera vez. Este proceso elimina la creación de nuevas imágenes durante la implementación, lo que le permite implementar métodos nuevos y ágiles de administración y distribución de dispositivos.

Además de estas nuevas herramientas, puede implementar Windows 10 con las herramientas de administración de escritorio y las herramientas existentes de su organización, incluidos Microsoft Endpoint Manager, que incluye Intune y Configuration Manager.

## Explicar cómo Windows se mantiene seguro y actualizado

Hay varias formas de obtener actualizaciones de Windows, así que considere qué estrategia es mejor para su organización.

Para reducir el consumo de ancho de banda, puede habilitar el uso compartido de contenido entre iguales. Hay dos opciones entre iguales para la distribución de contenido: **Optimización de entrega** y **BranchCache**.

Optimización de entrega permite a los clientes de Windows 10 obtener contenido de otros dispositivos en su red local que ya han descargado las actualizaciones o de otros a través de Internet. BranchCache es una tecnología de optimización del ancho de banda incluida en algunas ediciones de Windows Server 2016, el sistema operativo Windows 10 y algunos otros sistemas operativos. Con BranchCache, los archivos se almacenan en caché en cada cliente individual y otros clientes pueden recuperarlos según sea necesario.

O, si su organización usa Windows Intune, las actualizaciones de Windows se pueden implementar usando Intune.

Esta guía interactiva presenta dos formas de optimizar la entrega de actualizaciones de Windows 10. Aprenderá a:

- Reducir el consumo de ancho de banda.
- Acelerar la distribución de contenido al permitir el intercambio entre iguales.

## Describir las opciones de mantenimiento para Windows 10

En esta guía interactiva, aprenderá acerca de varias opciones de mantenimiento diferentes para Windows 10.

Verá cómo implementar actualizaciones de Windows 10 mediante secuencias de tareas y planes de servicio automatizados en System Center Configuration Manager. También verá cómo usar Microsoft Intune para administrar las actualizaciones de Windows 10 en todos sus dispositivos.

Puede crear una secuencia de tareas en Configuration Manager para actualizar automáticamente un sistema operativo, como de Windows 7 a Windows 10, en un equipo de destino. Este método le permite mantener las aplicaciones, la configuración y todos los datos del usuario en el equipo.

Con Microsoft Intune, puede administrar sus actualizaciones de Windows. Esto incluye ver información sobre la actualización, aprobar o rechazar la actualización y ver los equipos que instalarán la actualización cuando se apruebe.

Siga la guía interactiva para ver cómo:

- Implementar actualizaciones.
- Automatizar actualizaciones
- Administrar dispositivos con Microsoft Intune.

## Describir Azure Virtual Desktop (AVD)

Azure Virtual Desktop es un servicio que permite a los usuarios conectarse a un escritorio de Windows que se ejecuta en la nube. Disfrutan de todos los beneficios del escritorio de Windows y las aplicaciones Microsoft 365, sin la sobrecarga de instalar software en el dispositivo local.

Azure Virtual Desktop es un servicio de virtualización de escritorio y de aplicaciones que se ejecuta en Azure. Esto es lo que puede hacer:

- Configurar una **implementación de Windows 10 multisesión** que ofrece un Windows 10 completo con escalabilidad.
- **Virtualizar Office 365 ProPlus** y optimizarlo para que se ejecute en escenarios virtuales multiusuario.
- Proporcionar **Escritorios virtuales de Windows 7** con actualizaciones de seguridad extendidas gratuitas.

- Traer sus aplicaciones y escritorios de servicios de escritorio remoto (RDS) y Windows Server existentes a **cualquier PC**.
- **Virtualizar tanto escritorios como aplicaciones.**
- Administrar las aplicaciones y los escritorios de Windows 10, Windows Server y Windows 7 con una experiencia de **administración unificada**.

Para algunas situaciones, esto les otorga a las organizaciones beneficios significativos:

- **Implementar** aplicaciones y escritorios de Windows en minutos.
- **Escalar** fácilmente proporcionando acceso a los datos en todos los dispositivos rápidamente.
- Proporcionar acceso a los datos a la vez que se cumplen con las **regulaciones de seguridad y cumplimiento**.
- Proporcionar a los usuarios el **mismo aspecto y sensación** que al ejecutar aplicaciones de Office en un equipo dedicado.
- La organización **paga solo por lo que usa** con lo que consumen los usuarios en Azure Virtual Machines y Azure Storage.
- Cuando sus necesidades de almacenamiento difieren según la temporada, solo paga por lo que necesita cuando lo necesita.

Use Azure Virtual Desktop para necesidades específicas, como cuando la seguridad es importante, ya que todos los datos se almacenan en el servidor y no se pueden dejar en el dispositivo de un usuario.

**Nota:** Azure Virtual Desktop en Surface le permite ejecutar la infraestructura de escritorio virtual (VDI) en un dispositivo Surface. Azure Virtual Desktop en Surface difumina las líneas entre la experiencia del escritorio local y el virtual, donde las funciones táctiles, el uso de lápiz y la autenticación mediante datos biométricos abarcan los entornos físicos como los virtuales. Disfrute del soporte para lo siguiente:

- Factores de forma flexibles como dispositivos 2 en 1.
- Escenarios de trabajo persistentes, bajo demanda y justo a tiempo.
- Seguridad y capacidad de administración de dispositivos modernos de Windows 10.

Descubra más aquí: [Windows Autopilot y dispositivos Surface](#)

Obtenga más información sobre Azure Virtual Desktop aquí: [¿Qué es Azure Virtual Desktop?](#)

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Qué es Windows como servicio?

- A. La capacidad de ejecutar Windows como un escritorio virtual
- B. Windows 10 con actualizaciones periódicas de funciones
- C. Windows 10 Mobile

¿Cómo se controla la frecuencia de las actualizaciones con Windows como servicio?

- A. Actualizaciones de Windows
- B. Anillos de implementación
- C. Canal de servicio

¿Qué grupo de usuarios podría beneficiarse de Azure Virtual Desktop?

- A. Usuarios que necesitan ejecutar un escritorio Mac
- B. Usuarios que trabajan con datos confidenciales
- C. Usuarios con mala conectividad a Internet

¿Qué usaría para administrar Windows como servicio?

- A. Configuration Manager
- B. Actualizaciones de Windows
- C. Azure Virtual Desktop

# Aproveche la inteligencia empresarial con análisis e informes de Microsoft 365

## Introducción

Muchas organizaciones se centran en tomar decisiones basadas en datos y no en opiniones. Fomentar una cultura de datos afecta a todas las partes de una organización, incluida la forma en que trabajan las personas.

En este módulo, veremos las capacidades de informes y análisis en Microsoft 365.

Microsoft 365 incluye dos herramientas de análisis que recogen datos y utilizan la inteligencia artificial para proporcionar información sobre los hábitos de trabajo de los usuarios y las organizaciones:

- MyAnalytics
- Workplace Analytics

Además, use los diversos informes de actividad de Microsoft 365 en los centros de administración para averiguar cómo las personas de la organización están adoptando los servicios de Microsoft 365.

Al final de este módulo, podrá hacer lo siguiente:

- Describir las **funcionalidades de análisis** en Microsoft 365.
- Describir las funcionalidades de **Workplace Analytics** y **MyAnalytics**.
- Describir los informes disponibles en el **Centro de administración de Microsoft 365** y otros centros de administración.

## Descubrir cómo Workplace Analytics puede ayudar a las organizaciones a mejorar la productividad

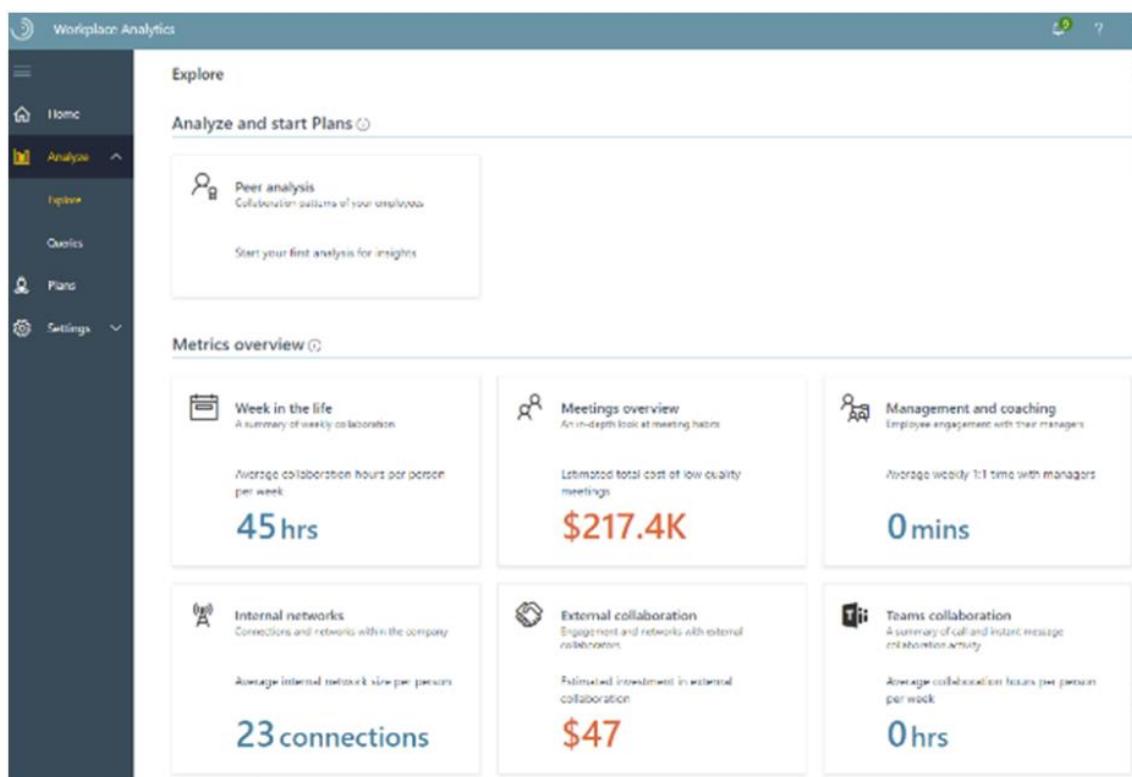
Ser más productivo no significa necesariamente trabajar más duro o durante más horas. A menudo, ser más productivo significa dedicar tiempo a concentrarse en el trabajo de alta prioridad o colaborar con las personas adecuadas. Workplace Analytics y MyAnalytics recopilan datos y utilizan inteligencia artificial para proporcionar información sobre los hábitos de trabajo de las personas y las organizaciones.

## Workplace Analytics

Workplace Analytics de Microsoft 365 usa datos de cómo las personas están trabajando actualmente para identificar áreas en las que podrían ser más productivas. Existe una variedad de métricas para ayudarle a comprender los datos y las prácticas laborales de su organización:

- **Vista semanal** da un resumen de la colaboración diaria en la organización.

- **Resumen de reuniones** ofrece un resumen de las normas de reuniones dentro de su organización.
- **Administración y entrenamiento** ofrece un resumen de la colaboración entre líderes, gerentes y empleados.
- **Redes internas** muestra conexiones de red exclusivamente entre diferentes personas dentro de una empresa, por ejemplo, entre el departamento de ventas y el departamento de recursos humanos.
- **Colaboración externa** ofrece un resumen de los patrones de red de los empleados con personas ajenas a la empresa.
- **Colaboración en Teams** muestra información y tendencias de comunicación sobre cómo los empleados de su organización usan Teams para comunicarse y colaborar.



Workplace Analytics identifica patrones de colaboración que afectan a la productividad, la efectividad de los recursos y el compromiso de los empleados. Tiene varios beneficios:

- Los datos se generan a partir de los patrones de trabajo reales de las personas.
- No hay interrupciones ni se requiere trabajo adicional.
- Tiene paneles e informes integrados que muestran los datos.
- Genera conclusiones para aprender e identifica mejoras para la forma de trabajar.

Workspace Analytics se ha diseñado para ayudar a las organizaciones a identificar las tendencias en países o regiones, departamentos o equipos. La cultura organizativa juega un papel importante en nuestra forma de trabajar. Con Workplace Analytics de Microsoft 365, las organizaciones pueden identificar patrones de trabajo entre grupos

similares y considerar cambios que podrían ayudar a las personas a trabajar de manera más eficaz.

Con los datos de Workspace Analytics, las personas reciben un impulso para pensar en la forma en que están trabajando. Workplace Analytics nos proporciona información sobre nuestras redes de colaboración y nuestros patrones de trabajo diarios, y nos anima a reflexionar sobre cómo trabajamos. Y Workplace Analytics utiliza Microsoft 365 fiable para mantener sus datos seguros y protegidos.

Los roles de Workplace Analytics se asignan para que los administradores puedan establecer los valores predeterminados del sistema y la configuración de privacidad, así como cargar y comprobar los datos de la organización. Los analistas de datos pueden iniciar sesión y utilizar Workplace Analytics después de que se proporcionen los datos. Véase [Asignar roles](#).

**Nota:** De forma predeterminada, Workplace Analytics no incluye datos personales en sus informes. Sin embargo, existe una confidencialidad potencial sobre el posible uso de los datos. La implementación exitosa de Workplace Analytics requiere una planificación y una reflexión cuidadosas, particularmente con respecto a la protección de datos. Más información sobre [Consideraciones de protección de datos](#).

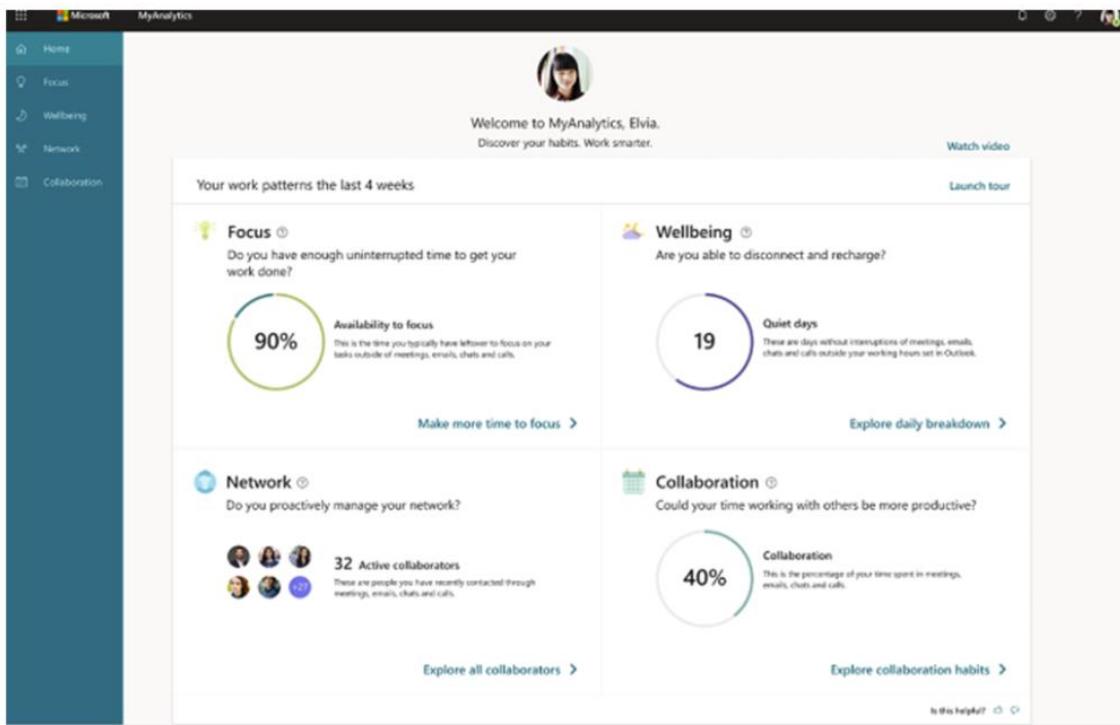
Para obtener más información sobre Workplace Analytics, eche un vistazo a estos recursos:

- [Workplace Analytics](#)
- [Explorar Workplace Analytics](#)

## MyAnalytics

MyAnalytics proporciona información sobre dos de los factores clave en la productividad personal: cómo y con quién invierten el tiempo las personas. Usted y su equipo pueden obtener estos beneficios después de que un administrador configure MyAnalytics en su organización. MyAnalytics se entrega por correo electrónico todas las semanas. Como alternativa, vaya a <https://myanalytics.microsoft.com> para acceder a su panel personal. Las métricas incluyen los elementos siguientes:

- **Enfoque y bienestar.** Muestra si tiene suficiente tiempo para el trabajo ininterrumpido, con consejos sobre cómo proteger su calendario y administrar las distracciones.
- **Red y colaboración.** Muestra información sobre sus relaciones con las personas de su red, según sus actividades laborales a lo largo del año en curso.
- **Perspectivas de productividad.** Muestra información sobre sus patrones de trabajo en torno a la concentración, la red, el bienestar y la colaboración durante las últimas cuatro semanas. Esta información muestra observaciones y tendencias de sus hábitos de trabajo más recientes a partir de sus datos de Office 365.



El panel de MyAnalytics se abre desde la página **Inicio** que muestra estadísticas sobre sus patrones de trabajo durante el mes pasado, incluido su tiempo de concentración y colaboración, cuántos días pudo desconectarse del trabajo y qué tan eficazmente establece redes con sus compañeros de trabajo.

Los objetivos individuales de MyAnalytics se pueden establecer encontrando la métrica relevante y estableciendo un objetivo medible. Puede establecer objetivos para aumentar su tiempo de concentración o asistir a menos reuniones ineficaces y recibir comentarios cada semana sobre su desempeño.

**Nota:** Solo usted puede ver sus datos. MyAnalytics procesa la información de una manera que protege la privacidad de los empleados y respalda el cumplimiento de las regulaciones locales de privacidad de datos. Si desea obtener más detalles, consulte la Guía de privacidad para administradores de MyAnalytics.

Descubra más aquí:

- [MyAnalytics](#)
- [Panel de MyAnalytics](#)
- [Establecer objetivos de MyAnalytics](#)
- [Pasos para habilitar el análisis de uso de Microsoft 365](#)

## Centro de administración de Microsoft 365

El **Centro de administración de Microsoft 365** está diseñado para que los profesionales de TI administren la suscripción de M365 de la organización. Se trata de un servicio en la nube que le permite realizar una serie de tareas, como añadir y eliminar usuarios, administrar licencias, restablecer contraseñas y ver **informes**.

The screenshot shows the Microsoft 365 Admin center interface. On the left is a vertical navigation bar with icons for Home, Users, Domains, Groups, Devices, Reports, Help, and Settings. The main area has a header "Office 365 Admin center". Below it is a search bar "Busque usuarios, grupos, opciones de configuración o tareas". The main content area is divided into several sections: "Users active" (with options to Add user, Delete user, Edit user, and Reset password), "Support" (with options to Create service request and View service requests), and "Software Office" (with options to Install software, Share download link, Configure download settings, and Solve installation problems). There's also a "Domains" section and a chart titled "Users active" showing usage trends for various services from August 20 to September 17, 2016.

Consulte de un vistazo cómo las personas de su organización utilizan los diferentes servicios de Microsoft 365. Debe tener permisos de administrador para poder ver informes.

Hay tres tipos de informes:

- **Puntuación de productividad.** Esta puntuación evalúa el trabajo realizado en su organización comparado con otras organizaciones como la suya.
- **Utilización.** Ver el uso por período de tiempo y el servicio de Microsoft 365 para comprender cómo las personas de su organización utilizan los servicios de Microsoft 365.
- **Seguridad y cumplimiento.** Ver los datos sobre detecciones de malware, usuarios afectados, protección contra amenazas, cifrado, etc.

Puede utilizar el panel prediseñado para visualizar el uso de los diferentes productos. El panel también le permite obtener más detalles de varios informes prediseñados y puede crear informes personalizados.

También puede usar Power BI con análisis de uso de Microsoft 365 para obtener más información sobre cómo está funcionando su organización. Para más información, consulte [Habilitar análisis de uso de Microsoft 365](#).

El Centro de administración de Microsoft 365 también le ofrece acceso para abrir centros de administración independientes para servicios específicos, como Exchange, Yammer y otros. Para acceder al centro de administración, vaya a [admin.microsoft.com](http://admin.microsoft.com) e inicie sesión con su cuenta de administrador. También puede acceder a la aplicación móvil de administración de Microsoft 365.

# Describir los centros de administración adicionales en Microsoft 365

El centro de administración de Microsoft 365 es el punto de entrada común para todos los administradores de Microsoft 365. Utilice su cuenta de administrador para acceder a ella en [admin.microsoft.com](https://admin.microsoft.com).

Si desea ver informes sobre un área específica, como **Seguridad y cumplimiento** o **Administración de dispositivos**, expanda el menú de navegación para encontrar los **Centros de administración** adicionales en la parte inferior.

Todos los centros de administración		
	Nombre	Descripción
	Azure ATP	Identifique, detecte e investigue las amenazas avanzadas, las identidades en peligro y las acciones sospechosas.
	Azure Active Directo	Consiga mejores resultados con la administración de identidades. Habilite la autenticación multi factor y la administración centralizada.
	Compliance	Administre sus necesidades de cumplimiento con soluciones integradas para gobierno de datos.
	Administrador de experiencia	Una única experiencia de administración para el equipo de informática de usuario final en el dispositivo.
	Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center.
	Microsoft Search	Administre la configuración de Búsqueda de Microsoft, incluidos los servicios y contenidos que se indexan.
	Power Apps	Use the Power Platform admin center to manage activity, licenses, and policies for user-generated apps.

Cada centro de administración especializado le ofrece más opciones para esa área específica. El menú le proporciona una lista de centros de administración adicionales, cada uno con sus propios informes, que incluyen los siguientes:

- **Seguridad y cumplimiento.** Incluye una puntuación de seguridad colectiva con el estado de las identidades, los datos, los dispositivos, las aplicaciones y la infraestructura.
- **SharePoint.** Obtenga una vista de alto nivel del valor que recibe de SharePoint en términos de la cantidad total de archivos que los usuarios almacenan en los sitios de SharePoint, cuántos archivos se están usando activamente y el almacenamiento consumido en todos estos sitios. Luego, puede profundizar en el informe de uso del sitio de SharePoint para comprender las tendencias y los detalles por nivel de sitio para todos los sitios.
- **Teams.** En el informe de actividad del usuario de Microsoft Teams puede obtener información sobre la actividad de Microsoft Teams en su organización. Obtenga una vista de la actividad consultando los gráficos Actividad y Usuarios.
- **Exchange.** Obtenga una vista de alto nivel del tráfico de correo electrónico dentro de su organización. Explore en profundidad el widget de actividad de

- correo electrónico para comprender las tendencias y los detalles por nivel de usuario de la actividad de correo electrónico dentro de su organización.
- **Administración de dispositivos.** Los informes de Microsoft Intune le permiten supervisar de forma proactiva el estado y la actividad de los puntos de conexión en toda su organización. Puede ver informes sobre el cumplimiento, el estado y las tendencias del dispositivo. Además, puede crear informes personalizados para obtener datos más específicos.

Ahora que ha practicado con la guía a través de clics, obtenga más información sobre los informes disponibles en el centro de administración de Microsoft 365:

- [Informes de Microsoft 365 en el centro de administración](#)
- [Asistencia del Centro de administración de Microsoft 365](#)

Para obtener más información, consulte:

- [Centros de administración especializados](#)
- [Informes en el Centro de seguridad y cumplimiento](#)
- [Informes del Centro de administración de SharePoint](#)
- [Informes del centro de administración de Teams](#)
- [Actividad de correo electrónico de Exchange](#)
- [Informes de Intune](#)

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Qué es MyAnalytics?

- A. La capacidad de ordenar automáticamente su correo electrónico
- B. Un análisis de sus patrones de trabajo enviados por correo electrónico
- C. La capacidad de ejecutar módulos de IA en Azure

¿Dónde se pueden encontrar los informes sobre la actividad y el uso de SharePoint?

- A. Centro de administración de SharePoint
- B. Configuration Manager
- C. Centro de administración de Intune

¿De qué formas se puede personalizar la página principal del Centro de administración de Microsoft 365?

- A. No puede personalizar la página principal del Centro de administración de Microsoft 365.
- B. Si se agregan tarjetas que se adapten a sus necesidades.
- C. Usar el Centro de cumplimiento de Microsoft 365.

¿Cuál es la principal ventaja de Workplace Analytics?

- A. Ayuda a la organización a comprender cómo colaboran los grupos.
- B. Reduce los costes al cobrar solo por el almacenamiento que realmente necesita.
- C. Reduce el tiempo necesario para escribir informes en Word.

## Module 3 - Demostrar conocimientos fundamentales de las licencias, el servicio y el soporte técnico de Microsoft 365

¿Qué es Microsoft 365?

### Introducción

En este módulo, se familiarizará con Microsoft 365, la nube de productividad del mundo que aporta experiencias innovadoras e inteligentes, información organizativa detallada y una plataforma de confianza para ayudar a las personas y a las organizaciones a ser más productivas. Además, mientras aprende sobre Microsoft 365, también se estará preparando para la certificación de Conceptos básicos de Microsoft 365 (MS-900). Este conjunto de rutas de aprendizaje le llevará paso a paso por los conceptos básicos de la plataforma Microsoft 365.

### ¿Qué es Microsoft 365?

Microsoft 365 ayuda a los usuarios con la innovación más reciente en experiencias de productividad nuevas y familiares, como Teams, Word, Excel, PowerPoint, Outlook y Windows. A diferencia de otros servicios de productividad, Microsoft 365 aprende de los usuarios y recopila información valiosa a través de Microsoft Graph para ofrecer experiencias mejoradas que mejoran continuamente a lo largo del tiempo y mantienen protegidos a los usuarios. Microsoft 365 ayuda a las organizaciones con las siguientes características:

Capacidad	Descripción
Productividad y trabajo en equipo	Incluye mensajería instantánea y reuniones en línea con Microsoft Teams, correo electrónico y calendario con Outlook, las conocidas aplicaciones de Office en todos los dispositivos, almacenamiento y uso compartido de archivos avanzados con OneDrive, sitios de intranet y de equipo, y redes sociales empresariales con Yammer.
Administración de empresas	Incluye la administración simplificada de TI con Microsoft Endpoint Manager, automatización de los procesos de negocio, extensibilidad con Teams y Power Platform, sistema de voz y teléfono empresarial con Teams, administración de formularios y flujos de trabajo, inteligencia empresarial con Workplace Analytics y administración del trabajo con Project Online.
Seguridad y cumplimiento	Incluye soluciones para la administración de la identidad y el acceso, protección de la información y gobernanza, protección contra amenazas, administración de la seguridad, administración de riesgos internos, administración de cumplimiento y eDiscovery.

Algunos componentes de Microsoft 365, como las aplicaciones Microsoft 365 y Windows, se entregan mediante el modelo de **software como servicio (SaaS)**. SaaS es un software hospedado y administrado centralmente por un **proveedor de servicios en la nube (CSP)** para clientes. En general, los CSP proporcionan una versión de una aplicación para todos los clientes que otorgan mediante una suscripción mensual o anual.

## Objetivos de aprendizaje

En este módulo, podrá hacer lo siguiente:

- Enumerar las capacidades de Microsoft 365
- Comprender el valor que aportan las soluciones de Microsoft 365
- Nombrar las opciones de suscripción de Microsoft 365
- Crear una evaluación de la organización en Microsoft 365
- Explorar las áreas de estudio y las rutas de aprendizaje del examen de Conceptos básicos de Microsoft 365

## Nivel

Principiante

## Público

El público de este curso está empezando a conocer la productividad en la nube y cómo Microsoft 365 ofrece ese servicio. El contenido del conjunto de rutas de aprendizaje se alinea con el dominio objetivo del examen MS-900.

## **Requisito previo**

- Conocimientos básicos de la informática en la nube. Si no tiene conocimientos sobre informática en la nube, le recomendamos que vea [Conceptos de la nube: principios de la informática en la nube](#)

## **Explore las ventajas de productividad de Microsoft 365**

Microsoft 365 usa la potencia de la nube para ayudar a las personas y organizaciones a aumentar su productividad para lograr mayores resultados.

### **Productividad personal**

Microsoft 365 ofrece funciones eficaces a través de herramientas con tecnología de IA para impulsar la creatividad y propiciar la innovación en su organización. Desde presentaciones atractivas hasta modelos 3D animados y experiencias inmersivas de realidad mixta, ahora puede crear contenido de alta calidad que realmente se destaque. Las herramientas con tecnología de IA le ayudan a convertir una masa cada vez mayor de datos en información procesable para transformar su organización. Manténgase al día con menos distracciones y acceda fácilmente a las personas y a la información que necesita sin salir del flujo de su trabajo. Cuando la inspiración llega, pasa sin esfuerzo del pensamiento al contenido gracias al uso de funciones de voz, entrada táctil y lápiz en cualquier dispositivo.

### ***Permitir el trabajo en equipo y simplificar el flujo de trabajo***

Colaborar, reunirse, llamar y conectar aplicaciones empresariales en un único sitio con Microsoft Teams.

### **Productividad desde cualquier lugar**

Pase fácilmente de equipos a dispositivos móviles con aplicaciones móviles innovadoras y eficaces.

### ***Obtenga mayor productividad con las herramientas habilitadas para IA***

Potencie la creatividad, descubra nuevas perspectivas, mejore las búsquedas y obtenga asistencia personalizada con características de inteligencia integradas.

### **Productividad en la organización**

Las organizaciones siempre intentan destacar en un entorno comercial en constante evolución. Quieren impulsar el crecimiento, reducir los costos y servir mejor a sus clientes. Quieren desbloquear el potencial de sus empleados, impulsar la automatización de procesos, capturar el conocimiento colectivo de su organización y evitar posibles riesgos de seguridad, cumplimiento normativo y privacidad que puedan interferir en el progreso.

### ***Aumentar los conocimientos de la organización***

Convierta rápidamente los datos en perspectivas y ofrezca a los empleados la información y la experiencia que necesitan para realizar su trabajo con Workplace Analytics.

### ***Administrar todos los puntos de conexión***

Implemente una solución de administración fluida de un extremo a otro y mejore la visibilidad entre todos los dispositivos conectados con Microsoft Endpoint Manager.

### ***Proteja su empresa***

Eleve y modernice su seguridad, administre los riesgos y cumpla los estándares de cumplimiento en la nube de confianza de Microsoft.

## **Explorar las opciones de suscripción de Microsoft 365**

Cada organización tiene requisitos únicos, por lo que Microsoft ofrece una amplia variedad de suscripciones y planes para satisfacer las necesidades de su organización. En esta unidad, resumimos estas suscripciones.

**NOTE:** Los planes, el conjunto exacto de características, precios y requisitos de licencia pueden variar entre países y regiones. Si necesita una suscripción a Microsoft 365 para una organización no estadounidense, póngase en contacto con su representante de ventas regional para averiguar qué suscripciones, planes, características y precios hay disponibles.

### **Microsoft 365 Enterprise**

Microsoft 365 Enterprise ofrece servicios de clase empresarial para organizaciones que quieren una solución de productividad que incluya características seguras de protección contra amenazas, seguridad, cumplimiento de normas y análisis.

Hay tres planes disponibles de Microsoft 365 Enterprise, que le permiten ajustar aún más lo que se incluye en su implementación: E3, E5 y F3 (anteriormente conocido como F1). E5 incluye las mismas características que E3 y las herramientas más recientes de protección contra amenazas avanzada, seguridad y colaboración. F3 está diseñado para personal de primera línea mediante recursos y herramientas dedicadas que les permiten dar lo mejor de sí.

Puede [comparar los planes para empresas](#) para ver cuál se adapta a sus necesidades específicas.

### **Microsoft 365 para empresas**

Microsoft 365 para empresas está diseñado para pequeñas y medianas organizaciones. Como Microsoft 365 Enterprise, Microsoft 365 para empresas ofrece el conjunto completo de herramientas de productividad de Office 365 e incluye características de seguridad y administración de dispositivos. No incluye algunas de las herramientas de protección de la información, cumplimiento y análisis más avanzadas disponibles para los suscriptores de Enterprise. Se ha diseñado para organizaciones que necesitan hasta

300 licencias. Si su organización es más grande, tendrá que suscribirse a un plan de Microsoft 365 Enterprise.

Existen tres planes disponibles de Microsoft 365 para empresas: Básico, Estándar y Premium. [Compare planes para pequeñas empresas](#) para determinar cuál es el que mejor se adapta a su organización.

## Microsoft 365 Educación

Microsoft 365 Education está disponible para organizaciones educativas y permite a los profesores dar rienda suelta a la creatividad, fomentar el trabajo en equipo y aporta una experiencia segura y sencilla en una única solución económica diseñada para el ámbito educativo. Las licencias académicas se pueden modificar para adaptarse a las necesidades de cualquier institución, incluidas soluciones de productividad y seguridad para profesores, miembros del personal y estudiantes.

[Obtenga más información sobre las oportunidades de Microsoft Educación](#) para ver cómo su organización puede beneficiarse de Microsoft 365 para la Educación.

## Microsoft 365 Home

Microsoft 365 Home tiene el propósito de ofrecer las mismas ventajas de productividad en su vida personal y familiar. Microsoft 365 Home viene en dos planes: Microsoft 365 Familia y Microsoft 365 Personal. Office Home y Estudiantes 2019 están disponibles como compras de pago único, pero no incluyen ninguno de los beneficios de la nube de Microsoft 365. [Compare los planes](#) para ver cuál se adapta mejor a sus necesidades.

## Explorar el inquilino de Microsoft 365

Microsoft ofrece evaluaciones gratuitas para muchos de servicios diferentes, y también puede inscribirse para obtener una suscripción gratuita de 30 días para Microsoft 365 Empresa Premium en los siguientes vínculos. La versión de prueba gratuita permite hasta 25 usuarios. Experimente cómo Microsoft 365 facilita a los empleados para crear su mejor trabajo, simplifica los procesos de negocio y le ayuda a proteger los usuarios, los datos y la información de los clientes.

- [Suscríbase a una prueba gratuita de Microsoft 365 Empresa Premium](#)

Una vez que haya adquirido la prueba gratuita, explore los centros de administración de Microsoft 365 y Azure Active Directory con los siguientes ejercicios.

### Ejercicio 1: Iniciar sesión en el inquilino

1. Abra **Microsoft Edge**.
2. Diríjase a [www.office.com](http://www.office.com).
3. Inicie sesión con las credenciales de la cuenta de administrador global de su espacio empresarial de Office 365. Consulte la introducción al Laboratorio para adquirir un espacio empresarial de prueba de Office 365.
4. Haga clic en el ícono **Admin**.

## Ejercicio 2: Explorar el Centro de administración de Microsoft 365

1. En el Centro de administración de Microsoft 365, en el panel de navegación, seleccione **Mostrar todo**.
2. Expanda **Usuarios** y luego seleccione **Usuarios activos**. Vea las cuentas disponibles.
3. Haga clic en el primer nombre de usuario de la lista para seleccionarlo. Se abre una hoja en la que se muestra información más detallada sobre la cuenta. Para cerrar la hoja seleccione la **X** en la esquina superior derecha de la hoja.
4. Expanda **Grupos** y, luego, seleccione **Grupos**. Si usa una versión de prueba de espacio empresarial de Office 365 recién creada, esta página probablemente estará vacía. Si aún no tiene grupos, haga clic en **Agregar un grupo** para agregar uno.
5. Expanda **Facturación** y luego seleccione **Licencias**. Se debería mostrar al menos un conjunto de licencias.

## Ejercicio 3: Explore del centro de administración de Azure Active Directory

1. Expanda **Centros de administración** y luego seleccione Azure Active Directory. Observe que se abre una pestaña nueva en Microsoft Edge.
2. En el **Panel** del centro de administración de Azure Active Directory, seleccione **Azure Active Directory** desde el panel de navegación.
3. Haga clic en **Usuarios**. Observe que se muestran las mismas cuentas de usuario de Office 365.
4. Cierre la hoja Usuarios: Todos los usuarios. Observe que en el panel del área Usuarios y grupos se muestra el grupo que creó anteriormente. Puede ver los mismos grupos de Office 365. Puede hacer clic en **Buscar un grupo** en el área Tareas rápidas para buscar un grupo específico.
5. Cierre la hoja Grupos: Todos los grupos.
6. En el panel del Centro de administración de Azure Active Directory, haga clic en **Personalización de marca de empresa**.
7. Observe las opciones configuradas para la personalización de marca.
8. Cierre la hoja de personalización de marca de la empresa.

## Ejercicio 4: Explorar el centro de administración de Microsoft Teams

1. Amplíe los **centros de administración** y, después, seleccione el centro de administración de **Teams**.
2. En el centro de administración de Teams, el panel muestra tarjetas de la actividad reciente, enlaces útiles, búsquedas de usuarios y más.
3. Utilice el panel de navegación de la izquierda para administrar los ajustes de **Teams, usuarios, reuniones, ubicaciones** y más.
4. Seleccione **Teams** en el panel de navegación para configurar los ajustes de funciones como la integración de correo electrónico, las opciones de almacenamiento en la nube, la pestaña de organización, la configuración de dispositivos en la sala de reuniones y el ámbito de la búsqueda. Cuando realice cambios en estos ajustes, se aplicarán a todos los equipos de la organización.

5. El centro de administración de Teams permite a los administradores configurar **directivas** para Teams, incluidas **directivas de reuniones**, **directivas de mensajes**, **directivas de actualizaciones**, así como crear **paquetes de directivas**.
  - Las **directivas** se utilizan en el servicio de Microsoft Teams para garantizar que la experiencia que reciben los usuarios finales se ajusta a las necesidades de la organización.
  - Un **paquete de directivas** es una recopilación de ajustes y directivas predefinidos.
  - Las **directivas de reuniones** controlan las funciones que están disponibles para los participantes durante las reuniones.
  - Las **directivas de mensajes** controlan las funciones mensajes de chats y canales que están disponibles para los usuarios.
6. En **ajustes de la organización**, los administradores pueden configurar ajustes globales para el **acceso externo** y el **acceso de invitado**.
  - El **Acceso externo**, antes conocido como federación, permite a los usuarios de Teams y Skype Empresarial comunicarse con usuarios fuera de su organización.
  - El **Acceso de invitado** permite que usuarios ajenos a su organización accedan a los grupos y canales.
7. Explorar las partes adicionales del **Centro de administración de Teams**, como el **Panel de calidad de llamadas**, **Análisis e informes** y **Voz**, para explorar las capacidades adicionales de Microsoft Teams.

## Explorar las áreas de examen

El examen de certificación [MS-900: Conceptos básicos de Microsoft 365](#) está diseñado para aquellos que buscan demostrar conocimientos básicos sobre las consideraciones y ventajas de la adopción de servicios en la nube en general y del modelo de nube de software como servicio (SaaS). Los candidatos también deben conocer las opciones disponibles y las ventajas al implementar las ofertas de servicios en la nube de Microsoft 365.

El examen está destinado a candidatos con experiencia no técnica, como los que participan en la venta o la compra de soluciones y servicios basados en la nube. También está diseñado para los candidatos que tienen alguna relación con las soluciones y servicios basados en la nube, así como los candidatos con experiencia técnica que necesitan validar sus conocimientos de nivel básico respecto a los servicios en la nube. No es necesario tener experiencia técnica en TI, pero sería beneficioso contar con algún conocimiento o experiencia general sobre ello.

Este examen puede realizarse como un primer paso opcional en el aprendizaje de conceptos sobre servicios en la nube o como precursor de otros exámenes sobre servicios en la nube de Microsoft. Aunque sería un primer paso beneficioso para validar los conocimientos de nivel básico, realizar este examen no es un requisito previo para obtener cualquier otra certificación basada en Microsoft 365.

## Áreas de estudio

El examen incluye cuatro áreas de estudio. Los porcentajes indican el peso relativo de cada área en el examen. Cuanto mayor sea el porcentaje, más preguntas contendrá el examen. Asegúrese de leer la página del examen para obtener detalles sobre las aptitudes que se cubren en cada área.

Áreas de estudio de MS-900	Pesos
Describir los conceptos de la nube	10-15%
Describir los servicios y conceptos principales de Microsoft 365	30-35 %
Explicar la seguridad, el cumplimiento, la privacidad y la confianza en Microsoft 365	30-35 %
Describir los precios y soporte técnico de Microsoft 365	20-25 %

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Cuál de las siguientes opciones de suscripción de Microsoft 365 es adecuada para empresas con menos de 300 empleados?

- A. Microsoft 365 Enterprise
- B. Microsoft 365 para empresas
- C. Microsoft 365 Educación

¿Cuál de las siguientes opciones se incluye en Microsoft 365 Enterprise E5, pero no en Microsoft Enterprise E3?

- A. Más licencias de usuario
- B. Versiones localizadas
- C. Herramientas de protección contra amenazas avanzada, seguridad y colaboración

¿De qué funcionalidad de Microsoft 365 forma parte Microsoft Endpoint Manager?

- A. Productividad y trabajo en equipo
- B. Administración empresarial
- C. Seguridad y cumplimiento

# Identificar las opciones de licencia disponibles en Microsoft 365

## Introducción

Microsoft 365 está disponible en una amplia gama de suscripciones para el hogar, los negocios y la empresa. Al elegir la suscripción óptima, puede estar seguro de la funcionalidad que necesita en el paquete más rentable.

Al finalizar este módulo, podrá:

- Identificar las opciones de licencia disponibles en Microsoft 365.
- Describir las opciones de gestión y licencias para Microsoft 365.
- Describir las prestaciones adicionales disponibles cuando un cliente compra Azure Active Directory P1, Azure Active Directory P2 y Azure AD Basic.
- Planificar, predecir y comparar precios.
- Describir el modelo de precios del proveedor de soluciones en la nube (CSP) para Windows y los servicios en la nube de Microsoft.
- Explicar las opciones de administración de facturas y facturación disponibles, incluidos la frecuencia de facturación y los métodos de pago.
- Optimizar costes según las opciones de licencia.

## Comparar las opciones para el hogar, el negocio y la empresa

### Microsoft 365 para casa

Microsoft 365 proporciona dos suscripciones para usuarios domésticos. Las características son las mismas, pero Microsoft 365 Personal es para una persona con varios dispositivos, mientras que Microsoft 365 Familia es para hasta seis personas con varios dispositivos.

Word, Excel, PowerPoint, OneNote y Outlook se proporcionan para Windows, macOS, iOS y Android, mientras que Access y Publisher se proporcionan como versiones solo para PC.

### Microsoft 365 para organizaciones

Microsoft 365 tiene dos categorías de suscripción para organizaciones, Microsoft 365 para empresas, para organizaciones pequeñas y medianas, y Microsoft 365 empresarial, para organizaciones de tamaño empresarial.

### Microsoft 365 para empresas

Microsoft 365 para la Empresa tiene tres niveles de suscripción con diferentes características.

	<b>Microsoft 365 Empresa Básico</b>	<b>Aplicaciones de Microsoft 365 para empresas</b>	<b>Microsoft 365 Empresa Estándar</b>	<b>Microsoft 365 Empresa Premium</b>
<b>Aplicaciones de Microsoft 365</b>		X	X	X
<b>Exchange</b>	X		X	X
<b>OneDrive</b>	X	X	X	X
<b>SharePoint</b>	X		X	X
<b>Teams</b>	X		X	X
<b>Intune</b>				X
<b>Azure Information Protection</b>				X

Para obtener más información, lea [Encuentre la solución adecuada para usted](#)

## Microsoft 365 para empresas

Microsoft 365 para empresas tiene tres niveles de suscripción con diferentes características.

<b>Grupo de capacidades</b>	<b>Microsoft 365 F3</b>	<b>Microsoft 365 E3</b>	<b>Microsoft 365 E5</b>
<b>Aplicaciones de Microsoft 365</b>	Aplicaciones móviles de Office y Office para la web solamente	Completo	Completo
<b>Correo electrónico y calendario</b>	Completo	Completo	Completo
<b>Reuniones y voz</b>	Parcial	Parcial	Completo
<b>Social e intranet</b>	Completo	Completo	Completo

<b>Archivos y contenido</b>	Completo	Completo	Completo
<b>Administración de tareas</b>	Completo	Completo	Completo
<b>Análisis avanzados</b>		Parcial	Completo
<b>Administración de dispositivos y aplicaciones</b>	Completo	Completo	Completo
<b>Administración de identidades y acceso</b>	Parcial	Parcial	Completo
<b>Protección contra amenazas</b>	Parcial	Parcial	Completo
<b>Protección de la información</b>	Parcial	Parcial	Completo
<b>Administración de la seguridad</b>	Completo	Completo	Completo
<b>Cumplimiento avanzado</b>			Completo

**Microsoft 365 se divide en varios grupos de capacidades.**

<b>Grupo de capacidades</b>	<b>Descripción</b>
<b>Aplicaciones de Microsoft 365</b>	Se pueden instalar las aplicaciones de escritorio de Office (Word, Excel, PowerPoint, OneNote, Access) en hasta 5 PC/Mac + 5 tabletas + 5 teléfonos inteligentes por usuario con las aplicaciones de Microsoft 365 para empresas. Microsoft 365 F3 incluye las aplicaciones móviles de Office y Office para la web.
<b>Correo electrónico y calendario</b>	Incluye Outlook y Exchange.
<b>Reuniones y voz</b>	Microsoft 365 E5 incluye Microsoft Teams, llamadas de audio y sistema telefónico. Las suscripciones de E3 y F3 incluyen Microsoft Teams.
<b>Social e intranet</b>	Incluye SharePoint y Yammer.
<b>Archivos y contenido</b>	Incluye OneDrive, Stream y Sway.

<b>Administración de tareas</b>	Incluye Planner, Power Apps, Power Automate y Tareas pendientes.
<b>Análisis avanzados</b>	Microsoft 365 E5 incluye MyAnalytics y Power BI Pro. Las suscripciones de E3 incluyen MyAnalytics.
<b>Administración de dispositivos y aplicaciones</b>	Incluye Windows Enterprise, Centro de administración de Microsoft 365, Microsoft Intune, Windows Autopilot, Estado de dispositivos de Windows Analytics y Microsoft Endpoint Configuration Manager.
<b>Administración de identidades y acceso</b>	Incluye Windows Hello, Credential Guard, acceso directo y Azure Active Directory Premium plan 1. Microsoft 365 E5 también incluye Azure Active Directory Premium plan 2.
<b>Protección contra amenazas</b>	Incluye Microsoft Advanced Threat Analytics, Antivirus de Windows Defender y Device Guard. Microsoft 365 E5 también incluye Protección contra amenazas avanzada de Microsoft Defender, Protección contra amenazas avanzada de Microsoft 365 y Protección contra amenazas avanzada de Azure.
<b>Protección de la información</b>	Incluye Windows Information Protection y BitLocker y Azure Information Protection P1. Las suscripciones a Microsoft 365 E5 y E3 también incluyen la prevención de pérdida de datos de Microsoft 365. Microsoft 365 E5 además incluye Azure Information Protection P2 y Cloud App Security.
<b>Administración de la seguridad</b>	Incluye la puntuación de seguridad de Microsoft y el Centro de seguridad y cumplimiento de Microsoft.
<b>Cumplimiento avanzado</b>	Microsoft 365 E5 incluye eDiscovery avanzado, Caja de seguridad del cliente, Gobierno de datos avanzado, Cifrado de servicio con clave de cliente Privileged Access Management.

## Describir las capacidades adicionales disponibles con Azure

### Capacidades incluidas con Azure

La suscripción de Microsoft 365 para empresas incluye Microsoft Azure Active Directory P1 para crear y administrar cuentas de usuario y de grupo.

La suscripción de Microsoft 365 para empresas F3 incluye Microsoft Azure Active Directory Premium P1, con características adicionales de protección de la identidad de

Azure Active Directory Premium P2, para detectar y corregir los riesgos basados en la identidad. La suscripción de Microsoft 365 para empresas E3 incluye Microsoft Azure Active Directory P1 para crear y administrar cuentas de usuario y de grupo. La suscripción a Microsoft 365 para empresas E5 incluye una suscripción a Microsoft Azure Active Directory P1 y P2 para crear, administrar y proteger cuentas de usuario y de grupo.

Si no está incluido, Microsoft Azure Active Directory P2 se puede comprar adicionalmente e incluye protección de la identidad y la funcionalidad Identity Governance.

## **Describir el modelo de proveedor de soluciones en la nube**

### **Modelo de proveedor de soluciones en la nube**

Con el modelo de proveedor de soluciones en la nube (CSP), su suscripción se aporta a través de un asociado de CSP experto que puede administrar la suscripción, las licencias y las configuraciones de Microsoft 365 en su totalidad, así como aportar soporte técnico de nivel 1.

El asociado de CSP puede proporcionar consultoría y asesoramiento adicionales para garantizar que se cumplan los objetivos de seguridad y productividad. El programa Proveedor de soluciones en la nube (CSP) proporciona un modelo de suscripción de pago por uso para Windows 10 con precios por usuario y por mes que permite que su empresa escale o se reduzca verticalmente cada mes a medida que cambien sus necesidades.

Además, se pueden agregar productos y servicios adicionales basados en la nube de Microsoft a la suscripción, como los servicios de Microsoft 365 y Microsoft Azure.

Puede encontrar un CSP adecuado en [Estoy buscando un proveedor de soluciones](#).

## **Explorar las opciones de administración de facturas**

### **Administración de facturas y opciones**

La facturación en Microsoft 365 se administra desde el Centro de administración de Microsoft 365. Las opciones disponibles y los precios que se aplican a cualquier cuenta dependen de la suscripción y la cantidad de usuarios con licencia. Cada servicio tiene un precio específico; por lo general, calculado por usuario y por mes.

Puede revisar y modificar todos los aspectos de la facturación en el Centro de administración de Microsoft 365, entre los que se incluyen los siguientes:

- La cantidad actual de licencias adquiridas y la cantidad de licencias asignadas a los usuarios para cada servicio.
- Los cargos actuales pendientes de una cuenta.
- El método y la frecuencia de pago (mensual o anual).

- Otros servicios o características que puede agregar a la suscripción. Por ejemplo, en función de la suscripción de Microsoft 365 que tiene, puede agregar el almacenamiento de eDiscovery avanzado o en el conjunto de aplicaciones de Dynamics 365.
- Las notificaciones de facturación, a las que puede agregar una lista de cuentas de correo electrónico de usuarios que deben recibir las notificaciones de facturación y los avisos de renovación automatizados sobre la suscripción a Microsoft 365.

## Explicar las formas en que Microsoft 365 ayuda a optimizar los costes

### Optimización de costes

Microsoft 365 ayuda a optimizar los costes de varias formas:

#### Consolidación de costes de licencias de proveedores

La consolidación en un único conjunto o plataforma puede costar mucho menos que elegir diferentes proveedores para múltiples capacidades.

#### Ahorros en implementación y administración de TI

Microsoft ahora puede ser responsable del mantenimiento de su hardware y software. Esto ayuda a la TI en la transición a actividades de mayor valor.

#### Reducir el coste total del riesgo

La seguridad mejorada puede reducir las brechas de seguridad, proteger la privacidad y simplificar la corrección. Las soluciones de cumplimiento ayudan a reducir su riesgo.

## **Desplazamiento de costes de gastos físicos y de viaje**

Reduzca los costes de espacio de oficina trasladando a los empleados en el lugar a puestos permanentes, seguros y remotos. Permita una colaboración valiosa al tiempo que reduce los costes de viajes y entretenimiento.

## **Ahorre en automatización y mejoras de procesos**

Transforme y simplifique los procesos comerciales a través de flujos de trabajo, paneles, capacidades de inteligencia artificial y más, haciendo que sus empleados sean más productivos.

## **Flujo de caja de gastos de capital a gastos operativos**

Cambie los pagos de licencia por adelantado por gastos operativos pagados a lo largo del tiempo. Optimice sus flujos de caja eligiendo entre gastos de capital y gastos operativos.

## **Prueba de conocimientos**

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Qué suscripción de Microsoft 365 para empresas incluye Azure Information Protection? ( )Microsoft 365 Empresa Básico { {No es correcto. Microsoft 365 Empresa Básico no incluye Azure Information Protection} }

- A. Microsoft 365 Empresa Básico
- B. Microsoft 365 Empresa Premium
- C. Microsoft 365 Empresa Estándar

Con el modelo de proveedor de soluciones en la nube (CSP), ¿quién aporta su suscripción?

- A. Lo proporciona un socio de CSP
- B. Se proporciona directamente desde Microsoft
- C. Lo proporciona una tienda minorista

¿Cuál de los siguientes portales permite modificar el método de pago y la frecuencia de una suscripción a Microsoft 365?

- A. Centro de suscripciones de Microsoft 365
- B. Centro de seguridad de Microsoft 365
- C. Centro de administración de Microsoft 365

¿Cómo reduce Microsoft 365 el coste total del riesgo?

- A. Mejorando la seguridad
- B. Reduciendo los costes de espacio de oficina
- C. Transformando y optimizando los procesos de negocio

# Describir los beneficios de los servicios de Microsoft 365

## Introducción

Con otros servicios en la nube, el soporte técnico no se ofrece de manera gratuita y fácil, a menudo solo está disponible a través de complementos pagados o se paga por incidente. Sin embargo, Microsoft se compromete a ayudarlo a aprovechar al máximo los servicios de Microsoft 365. Puede confiar en las opciones de soporte de fácil acceso que vienen con los servicios de Microsoft 365 para ayudar a organizaciones como la suya a seguir siendo productivas y eficientes. Sus administradores y usuarios pueden aprovechar una variedad de formas de obtener soporte directo con los servicios de Microsoft 365. Su organización también se beneficiará de las actualizaciones transparentes del estado de mantenimiento del servicio, los Acuerdos de Nivel de Servicio para garantizar el tiempo de actividad de los servicios y el intercambio abierto de ideas y la colaboración para mejorar los servicios según la experiencia del usuario.

Al final de este módulo, debería ser capaz de hacer lo siguiente:

- Describir los beneficios de los servicios de Microsoft 365.
- Describir cómo crear una solicitud de soporte para los servicios de Microsoft 365.
- Describir los conceptos de los acuerdos de nivel de servicio (SLA), casos prácticos de los SLA, niveles de los SLA, funciones y responsabilidades.
- Determinar el estado de mantenimiento del servicio mediante el panel de Microsoft 365 o el panel de inquilino.
- Describir cómo se comunican las organizaciones con Microsoft mediante UserVoice.

## Explorar las opciones de soporte técnico de servicios para Microsoft 365

Los administradores y usuarios de su organización pueden tener dificultades para resolver los problemas por sí mismos. Es útil saber que los usuarios y administradores de su organización pueden recibir asistencia siempre que la necesiten.

## Opciones de soporte técnico

Cuando su organización usa los servicios de Microsoft 365, puede aprovechar las diferentes opciones de soporte técnico para resolver problemas. La opción de soporte técnico elegida para tratar un problema en particular depende de lo siguiente:

- La herramienta o servicio donde ha surgido el problema.
- El tipo de suscripción que usa su organización.
- El tipo de soporte técnico que necesita su organización.

Su organización puede obtener acceso al soporte técnico de las siguientes formas:

Tipo de soporte técnico	Descripción
<b>Soporte técnico de la comunidad</b>	Su organización puede aprovechar el soporte de la comunidad a través de <a href="#">Microsoft 365 Tech Community</a> , donde puede colaborar con otros y resolver problemas. Su organización también puede utilizar los formularios de soporte técnico de Microsoft 365 para hacer preguntas y resolver problemas con miembros de Microsoft y de la comunidad.
<b>Asistente de soporte de Microsoft 365</b>	Su organización puede usar el bot del Asistente de soporte en el Centro de administración de Microsoft 365 para encontrar rápidamente respuestas a preguntas relacionadas con el soporte.
<b>Soporte técnico en la Web, por correo electrónico y teléfono</b>	Su organización puede enviar problemas al soporte técnico de Microsoft para recibir soporte técnico, de facturación y de cuentas las 24 horas mediante el soporte por correo electrónico, chat en línea o telefónico.
<b>FastTrack</b>	Aquí, su organización está conectada con ingenieros, administradores de proyectos y recursos dedicados de Microsoft para ayudar a implementar los servicios de Microsoft 365 y resolver problemas sobre la marcha
<b>Soporte técnico Premier para Microsoft 365</b>	Microsoft ofrece servicios de soporte técnico Premier que su organización puede aprovechar para recibir soporte en el sitio, un administrador de cuentas técnico dedicado y acceso a servicios de asesoría.
<b>Soporte técnico a través de un socio de Microsoft</b>	Su organización puede obtener soporte directamente a través de un socio certificado de Microsoft 365. Por ejemplo, si su organización ha comprado una suscripción a Microsoft 365 a través de un proveedor de servicios en la nube de nivel 1, recibirá asistencia directa del CSP. El CSP actuará como el soporte de primera línea para todos los problemas y remitirá los problemas a Microsoft si no puede resolverlos.

## Explicar los acuerdos de nivel de servicio

Es fundamental que las organizaciones sepan que los servicios que utilizan son confiables y seguros. De esta manera, pueden tener la mente tranquila sobre los servicios que usan a diario. Con los servicios de Microsoft 365, su organización se beneficia de niveles de servicio garantizados, que se detallan en un acuerdo legal denominado Acuerdo de nivel de servicio.

## Acuerdo de Nivel de Servicios de Microsoft Online

Microsoft detalla su compromiso de proporcionar y mantener los niveles de servicio acordados para los servicios de Microsoft 365 a través de su [Acuerdo de nivel de servicios en línea de Microsoft](#). Por ejemplo, Microsoft garantiza un promedio de tiempo de actividad del 99,9 % durante un período de un mes para servicios como Microsoft Teams y Microsoft Stream.

Además del Acuerdo de nivel de servicios en línea de Microsoft, su organización también puede aprovechar los Acuerdos de nivel de servicio con su proveedor de servicios en la nube, que también aportará garantías específicas de servicio para los servicios de Microsoft 365. Los acuerdos de nivel de servicio variarán entre los proveedores de servicios en la nube.

El Acuerdo de Nivel de Servicio en línea de Microsoft presenta varios conceptos:

Concepto	Descripción
<b>Incidente</b>	Un conjunto de eventos o evento único que ocasiona tiempo de inactividad.
<b>Tiempo de inactividad</b>	La definición de tiempo de inactividad depende del servicio correspondiente. Por ejemplo, para Microsoft Teams, se considera tiempo de inactividad cualquier período de tiempo en el que los usuarios no puedan iniciar reuniones en línea, ver estadísticas de presencia o no puedan tener conversaciones de mensajería instantánea. Su tiempo de inactividad reduce el tiempo total de funcionamiento de sus servicios (su tiempo de actividad).
<b>Notificación</b>	Su organización envía una notificación al servicio de asistencia al cliente de Microsoft para obtener información sobre un incidente, el tiempo de inactividad experimentado, los usuarios afectados y compartir detalles sobre cómo ya intentó resolver el incidente. Microsoft es entonces responsable de procesar su notificación.
<b>Crédito de servicio</b>	Si Microsoft aprueba su notificación, su organización recibirá como Créditos de servicio un porcentaje de las tarifas mensuales totales que pagó durante el mes en el que experimentó el tiempo de inactividad.

Microsoft confía en su compromiso con los Niveles de servicio. El porcentaje de Crédito de servicio que puede recibir su organización está vinculado a su porcentaje de tiempo de actividad mensual:

<b>Porcentaje de tiempo de actividad mensual</b>	<b>Crédito de servicio</b>
< 99,9%	25%
< 99%	50%
<95 %	100 %

Por ejemplo, si el tiempo de inactividad ha dado lugar a un porcentaje de tiempo de actividad mensual inferior al 95 %, su organización podría recibir un Crédito de servicio del 100 %.

Su organización siempre debe revisar todos los Acuerdos de nivel de servicio y hacer preguntas, incluidas las siguientes:

- Si utiliza un proveedor de servicios en la nube, ¿cómo se determinan los niveles de servicio y si se logran o no?
- ¿Quién es responsable de los informes? ¿Cómo puede su organización acceder a los informes?
- ¿Existen excepciones en el acuerdo?
- ¿Qué dice el acuerdo sobre el mantenimiento programado e inesperado?
- ¿Qué dice el acuerdo sobre lo que sucede si su infraestructura falla debido a un ataque? ¿Qué ocurre con los desastres naturales y otras situaciones fuera de su control?
- ¿El acuerdo cubre errores de sistemas o servicios que no son de Microsoft?
- ¿Cuáles son los límites de la responsabilidad del proveedor de servicios en la nube en el acuerdo?

## Describir cómo realizar un seguimiento del estado de mantenimiento del servicio

Conocer el estado de los servicios de Microsoft 365 utilizados por una organización es fundamental. Por ejemplo, esto ayudará a su organización a saber cuándo se someterá a mantenimiento un servicio específico, de modo que su organización pueda preparar y minimizar el impacto en sus usuarios y sistemas.

### Ver el estado de mantenimiento de los servicios

Los administradores de su organización pueden usar el centro de administración de Microsoft 365 para ver el estado actual de los servicios y el espacio empresarial de Microsoft 365, e información sobre interrupciones en los servicios. Esto permite comprobar rápidamente el estado de los servicios para averiguar si está lidiando con un problema conocido que tiene una solución que se está implementando sin tener que dedicar tiempo a solucionar problemas o llamar al soporte técnico.

Los administradores pueden usar la página de estado del servicio del centro de administración de Microsoft 365 para ver el estado de mantenimiento de cada servicio:

Los administradores pueden notificar una incidencia si la organización tiene problemas con el servicio. Además, pueden ver detalles específicos de una incidencia para comprender el impacto que pueda tener en el servicio:

## Estado del servicio

Todos los servicios    Incidentes    Advertencias    Historial    Problemas notificados

Vea el estado de mantenimiento de todos los servicios disponibles en sus suscripciones ac ...

 Informar de un problema  Preferencias

Servicio	Estado
 Exchange Online	 Correcto
 Skype for Business	 Correcto
 Azure Information Protection	 Correcto
 Identity Service	 Correcto
 Microsoft 365 suite	 Correcto

## Realizar un seguimiento de los incidentes

Un incidente de servicio es cualquier evento que afecte a un servicio. Los incidentes pueden ocurrir debido a errores o problemas de hardware o software. Su organización puede configurar notificaciones para cualquier incidente nuevo o notificaciones para actualizaciones de cualquier incidente activo que pueda afectar a su organización. Microsoft proporcionará dos tipos distintos de notificaciones:

- **Tiempo de inactividad imprevisto:** Cuando un incidente ha provocado que un servicio no responda o no esté disponible.
- **Mantenimiento planeado:** El mantenimiento planeado es la actualización periódica del servicio Iniciado por Microsoft para las aplicaciones de infraestructura y software que ejecutan los servicios.

Microsoft también analiza los incidentes de servicio no planificados para usted a través de revisiones preliminares posteriores al incidente, donde recibirá una revisión preliminar en 48 horas de resolución del incidente y una revisión final en cinco días hábiles. Las revisiones finales posteriores al incidente incluirán la siguiente información:

- Cómo puede haber tenido un impacto para usted y para la experiencia del usuario.
- Un desglose de fecha y hora que detalla cuándo comenzó un incidente y cuándo se resolvió
- Análisis de causas originarias y acciones emprendidas para evitar el incidente en el futuro.

Su organización puede realizar un seguimiento del estado de mantenimiento de los servicios de diferentes maneras:

Herramienta	Descripción
<b>Aplicación de administración</b>	Sus administradores pueden utilizar la aplicación de administración para ver y mantenerse al día sobre la marcha respecto al estado de mantenimiento de los servicios.
<b>Microsoft System Center</b>	Sus administradores pueden ver todas las comunicaciones del servicio desde System Center si su organización tiene el paquete de administración de Office 365.
<b>API</b>	Su organización puede utilizar la API de comunicaciones de servicio de Office 365 para crear o utilizar herramientas que puedan conectarse y supervisar el estado del servicio en tiempo real en su lugar.

## Continuidad y disponibilidad

Los servicios de Microsoft se ejecutan en infraestructuras y sistemas altamente resistentes que ayudan a mantener la demanda y el rendimiento máximos del servicio. Esto permite que Microsoft se recupere rápidamente de eventos inesperados, como errores de hardware o de software o incluso catástrofes, como desastres naturales.

Por ejemplo, para proteger y garantizar que los datos de su organización estén siempre disponibles, Microsoft hace lo siguiente:

- **Redundancia de almacenamiento de datos:** Microsoft almacena sus datos a través de varios niveles de redundancia usando la replicación de datos y las capacidades de protección de datos seguras para permitir una rápida disponibilidad y recuperación de sus datos.
- **Supervisión de datos:** Sus bases de datos se supervisan para usted. Se supervisan sus datos, la pérdida de paquetes, las latencias de consultas, etc.

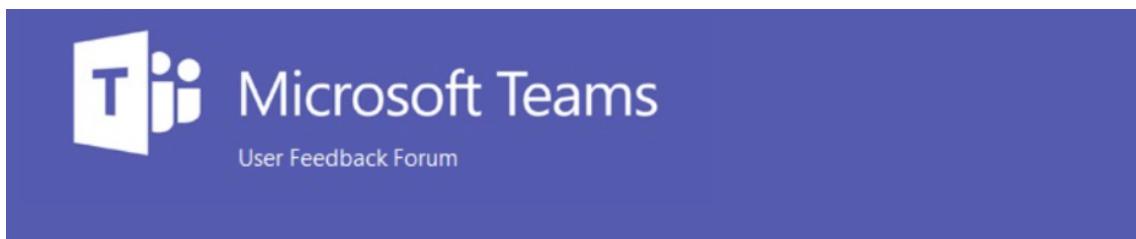
- **Medidas preventivas:** Microsoft realiza comprobaciones periódicas de coherencia de bases de datos, revisiones de registros de errores, etc.

## Comunicar y compartir ideas con UserVoice

Siempre hay margen de mejora y Microsoft se compromete a mejorar sus servicios. Los administradores y usuarios de su organización a menudo tienen un gran conocimiento de cómo se pueden mejorar partes y servicios específicos en función de sus experiencias diarias. Microsoft fomenta el intercambio de ideas para mejorar los servicios para todos.

Su organización puede enviar comentarios sobre el rendimiento de los servicios de Microsoft 365 y la experiencia del usuario. Microsoft se ha asociado con UserVoice para que usted y otros clientes de servicios de Microsoft 365 puedan compartir ideas sobre cómo creen que Microsoft puede mejorar los servicios y las experiencias. Es la mejor manera de asegurarse de que le escuchen. UserVoice le permite utilizar foros dedicados para cada servicio, publicar sus ideas y obtener respuestas de Microsoft sobre si ciertas funcionalidades y características ya están en curso o si pueden incluirse en actualizaciones futuras.

Por ejemplo, el sitio [UserVoice de Microsoft Teams](#) muestra que sus sugerencias y comentarios se supervisan y se presentan directamente al equipo de defensa del cliente dentro de Microsoft Teams Engineering:



### Welcome to the Microsoft Teams UserVoice!

[← Microsoft Teams UserVoice](#)

Hi there, you've reached the user feedback site for Microsoft Teams. It's managed by our Customer Advocacy Team inside Microsoft Teams Engineering led by Karuana Gatimu. Our entire team believes in representing your needs inside our engineering group and we appreciate the time you take to share them with us. Rest assured that a large team of dedicated people read and discuss your feedback!

Here's how to get your voice heard:

- 1 — VOTE for existing ideas (this will also subscribe you to the idea's status updates)
- 2 — SUBMIT new ideas (Please include only one suggestion per post. Duplicates are merged together.)
- 3 — RATE the product by clicking the little orange star on this page. This helps us understand our overall standing with users. It will collect your rating every six weeks.
- 4 — COMMENT in ideas' threads, which we check regularly

For official product and feature updates we recommend three things:

**Stay tuned here:** We update our work items monthly

**Read our Blog:** Official announcements come from our blog at <https://aka.ms/TeamsBlog>

**Review the Roadmap:** Our upcoming features can be seen within the Microsoft 365 roadmap site at <https://aka.ms/M365Roadmap>

Puede ver que el equipo ha aportado información sobre su blog de productos dedicado y acceso al plan de desarrollo para características futuras.

Los usuarios de sus organizaciones pueden compartir fácilmente sus ideas con el equipo y responderán de manera adecuada:

### How can we make Microsoft Teams better?

The screenshot shows a Microsoft UserVoice interface. At the top, there's a search bar with the placeholder "Enter your idea". Below it is a navigation bar with tabs: "Hot", "Top ideas" (which is selected and highlighted in blue), "New", and "Category". There are also buttons for "Status" and "My feedback".

A proposal card is displayed, featuring a large blue button on the left with the text "55,462 votes" and a "Vote" button below it. The title of the proposal is "Show video for all people in Video meeting". The description reads: "Currently when in a video chat it only shows the active video for the last 4 people that have spoken in the chat. On the bottom bar it shows icons for all those in the chat. If it could show small video for all those in the chat that have their cameras turned on it would be beneficial. Then everyone on the video conference can see the reactions of others, whether they were the last to speak or not." Below the description, it says: "This is a problem with most video chatting applications. Google Hangouts is the only one we have found that shows video... [more](#)".

At the bottom of the proposal card, there are links for "6288 comments · Meetings · Flag idea as inappropriate...".

Below the proposal card, a response from a user named "Alex (Teams Engineering, Microsoft Teams)" is shown, with the status "PARTIALLY DONE". The response says: "We are excited to announce the 3x3 video view has been rolled out 100% to for Windows and Mac Clients. If you aren't seeing 3x3 yet, please logout and log back in to the client." It continues: "We realize 3x3 is a start, but not good enough... as mentioned, we are continuing to work to include more videos during a meeting, as well as enabling support for mobile devices. Hence, the 'partially done' status." A link to documentation is provided: "Please see documentation here: <https://support.office.com/article/using-video-in-microsoft-teams-3647fc29-7b92-4c26-8c2d-8a596904cd4>".

Finally, the response ends with "Enjoy!"

Puede encontrar foros de UserVoice para todos los servicios de Microsoft 365, por ejemplo:

- [Microsoft Stream](#)
- SharePoint
- [Microsoft Teams](#)
- Yammer
- [Word](#)
- [Microsoft Planner](#)

Aproveche los sitios de UserVoice para contribuir directamente y ayudar a mejorar los servicios que Microsoft presta a su organización y a otros usuarios de todo el mundo.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Cómo puede su organización recibir soporte técnico en sus instalaciones por parte de Microsoft?

- A. A través del soporte técnico de la comunidad.
- B. A través del Asistente de soporte
- C. A través del soporte técnico Premier

¿Quién es el responsable de enviar una notificación para crédito de servicio?

- A. El proveedor de servicios en la nube
- B. Su organización
- C. Microsoft

¿Cuál es el mejor lugar para compartir ideas sobre cómo mejorar una característica de Microsoft Stream?

- A. Cree un comentario en la página de documentación de Microsoft para Microsoft Stream.
- B. Cree un vale de soporte para Microsoft Stream mediante el portal.
- C. Crear una publicación en el foro de comentarios de Microsoft Stream UserVoice.

## Seleccionar una implementación en la nube

### Introducción

En este módulo, verá cómo las implementaciones híbridas y solo en la nube requieren diferentes enfoques y cómo una organización aborda la migración de sistemas con versiones anteriores de Office, Windows y Office Server a Microsoft 365.

### Objetivos de aprendizaje

En este módulo, aprenderá lo siguiente:

- Consideraciones que debe tener en cuenta al seleccionar un servicio en la nube.
- Terminología asociada a la adopción de un servicio en la nube.
- La diferencia entre los modelos de migración solo en la nube e híbridos y cómo elegir entre ellos.
- Cuando es posible que una organización quiera mover los sistemas con sistemas operativos más antiguos y Microsoft Office directamente a Microsoft 365 en lugar de actualizar software antiguo.

## Requisitos previos

- Ninguno

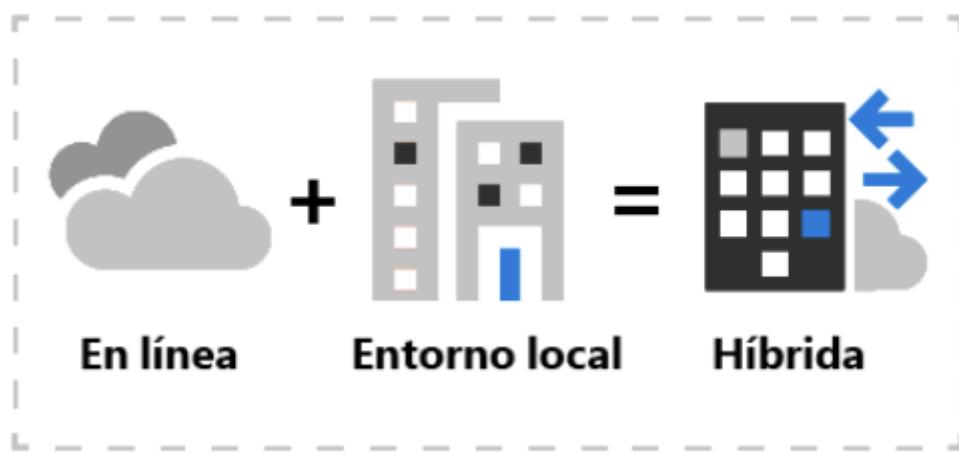
*Solo en la nube* describe una situación en la que los modelos de servicio que desea utilizar (software como servicio [SaaS], plataforma como servicio [PaaS] o infraestructura como servicio [IaaS]) se ejecutan estrictamente en la nube sin conexión con los sistemas locales existentes. Una de las ventajas de usar el modelo solo en la nube es que no tiene que preocuparse por la infraestructura en la que se ejecutan los servicios. La funcionalidad de back-end es invisible para los usuarios y el departamento de TI.

Para empresas más pequeñas como las startups o aquellas que no tienen recursos de TI internos o capital para comprar y mantener su propia infraestructura, el modelo solo en la nube, con su infraestructura administrada, puede ser una buena elección, porque no tiene que comprar o administrar la infraestructura, ya que el proveedor de servicios en la nube (CSP) se ocupa de ello. Pero tenga en cuenta que el modelo solo en la nube puede limitar el nivel de adaptación de sus servicios, ya que los usuarios y el personal de TI no pueden personalizar el SaaS y los servicios basados en PaaS que se ejecutan en la nube.

Si necesita poder personalizar sus servicios y su infraestructura, es posible que requiera un modelo híbrido.

## Modelo de nube híbrida

El modelo solo en la nube evita que tenga que crear y mantener su propia infraestructura. Pero, ¿qué sucede si su empresa ha invertido mucho en hardware local, sistemas de línea de negocio, aplicaciones personalizadas, etc.? ¿Necesita abandonar todos los recursos y personalizaciones para disfrutar de las ventajas de la informática en la nube? Aquí es donde surge el modelo híbrido.



*El sistema híbrido es una combinación de servicios en la nube con servicios locales para satisfacer sus necesidades de TI.*

Una migración de *nube híbrida* le permite mantener los recursos críticos locales mientras trabaja con los servicios en la nube. Conecta los recursos locales a la nube, lo que convierte eficazmente a los nuevos servicios en la nube en una extensión de su

infraestructura local. El modelo de nube híbrida le permite ampliar funciones o características que no están disponibles en sus sistemas locales existentes (como movilidad y productividad) a su infraestructura.

Entonces, ¿cómo elegir cuál es el mejor modelo para usted?

## ¿Qué modelo de nube deberían elegir las organizaciones?

Cuando las organizaciones consideran el uso de soluciones en la nube, normalmente se centran en tres áreas:

- Coste
- Seguridad, confiabilidad y cumplimiento
- Funcionalidad

Estas tres categorías no necesariamente tienen el mismo nivel de importancia. Es posible que algunas organizaciones pequeñas den más valor al coste de las funciones, mientras que las organizaciones más grandes y complejas podrían tener como principal prioridad la seguridad y el cumplimiento.

Tenga en cuenta lo siguiente cuando elija el modelo más adecuado para su organización:

- **Inversión reciente en hardware.** Hace un año, una organización de tamaño medio invirtió en hardware nuevo para su centro de datos local. Por tanto, es probable que la organización no esté interesada en hacer un cambio importante hacia la nube durante, al menos, uno o dos años. Las organizaciones en una situación similar probablemente optarán por un modelo de nube híbrida limitado que se centra en ofrecer funcionalidades que no existen en su centro de datos local.
- **Hardware y sistemas obsoletos.** En contraste con el ejemplo anterior, una organización que considere la renovación de un centro de datos local frente a las soluciones basadas en la nube puede tener una perspectiva muy diferente. Si el centro de datos tiene hardware antiguo y versiones de software no compatibles, es más probable que se considere la posibilidad de pasar a la nube. Y, si la oferta de la nube cumple con sus requisitos de seguridad y cumplimiento, el coste relativo y el tipo de modelo de costes (gastos operativos [costes diarios] frente a gastos de capital [coste único]) serán probablemente los factores decisivos.
- **Recursos internos de TI limitados.** El tamaño y la capacidad del departamento de TI son aspectos importantes al considerar la posibilidad de cambiar a una solución basada en la nube. A menudo, una organización con recursos de TI limitados se cambia más rápidamente a los servicios en la nube, ya que no es necesario realizar el mantenimiento de software y hardware de TI. Algunas organizaciones con grupos de TI de mayor tamaño también podrían considerar la nube como una forma de liberar sus recursos de TI para centrarse en funciones más estratégicas y, de esta manera, agregar valor a la organización.

- **Capital disponible.** Las soluciones SaaS basadas en la nube están diseñadas para ayudarle a evitar grandes inversiones de capital en TI, en vez de que pague para acceder a un software por un tiempo determinado con un modelo de suscripción. Si su organización tiene capital limitado para TI o tiene otras prioridades para la inversión de capital, el modelo de solo en la nube podría ser la mejor opción.

## Migración frente a coexistencia: planificación de su traslado a Microsoft 365

Cuando haya elegido el modelo de implementación adecuado para su organización, es hora de comenzar a planear la migración. Los dos modelos de servicio requieren enfoques diferentes: la *migración* para implementaciones solo en la nube y la *coexistencia* para implementaciones híbridas.

- La migración consiste en mover todo de un sistema antiguo a uno nuevo, con la intención de quitar eventualmente el sistema antiguo. En el contexto de la implementación en la nube, los datos y las aplicaciones se mueven de los recursos locales a la nube, hasta la infraestructura proporcionada por el CSP. Por ejemplo, si tiene un servicio de correo gratuito basado en Web y decide pasar al sistema de correo electrónico más seguro de Microsoft 365, tendrá que migrar todas las cuentas de correo electrónico de los usuarios desde el servicio en línea gratuito a Exchange online en Microsoft 365. Después de esa migración, los usuarios tienen acceso a su correo electrónico y a las bandejas de entrada antiguos mediante Outlook y los datos se almacenan en Exchange Online. no queda nada por usar en el antiguo sistema.
- Coexistencia significa que dos sistemas diferentes, uno de forma local y otro en la nube, se conectan y trabajan juntos al mismo tiempo (o *coexisten*) como un único servicio (como el correo electrónico). Por ejemplo, al contrario en el ejemplo anterior, ha elegido ir con un entorno híbrido en el que la suscripción a Microsoft 365 amplía sus servidores de Microsoft Exchange existentes. Debe establecer un vínculo entre el servidor local de Active Directory de Windows y el servidor de Exchange en sus complementos en línea de Azure Active Directory y Exchange Online.

## Consideraciones de migración

Cuando planee la migración, las siguientes consideraciones pueden ayudarle a guiar sus planes.

Qué necesita para migrar	Estrategias/consideraciones
Office 2013 o anterior a aplicaciones de Microsoft 365	Razones para actualizar a las licencias de Microsoft 365: - Después de abril de 2023, el acceso a los servicios de Office 365 (como Exchange Online, SharePoint) no será

	<p>compatible si utiliza Office 2013.</p> <ul style="list-style-type: none"> <li>- Office 2010 solo es compatible hasta 2020 y Office 2007 no es compatible en absoluto.</li> </ul>
Versiones de Office Server a servicios equivalentes de Office 365	<p>Razones para actualizar a los servicios de Office 365:</p> <ul style="list-style-type: none"> <li>- Los productos de Office Server 2013 y Office Server 2016 (como Exchange Server y SharePoint Server) no aprovechan los servicios y mejoras basados en la nube.</li> <li>- Algunos productos de Office Server 2010 tienen una fecha de fin de soporte especificada.</li> <li>- Los productos de Office Server 2007 ya no son compatibles. Para ayudar con la migración desde esta versión, contrate a un socio de Microsoft. A continuación, puede desplegar las nuevas funciones y procesos de trabajo a sus usuarios y retirar los servidores locales que ejecutan los productos de servidor de Office 2007 cuando ya no los necesite.</li> </ul>
Windows 7 y Windows 8.1 en sus dispositivos a Windows 10 Enterprise	Realice una actualización local a Windows 10 Enterprise.

Estas migraciones permiten que su organización se aproxime más al área de trabajo moderna: un entorno integrado y seguro que desbloquea el trabajo en equipo y la creatividad de su organización mediante Microsoft 365.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Luego seleccione **Comprobar sus respuestas**.

¿Para cuál de las siguientes organizaciones tiene más sentido una implementación híbrida?

- A. Un negocio establecido con un centro de datos que está adquiriendo un nuevo negocio.
- B. Una pequeña organización sin fines de lucro
- C. Un nuevo negocio

¿Cuál de las siguientes afirmaciones sobre migración frente a coexistencia es verdadera?

- A. La coexistencia es para implementaciones solo en la nube y la migración es para implementaciones híbridas.
- B. La migración es para implementaciones solo en la nube y la coexistencia es para implementaciones híbridas.
- C. La migración y la coexistencia funcionan para implementaciones solo en la nube.

# Module 4 - Demostrar conocimientos fundamentales de las funcionalidades de seguridad y cumplimiento de Microsoft 365

Describir los principios de seguridad y cumplimiento de Microsoft

## Introducción

A medida que se accede a más datos empresariales desde ubicaciones fuera de la red corporativa tradicional, la seguridad se ha convertido en una preocupación principal. Las organizaciones necesitan entender cómo pueden proteger mejor sus datos, independientemente de desde dónde se acceda a ellos y de si se encuentran en su red corporativa o en la nube.

Esta lección introduce algunos conceptos y metodologías importantes sobre seguridad. Aprenderá sobre el modelo de Confianza cero, el modelo de responsabilidad compartida, y la defensa en profundidad. También estudiará las amenazas de ciberseguridad más comunes. La lección introduce el cifrado y el hash como formas de proteger los datos. Por último, conocerá Cloud Adoption Framework para guiar la adopción de la nube.

Después de completar esta lección, podrá hacer lo siguiente:

- Describir los modelos de confianza cero y de responsabilidad compartida.
- Describir las amenazas de seguridad más comunes y las formas de protegerse mediante el modelo de seguridad de defensa en profundidad.
- Describir los conceptos de cifrado y hash.
- Describir Cloud Adoption Framework.

## Descripción de la metodología de Confianza cero

La Confianza cero asume que todo está en una red abierta y no confiable, incluso en el caso de los recursos tras los firewalls de la red corporativa. El modelo de Confianza cero funciona mediante el siguiente principio: “**no confíe en nadie y compruébelo todo**”.

La habilidad de los atacantes para eludir los controles de acceso convencionales está acabando con la ilusión de que las estrategias de seguridad tradicionales son suficientes. Si se deja de confiar en la integridad de la red corporativa, se reforzará la seguridad.

En la práctica, esto significa que ya no asumimos que una contraseña es suficiente para validar a un usuario, sino que agregamos la autenticación multifactor para aportar comprobaciones adicionales. En lugar de concederles acceso a todos los dispositivos de la red corporativa, los usuarios solo tendrán acceso a las aplicaciones o datos específicos que necesiten.

## Principios rectores de la Confianza cero

El modelo de Confianza cero cuenta con tres principios que rigen y sustentan la implementación de la seguridad. Son los siguientes: comprobar de forma explícita, acceso con privilegios mínimos y asumir la brecha.

- **Comprobar de forma explícita.** Autentique y autorice siempre en función de los puntos de datos disponibles, lo que incluye la identidad del usuario, la ubicación, el dispositivo, el servicio o la carga de trabajo, la clasificación de datos y las anomalías.
- **Acceso con privilegios mínimos.** Limite el acceso del usuario con acceso justo a tiempo y suficiente (JIT/JEA), directivas adaptables basadas en los riesgos y protección de datos para ayudar a proteger los datos y la productividad.
- **Asumir la vulneración.** Segmenta el acceso por red, usuario, dispositivos y aplicación. Proteja datos mediante el cifrado y utilice análisis para obtener visibilidad, detectar amenazas y mejorar su seguridad.

## Seis pilares fundamentales

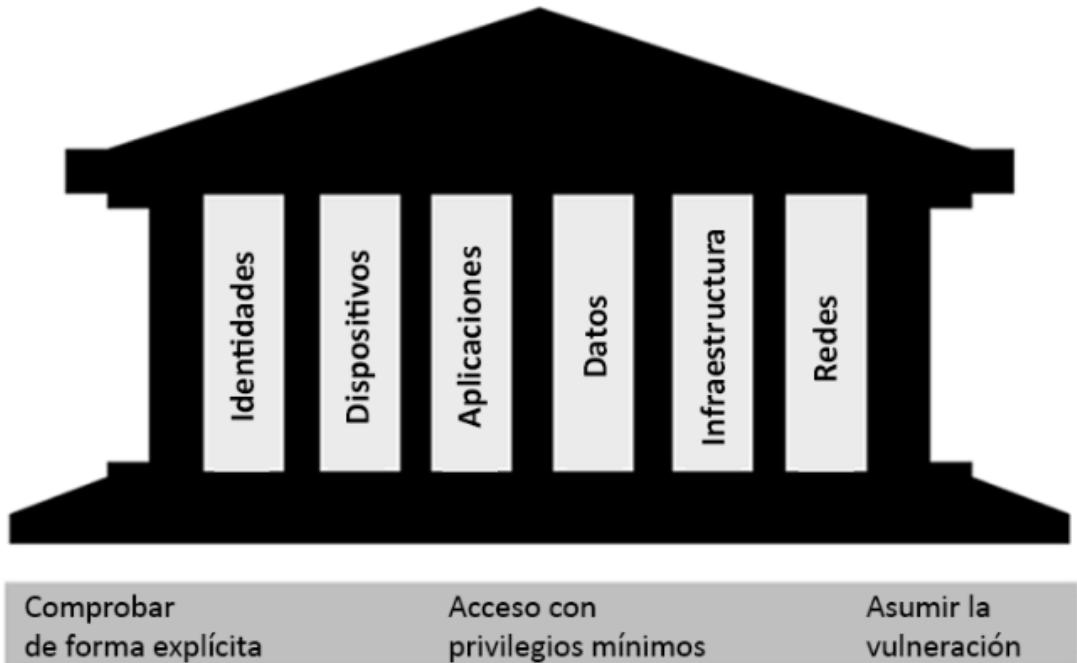
En el modelo de Confianza cero, todos los elementos trabajan juntos para ofrecer seguridad de un extremo a otro. Estos seis elementos son los pilares fundamentales del modelo de Confianza cero:

- Las **identidades** pueden ser usuarios, servicios o dispositivos. Cuando una identidad intenta acceder a un recurso, debe comprobarse con una autenticación segura, además de seguir los principios de acceso con privilegios mínimos.
- Los **dispositivos** crean una gran superficie expuesta a ataques a medida que los datos pasan de los dispositivos a cargas de trabajo locales y en la nube. Supervisar el estado y el cumplimiento de los dispositivos es un aspecto importante de la seguridad.
- Las **aplicaciones** son el modo en que se consumen los datos. Esto incluye el descubrimiento de todas las aplicaciones que se utilizan, llamadas a veces Shadow IT, ya que no todas se administran de forma centralizada. Este pilar incluye también la administración de permisos y accesos.
- Los **datos** deben clasificarse, etiquetarse y cifrarse según sus atributos. Los esfuerzos en el ámbito de la seguridad consisten, principalmente, en proteger datos y garantizar que se mantengan seguros cuando salgan de dispositivos, aplicaciones, infraestructuras y redes que la organización controle.
- **Infraestructuras:** representan un vector de amenaza, ya sean locales o se encuentren en la nube. Para mejorar la seguridad, evalúe la versión, la configuración y el acceso JIT, y utilice la telemetría para detectar ataques y anomalías. Esto le permitirá bloquear o marcar de forma automática comportamientos peligrosos y aplicar medidas de protección.

- **Redes:** deberían segmentarse; esto incluiría una microsegmentación más profunda en la red. Además, deberían emplearse la protección contra amenazas en tiempo real, el cifrado de un extremo a otro y análisis, y deberían supervisarse. [!div class="mx-imgBorder"]

**Metodología de cero**  
Highlight Note

**“No confiar en nadie, comprobar todo”**



## Describir el modelo de responsabilidad compartida

El *modelo de responsabilidad compartida* identifica qué tareas de seguridad administra el proveedor de la nube y qué tareas de seguridad administra usted como cliente.

En las organizaciones que ejecutan solo hardware y software locales, la organización es totalmente responsable de implementar la seguridad y el cumplimiento. En el caso de los servicios basados en la nube, el cliente y el proveedor de nube comparten esa responsabilidad.

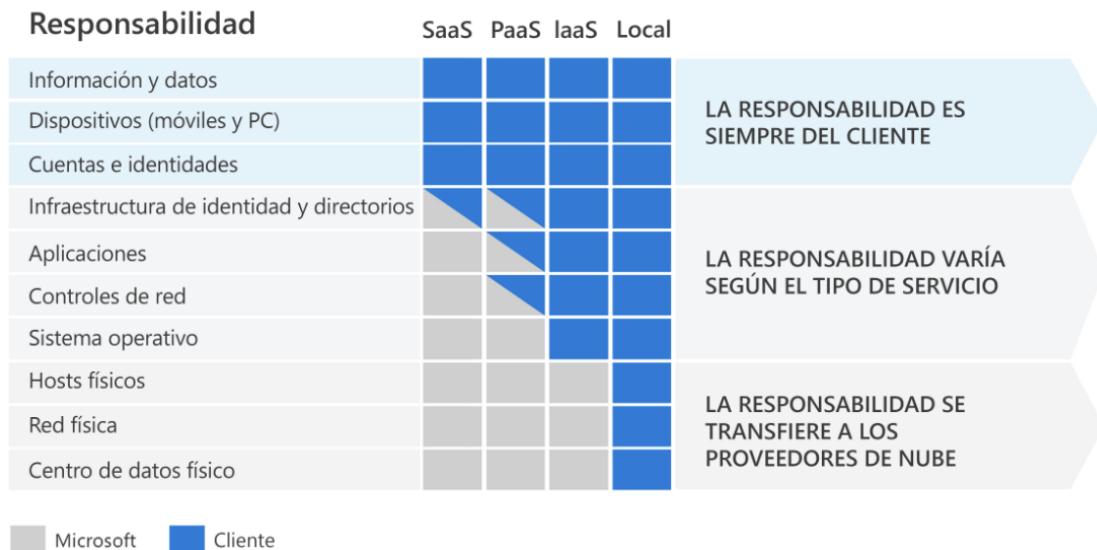
Las responsabilidades varían según dónde se aloje la carga de trabajo:

- Software como servicio (SaaS)
- Plataforma como servicio (PaaS)
- Infraestructura como servicio (IaaS)
- Centro de datos local (local)

El modelo de responsabilidad compartida identifica las responsabilidades de forma clara. Cuando las organizaciones mueven datos a la nube, algunas responsabilidades se transfieren al proveedor de nube y otras a la organización del cliente.

El siguiente diagrama ilustra las áreas de responsabilidad entre el cliente y el proveedor de nube según dónde se alojen los datos.

### Modelo de responsabilidad compartida



## Centros de datos locales

En un centro de datos local, usted es responsable de todo, desde la seguridad física hasta el cifrado de los datos confidenciales.

## Infraestructura como servicio (IaaS)

De todos los servicios en la nube, la IaaS es la que requiere mayor administración por parte del cliente de la nube. Con IaaS, utiliza la infraestructura informática del proveedor de nube. El cliente de la nube no se hace responsable de los componentes físicos, tales como los equipos y la red, ni de la seguridad física del centro de datos. Sin embargo, el cliente de la nube sí es responsable de los componentes de software, como los sistemas operativos, los controles de red, las aplicaciones y la protección de datos.

## Plataforma como servicio (PaaS)

PaaS proporciona un entorno para compilar, probar e implementar aplicaciones de software. El objetivo de PaaS es ayudarle a crear una aplicación rápidamente sin tener que administrar la infraestructura subyacente. Con PaaS, el proveedor de nube administra los sistemas operativos y el hardware, mientras que el cliente se responsabiliza de las aplicaciones y los datos.

## Software como servicio (SaaS)

El proveedor de nube hospeda y administra el SaaS para el cliente. Generalmente tiene licencia a través de una suscripción mensual o anual. Microsoft 365, Skype y Dynamics CRM Online son ejemplos de software de SaaS. SaaS requiere la menor cantidad de

administración de parte del cliente de la nube. El proveedor de nube es responsable de administrarlo todo, excepto los datos, los dispositivos, las cuentas y las identidades.

Para todos los tipos de implementación de nube, usted, como cliente de la nube, es el propietario de los datos y las identidades. Usted es el responsable de proteger la seguridad de sus datos, identidades y recursos locales.

En resumen, las responsabilidades que siempre pertenecen a la organización del cliente incluyen las siguientes:

- Información y datos
- Dispositivos (móviles y PC)
- Cuentas e identidades

La ventaja del modelo de responsabilidad compartida es que las organizaciones tienen claro cuáles son sus responsabilidades y cuáles las del proveedor de nube.

## Descripción de la defensa en profundidad

La defensa en profundidad protege mediante un enfoque por capas, en lugar de depender de un único perímetro. Una estrategia de defensa en profundidad usa una serie de mecanismos para ralentizar el avance de un ataque. Cada capa ofrece una protección tal que, si una de ellas se vulnera, una capa posterior evitará que el atacante obtenga acceso no autorizado a los datos.

Por ejemplo, las capas de seguridad pueden incluir lo siguiente:

- La seguridad **física**, como limitar el acceso al centro de datos al personal autorizado.
- Controles de seguridad de **identidad y acceso**, como la autenticación multifactor o el acceso basado en condiciones, para controlar el acceso a la infraestructura y el control de los cambios.
- La seguridad **perimetral** incluye la protección frente a ataques de denegación de servicio distribuido (DDoS) para filtrar los ataques a gran escala antes de que puedan producir una denegación de servicio para los usuarios.
- La seguridad de la **red**, como la segmentación de la red y los controles de acceso a la red, para limitar la comunicación entre los recursos.
- La capa de seguridad **informática**, como la protección del acceso a máquinas virtuales, tanto locales como en la nube, mediante el cierre de determinados puertos.
- La capa de seguridad de **aplicación** para garantizar que las aplicaciones sean seguras y estén libres de vulnerabilidades de seguridad.
- La capa de seguridad de **datos** incluye controles para administrar el acceso a los datos empresariales y de los clientes y el cifrado para protegerlos.



## Confidencialidad, integridad y disponibilidad (CIA)

La confidencialidad, integridad y disponibilidad, o CIA, es una manera de tener en cuenta las ventajas y desventajas de la seguridad. No se trata de un modelo de Microsoft, sino que es común a todos los profesionales de la seguridad.



La **confidencialidad** alude a la necesidad de mantener la confidencialidad de los datos confidenciales, como la información de los clientes, las contraseñas o los datos financieros. Puede cifrar los datos para que sean confidenciales, pero también deben ser confidenciales las claves de cifrado. La confidencialidad es la parte más visible de la seguridad; es evidente que es necesario mantener la confidencialidad de datos, claves, contraseñas y otros secretos.

La **integridad** hace referencia a que los datos o mensajes se mantengan correctos. Cuando envía un mensaje de correo electrónico, quiere asegurarse de que el mensaje que se recibe es el mismo que el que envía. Cuando almacena datos en una base de datos, quiere asegurarse de que los datos que recupera son los mismos que los que están almacenados. El cifrado de datos mantiene su confidencialidad, pero debe ser capaz de descifrarlos de forma que sean los mismos que antes del cifrado. La integridad se refiere a tener la confianza de que los datos no se han manipulado ni alterado.

La **disponibilidad** hace referencia a que los datos estén disponibles para quienes los necesiten. Es importante que la organización mantenga la seguridad de los datos de los clientes, pero estos también deben estar disponibles para los empleados que tratan con clientes. Aunque resulte más seguro almacenar los datos en un formato cifrado, los empleados necesitan acceso a esos datos cifrados.

Aunque todos los aspectos del modelo CIA son importantes, también representan las ventajas y desventajas que deben tenerse en cuenta.

## Descripción de las amenazas comunes

Existen diferentes tipos de amenazas de seguridad. El objetivo de algunos es robar datos, el de otros conseguir dinero y el de otros interrumpir las operaciones normales, como los ataques de denegación de servicio. En esta unidad se examinan algunas de estas amenazas comunes.

### Vulneración de datos

La vulneración de datos se da cuando se roban datos, incluidos datos personales. Los datos personales hacen referencia a cualquier información relacionada con una persona y que pueden utilizarse para identificarla directa o indirectamente.

Entre las amenazas de seguridad comunes que pueden resultar en una vulneración de datos se incluyen la suplantación de identidad (phishing), el phishing de objetivo definido, las estafas de soporte técnico, los ataques por inyección de código SQL y los ataques de malware diseñados para robar contraseñas o datos bancarios.

### Ataque por diccionario

El ataque por diccionario es un tipo de ataque de identidad en el que el hacker trata de robar la identidad del usuario mediante la prueba de una gran cantidad de contraseñas conocidas. Cada contraseña se prueba de forma automática con un nombre de usuario conocido. Los ataques por diccionario también se conocen como ataques por fuerza bruta.

### Ransomware

El término malware hace referencia a las aplicaciones y códigos malintencionados que pueden causar daños e interrumpir el uso normal de los dispositivos. El malware puede dar a los atacantes acceso no autorizado, lo que les permite usar los recursos de los sistemas, bloquear equipos y hacer chantaje.

El ransomware es un tipo de malware que cifra archivos y carpetas, lo que impide el acceso a archivos importantes. El ransomware se utiliza para extorsionar a las víctimas por dinero, generalmente en forma de criptomonedas, a cambio de la clave de descifrado.

Los ciberdelincuentes que distribuyen malware suelen estar motivados por el dinero, y lanzan los ataques mediante equipos infectados, de forma que consiguen credenciales bancarias, obtienen información que pueden vender, venden acceso a recursos informáticos o exigen dinero de las víctimas.

## Ataques de interrupción

Los ataques de denegación de servicio distribuido (DDoS) intentan agotar los recursos de una aplicación y hacen que esta no esté disponible para los usuarios legítimos. Los ataques DDoS pueden dirigirse a cualquier punto de conexión al que se pueda acceder públicamente a través de Internet.

Otras amenazas comunes son los mineros de criptomoneda, rootkits, troyanos, gusanos y kits para aprovecharse de las vulnerabilidades. Los rootkits interceptan y cambian los procesos estándar de los sistemas operativos. Cuando un rootkit infecta un dispositivo, no se debe confiar en la información que da el dispositivo sobre sí mismo.

Los troyanos son un tipo común de malware que no se pueden propagar por sí mismos. Eso quiere decir que se deben descargar de manera manual u otro malware debe descargarlos e instalarlos. A menudo, los troyanos utilizan los mismos nombres de archivo de aplicaciones legítimas y auténticas, por lo que es muy fácil descargar un troyano por accidente, creyendo que es de fiar.

Un gusano es un tipo de malware que se puede copiar a sí mismo y, generalmente, se propaga por una red aprovechando las vulnerabilidades de seguridad. Se puede propagar mediante archivos adjuntos en el correo electrónico, mensajes de texto, programas para compartir archivos, sitios de redes sociales, recursos compartidos de red, unidades extraíbles y vulnerabilidades del software.

Se aprovecha de las vulnerabilidades en el software. Una vulnerabilidad es un punto débil en su software que el malware utiliza para acceder su dispositivo. El malware aprovecha estas vulnerabilidades para burlar las medidas de seguridad del equipo e infectar el dispositivo.

Estos ejemplos son solo algunas de las amenazas más habituales. Esta es un área en constante evolución, por lo que continuamente surgen nuevas amenazas.

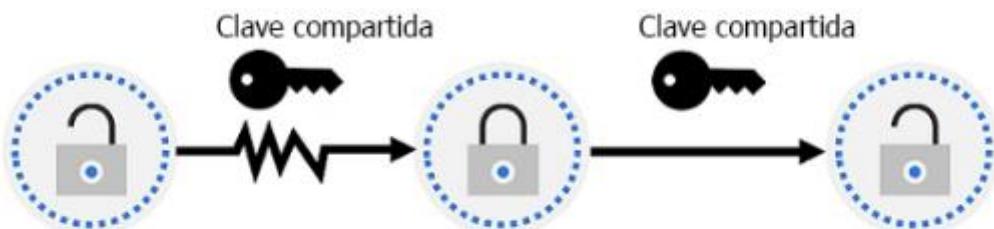
## Describir Cloud Adoption Framework

Una manera de mitigar las amenazas de ciberseguridad más comunes es cifrar datos confidenciales o valiosos. El cifrado es el proceso para hacer que los datos aparezcan ilegibles e inútiles para visores no autorizados. Para usar o leer datos cifrados, es necesario descifrarlos, lo que exige el uso de una clave secreta.

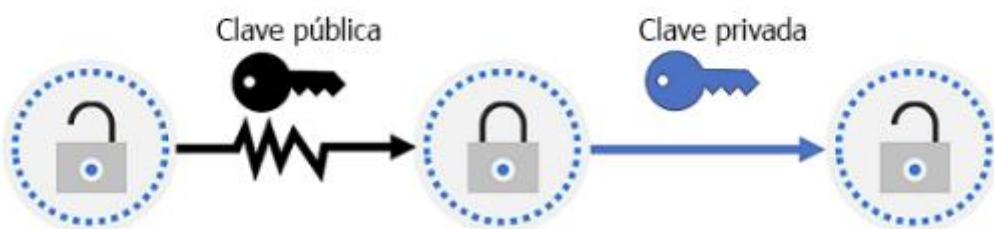
Hay dos tipos de cifrado de nivel superior: simétrico y asimétrico. El cifrado simétrico usa la misma clave para cifrar y descifrar los datos. El cifrado asimétrico usa un par de

claves pública y privada. Cualquiera de las dos puede cifrar datos, pero una sola clave no puede utilizarse para descifrar datos cifrados. Para descifrar se necesita otra clave del par. El cifrado asimétrico se utiliza, por ejemplo, para Seguridad de la capa de transporte (TLS), como en el protocolo HTTPS y la firma de datos. El cifrado puede proteger los datos en reposo o en tránsito.

## Cifrado simétrico



## Cifrado asimétrico



## Cifrado en reposo

Los datos en reposo son aquellos que se almacenan en un dispositivo físico, como un servidor. Se pueden almacenar en una base de datos o una cuenta de almacenamiento; pero, independientemente de dónde estén, el cifrado de datos en reposo asegura que los datos no puedan leerse sin las claves y los secretos necesarios para descifrarlos.

Si un atacante obtuviera una unidad de disco duro con datos cifrados, pero no tuviera acceso a las claves de cifrado, no podría leer los datos.

## Cifrado en tránsito

Los datos en tránsito son los que se están moviendo de una ubicación a otra, por ejemplo, por Internet o a través de una red privada. La transferencia segura se puede controlar mediante varias capas diferentes. Se puede hacer mediante el cifrado de los datos en la capa de aplicación antes de enviarlos a través de una red. HTTPS es un ejemplo de cifrado en tránsito.

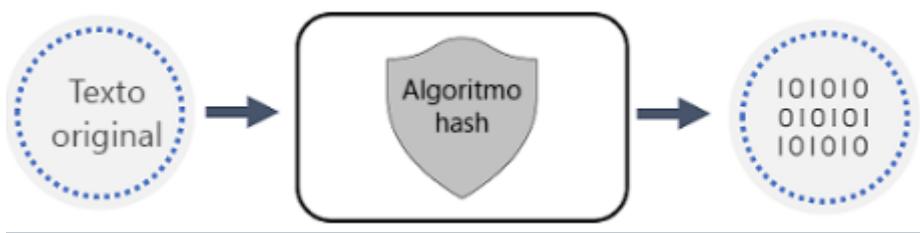
El cifrado de datos en tránsito le protege de observadores externos y da un mecanismo para transmitir datos, mientras limita el riesgo de exposición.

## Hash

El hash utiliza un algoritmo para convertir el texto original en un valor hash *único* de longitud fija. Cada vez que se realiza el hash del mismo texto con el mismo algoritmo, se produce el mismo valor hash. Dicho hash puede utilizarse entonces como un identificador único de sus datos asociados.

El hash es diferente al cifrado porque no usa claves y el valor hash no se descifra posteriormente al original.

El hash se usa para almacenar contraseñas. Cuando un usuario introduce su contraseña, el mismo algoritmo que creó el hash almacenado crea un hash de la contraseña introducida. Se compara con la versión hash almacenada de la contraseña. Si coinciden, el usuario ha introducido su contraseña de forma correcta. Esto es más seguro que almacenar contraseñas en texto plano, pero los hackers también conocen los algoritmos de hash. Como las funciones hash son deterministas (la misma entrada produce la misma salida), los hackers pueden usar ataques por diccionario por fuerza bruta mediante el hash de las contraseñas. Para cada hash que coincide, conocen la contraseña real. Para mitigar este riesgo, a menudo se “cifran con sal” las contraseñas. Se trata de agregar un valor aleatorio de longitud fija a la entrada de las funciones hash para crear hash únicos para cada entrada. Como los hackers no pueden conocer el valor del cifrado con sal, las contraseñas con hash son más seguras.



## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Luego seleccione **Comprobar sus respuestas**.

¿Cuál de las siguientes medidas podría implementar una organización como parte de la metodología de seguridad de defensa en profundidad?

- A. Autenticación multifactor para todos los usuarios.
- B. Situar todos sus servidores en una única ubicación física.
- C. Asegurarse de que no hay segmentación de su red corporativa.

Una organización ha implementado aplicaciones de Microsoft 365 para toda la plantilla. ¿Quién es el responsable de la seguridad de los datos personales de los empleados?

- A. La organización.
- B. Deben utilizar Azure Policy para orientarse en la transición a la nube.
- C. Deben utilizar Azure Cloud Succeed Framework

La organización de recursos humanos quiere asegurarse de que los datos almacenados de los empleados están cifrados. ¿Qué mecanismo de seguridad utilizarían?

- A. Cifrado en reposo.
- B. Hash.
- C. Cifrado en tránsito.

## Describir las capacidades de administración de identidad y acceso de Microsoft 365

### Introducción

El panorama de la seguridad evoluciona y se desarrolla continuamente para hacer frente a los crecientes desafíos que plantean sus usuarios y aquellos que buscan aprovechar las debilidades. Cualquier sistema de seguridad es tan bueno como el eslabón más débil de la cadena.

Proporcionar acceso a los recursos y datos es un requisito esencial para todas las organizaciones. Microsoft 365 le permite mejorar la experiencia de inicio de sesión de los usuarios manteniendo al mismo tiempo la seguridad; para ello, ofrece herramientas y servicios como Windows Hello, Multi-Factor Authentication y Azure Active Directory (Azure AD).

### Objetivos de aprendizaje

Al final de este módulo, debería ser capaz de:

- Comprender bien cómo funcionan los principios de Confianza cero de Microsoft y cómo puede aplicarlos en su organización
- Administrar identidades y accesos en Microsoft 365 con Azure Active Directory (Azure AD)
- Reducir el riesgo de brechas de seguridad con servicios sin contraseña como Windows Hello y Multi-factor Authentication (MFA)

## Describir el modelo de Confianza cero de Microsoft y los conceptos de administración de identidad y acceso

Las aplicaciones en la nube y la plantilla móvil redefinieron el perímetro de seguridad. Las aplicaciones y los datos corporativos se están moviendo de entornos locales a entornos híbridos y en la nube. Ahora, sus empleados pueden llevar sus propios dispositivos al trabajo y, cada vez más, tienen la capacidad de trabajar de manera remota desde sus propios hogares. Se obtiene acceso a los activos, recursos y datos de la organización fuera de la red corporativa y se comparten con colaboradores externos como socios y proveedores.

La ubicación física de la organización ya no define el perímetro de seguridad; ahora se extiende a todos los puntos de acceso que hospedan y almacenan recursos y servicios corporativos, o acceden a ellos. Por ejemplo, su personal esperará poder trabajar en el aeropuerto mientras espera un vuelo, pero en lugar de un equipo portátil, podrían usar su tableta o smartphone.

En la actualidad, las interacciones con los servicios y recursos de la compañía suelen eludir los modelos de seguridad locales basados en perímetro que dependen de firewalls de red y VPN. Las organizaciones que dependen únicamente de los firewalls y VPN locales carecen de la visibilidad, la integración de soluciones y la agilidad para ofrecer una cobertura de seguridad oportuna de un extremo a otro.

Hoy en día, las organizaciones necesitan un nuevo modelo de seguridad que se adapte de manera más eficaz a la complejidad del entorno moderno, adopte los recursos móviles y proteja a las personas, dispositivos, aplicaciones y datos dondequiera que estén ubicados.

## Administración de identidades y acceso

La administración de identidad y acceso es el principio fundamental sobre el que se basa la creación de un patrimonio digital seguro. Las credenciales que emita para sus usuarios los identificarán como pertenecientes a Microsoft 365 y, cuando se combinen con métodos de autenticación sólidos, como Multi-Factor Authentication, se tomarán como una prueba de que la persona que las utiliza es quien dice ser. Una vez que se establezca su identidad a través de la autenticación, Access Management se hace cargo, utilizando controles como el acceso condicional para evaluar más al usuario. Tiene en cuenta factores como la ubicación geográfica, el dispositivo desde el que se conectan, la aplicación que utilizaron para realizar la conexión y la hora del día. Todos estos factores se usan para decidir si el usuario está autorizado a acceder al recurso solicitado.

La identidad es la nueva defensa central y punto de control. Protege los datos de su organización en múltiples aplicaciones, ubicaciones y dispositivos, al tiempo que ofrece una estrategia integral de administración de identidad y acceso.

## Identidad híbrida

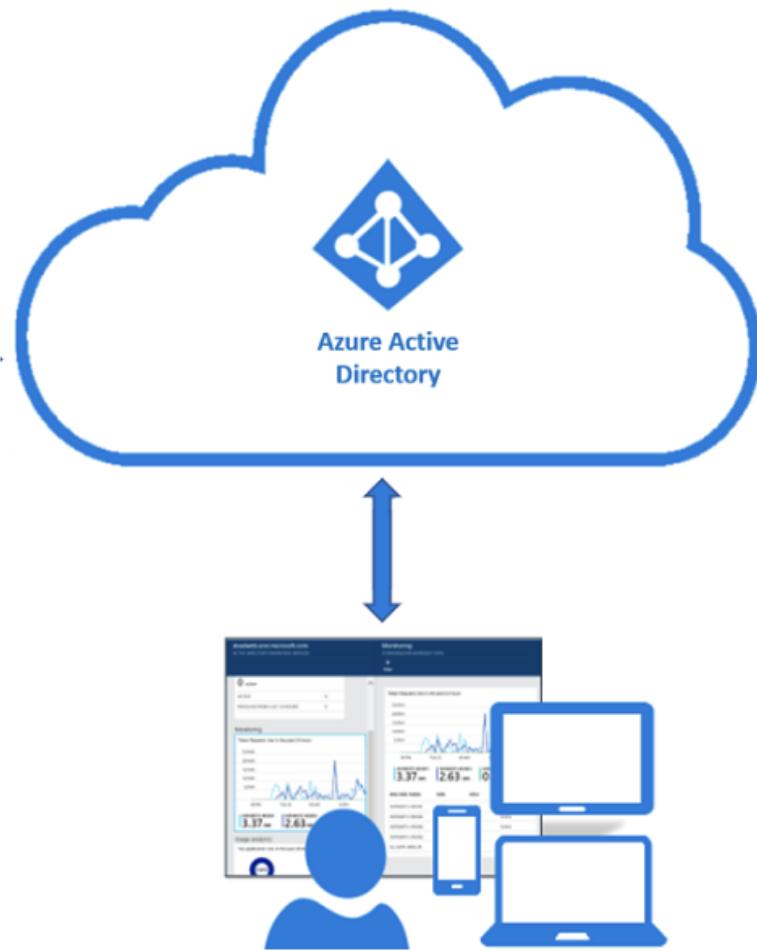
La identidad híbrida usa cuentas que se originan en un sistema de Dominio de Active Directory (AD DS) local y que se han transferido o copiado en el inquilino de Azure AD de una suscripción de Microsoft 365.

Cuando implementa la identidad híbrida, su AD DS local es la fuente autorizada para la información de la cuenta. El uso de Azure AD Connect sincroniza las cuentas de usuario en Azure AD. La integración de sus directorios locales con Azure AD hace que sus usuarios sean más productivos al aportar una identidad común para acceder tanto a los servicios en la nube como a los locales.

El inquilino de Azure AD tiene una copia de las cuentas de AD DS locales. En esta configuración, los usuarios que acceden a los servicios locales y basados en la nube pueden autenticarse con Azure AD.

## Identidad en la nube

Una identidad solo en la nube usa cuentas de usuario que solo existen en Azure AD. Aunque inicialmente la nube fue adoptada por organizaciones pequeñas que no tenían capacidades locales, cada vez más organizaciones empresariales ven las ventajas de mover todo su patrimonio digital, datos, aplicaciones y recursos a la nube.



En esta configuración, todos los usuarios usan sus cuentas de usuario y contraseñas de Azure AD para acceder a los servicios en la nube de Microsoft 365. Azure AD autentica las credenciales de usuario en función de sus contraseñas y cuentas de usuario almacenadas.

## Modelo de seguridad de Confianza cero

En lugar de creer que todo lo que hay detrás de un firewall corporativo es seguro, el modelo de Confianza cero da por hecho que toda solicitud es una brecha en la seguridad y comprueba cada solicitud como si se hubiera originado en una red no segura. Independientemente de dónde se origina la solicitud o de los recursos a los que accede, Confianza cero nos enseña a “desconfiar y comprobar siempre”.

En un modelo de Confianza cero, cada solicitud de acceso se autentica sólidamente, se autoriza según las restricciones de las directivas y se inspecciona en busca de anomalías antes de conceder el acceso. Para evitar una brecha, se usa todo, desde la identidad del usuario hasta el entorno de hospedaje de la aplicación. Se aplican los principios de acceso con privilegios mínimos y microsegmentación para minimizar el movimiento lateral. La microsegmentación es donde se crean zonas seguras para separar cargas de trabajo, cada una de las cuales se puede proteger. Por último, el análisis y la inteligencia sofisticados nos ayudan a identificar lo que sucedió, lo que se ha visto comprometido y cómo evitar que vuelva a ocurrir.

Principios básicos de la Confianza cero:

- **Comprobar de forma explícita.** Siempre autenticar y autorizar en función de todos los puntos de datos disponibles, lo que incluye la identidad del usuario, la ubicación, el estado del dispositivo, el servicio o la carga de trabajo, la clasificación de datos y las anomalías.
- **Usar el acceso con privilegios mínimos.** Limite el acceso de los usuarios con los tipos de acceso justo a tiempo y suficiente (JIT/JEA), directivas adaptables basadas en los riesgos y protección de datos para ayudar a proteger los datos y la productividad.
- **Asumir la brecha.** Minimice el radio del alcance de las brechas y evite el movimiento lateral mediante la segmentación del acceso por red, usuario, dispositivo y aplicación. Compruebe que todas las sesiones estén cifradas de extremo a extremo. Use los análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

La confianza cero hace que control de acceso deje de estar centrado en la red con sus controles de acceso inteligentes. Estos controles aprovechan las señales dinámicas de riesgo de dispositivos y usuarios, además de otra telemetría, para tomar decisiones de acceso más fundamentadas sobre los datos y recursos de una organización caso por caso.

Al bloquear el acceso a los recursos individuales mediante decisiones dinámicas de confianza, las organizaciones pueden aprovechar el control detallado para mejorar aún más la experiencia del usuario y las garantías de seguridad.

Un modelo de Confianza cero tiene tres aspectos.

- Necesita *señales* para informar las decisiones. Confianza cero considera muchas fuentes de señales, desde los sistemas de identidad hasta la administración de dispositivos y las herramientas de seguridad de los dispositivos, para crear conclusiones con contenido enriquecido que ayuden a tomar decisiones informadas.
- Directivas para tomar *decisiones* respecto al acceso. Cuando se solicita el acceso, se analiza la señal para tomar una decisión basada en directivas de acceso muy ajustadas, aportando un control de acceso granular y centrado en la organización.
- Capacidades de *cumplimiento* para implementar esas decisiones de forma efectiva. Las decisiones se aplican en todo el patrimonio digital, como el acceso de solo lectura a la aplicación SaaS o la reparación de contraseñas en peligro con un autoservicio de restablecimiento de contraseña.

# Administrar identidades y acceso en Microsoft 365 con Azure Active Directory

El perímetro de seguridad moderno ahora se extiende más allá de la red de una organización para incluir la identidad del usuario y del dispositivo. Las organizaciones pueden utilizar estas señales de identidad como parte de sus decisiones de control de acceso. Microsoft 365 usa el acceso condicional de Azure AD para administrar el acceso y el control a todos los activos y recursos de su organización.

El acceso condicional es la base del nuevo plano de control controlado por identidades. El acceso condicional abarca los servicios de Microsoft 365 como Intune, Microsoft 365 y Windows 10. Aporta acceso granular para mantener seguros sus datos corporativos, al mismo tiempo que permite a los usuarios hacer su mejor trabajo desde cualquier dispositivo y desde cualquier ubicación. El acceso condicional protege los datos confidenciales mediante la evaluación de usuarios, dispositivos, aplicaciones, ubicación y riesgo antes de otorgar acceso a los datos corporativos. Esto le permite garantizar que solo los usuarios y dispositivos aprobados puedan acceder a los recursos críticos de la empresa.



Las directivas del acceso condicional, en su forma más simple, son evaluaciones if-then. Si un usuario desea acceder a un recurso, entonces debe completar una acción, por ejemplo, un administrador de nómina desea acceder a la aplicación de nómina y debe realizar una autenticación multifactor para acceder a ella.

## Evaluación de la señal de acceso condicional

Cuando se recibe una solicitud de acceso, el acceso condicional usa la información de la señal del origen de la solicitud para obtener un contexto y determinar el riesgo general, que se usa para tomar una decisión fundamentada sobre si la solicitud de sesión debe concederse o revocarse. Las señales comunes que el acceso condicional puede tener en cuenta al tomar una decisión sobre una directiva incluyen:

Tipo de señal	Caso práctico
Pertenencia a un usuario o grupo	Las directivas pueden dirigirse a usuarios y grupos concretos, lo que aporta a los administradores un mayor control sobre el acceso.
Información sobre la ubicación de la IP	Las organizaciones pueden crear intervalos de direcciones IP de confianza que se pueden usar al tomar decisiones sobre directivas. Además, los administradores pueden optar por bloquear o permitir el tráfico de todo el intervalo de IP de un país o región.
Dispositivo	Al aplicar directivas de acceso condicional, se pueden usar usuarios con dispositivos de plataformas concretas o marcados con un estado concreto
Aplicación	Los usuarios que intentan acceder a aplicaciones específicas pueden activar diferentes directivas de acceso condicional.
Detección de riesgo calculado y en tiempo real	La integración de señales con Azure AD Identity Protection permite que las directivas de acceso condicional identifiquen un comportamiento de inicio de sesión peligroso. Luego, las directivas pueden obligar a los usuarios a realizar cambios de contraseña o a usar la autenticación multifactor para reducir su nivel de riesgo, o a bloquear su acceso hasta que algún administrador lleve a cabo una acción manual.
Microsoft Cloud App Security (MCAS)	Permite el control y la supervisión en tiempo real de las sesiones y el acceso a las aplicaciones de usuario, lo que aumenta la visibilidad y el control sobre el acceso y las actividades realizadas dentro del entorno de nube.

## Decisión de acceso condicional

Una vez que haya establecido que la solicitud de señal pasa la evaluación de riesgos, es hora de aplicar una directiva a la solicitud basada en la posición de seguridad y el apetito por el riesgo de su organización. El acceso condicional aporta un conjunto flexible de directivas que se pueden configurar para ofrecer un control granular sobre las circunstancias en las que los usuarios pueden acceder a los recursos de una organización.

El resultado de la decisión del acceso condicional será:

- **Bloquear acceso:** esta es la decisión más restrictiva.
- **Autorizar el acceso:** la decisión menos restrictiva. Todavía puede requerir una o más de las siguientes comprobaciones:
  - Autenticación multifactor
  - Que el dispositivo esté marcado como compatible
  - Dispositivo unido a Azure AD híbrido
  - Aplicación de cliente aprobada
  - Directiva de protección de la aplicación (versión preliminar)

## Cumplimiento a través de directivas aplicadas

Muchas organizaciones tienen [preocupaciones de acceso comunes con las que las directivas de acceso condicional pueden ayudar](#), como:

- Requerir autenticación multifactor para usuarios con roles administrativos
- Exigir autenticación multifactor para las tareas de administración de Azure
- Bloqueo de inicios de sesión para usuarios que intentan utilizar protocolos de autenticación heredados
- Exigir ubicaciones de confianza para el registro de Azure Multi-Factor Authentication
- Bloquear u otorgar acceso desde ubicaciones específicas
- Bloquear comportamientos de inicio de sesión de riesgo
- Requerir dispositivos administrados por la organización para aplicaciones específicas

## Licencias para identidad y acceso condicional

Azure AD es un servicio de identidad basado en la nube que centraliza la administración de identidades y accesos en entornos de nube y locales. Tiene soporte técnico integrado para la sincronización con su Active Directory local existente o se puede usar de forma independiente. Esto significa que todas sus aplicaciones, ya sean locales, en la nube o incluso móviles, pueden compartir las mismas credenciales.

Azure AD tiene varios niveles de servicio, incluidas las ediciones gratuitas de Microsoft 365 y Premium P1 y P2. Las ediciones Premium pueden requerir un coste adicional según sus niveles de suscripción a la nube de Microsoft. Azure AD Premium P1 se incluye como parte de los planes Microsoft 365 E5, E3 y F3. Azure AD Premium P2 se incluye con Microsoft 365 E5.

Estas son algunas de las características clave de cada nivel:

- Gratis: incluye inicio de sesión único, autoservicio de cambio de contraseña, autenticación multifactor, informes básicos de seguridad y uso y colaboración de empresa a empresa
- Microsoft 365 Apps: incluye todas las características gratuitas más identidad, autoservicio de restablecimiento de contraseña y reescritura del dispositivo (sincronización bidireccional entre directorios locales y Azure)
- Premium P1: incluye funciones gratuitas, de Office 365 y premium, como el acceso condicional basado en el grupo, la ubicación y el estado del dispositivo, Microsoft Cloud App Discovery, informes de uso y seguridad avanzados, administración avanzada de acceso de grupos e identidades híbridas
- Premium P2: contiene todo lo anterior más la protección de Azure Identity, que consta de directivas de acceso condicional basadas en riesgos, detección de cuentas de riesgo, investigaciones de eventos de riesgo y capacidades de gobernanza de identidad, incluida Privileged Identity Management (PIM)

# Reducir el riesgo de infracciones de seguridad con una autenticación segura

La mayoría de las vulneraciones de seguridad son el resultado del robo de identidad de un usuario por parte de los atacantes. A lo largo de los años, los atacantes se han vuelto cada vez más eficaces al vulnerar a terceros y al realizar sofisticados ataques de suplantación de identidad. Tan pronto como un atacante obtiene acceso a las cuentas de usuario, incluso las de bajo privilegio, les resultará relativamente fácil acceder a los recursos importantes de la empresa. La mayoría de las vulneraciones son el resultado de contraseñas en peligro.

Microsoft 365 y Azure AD pueden mejorar la postura de seguridad de una organización al adoptar métodos de autenticación más seguros, como MFA o medidas de autenticación sin contraseña.

## Autenticación segura

Proteger a sus usuarios le ayuda a protegerse contra las vulneraciones de seguridad. La calidad de las contraseñas de los usuarios es un aspecto importante. Las contraseñas son problemáticas. Se espera que los usuarios recuerden contraseñas complejas para cuentas distintas, tanto personales como de trabajo. Entre los problemas con las contraseñas se incluyen:

- Las contraseñas seguras pueden ser difíciles de recordar.
- Los usuarios a menudo reutilizan contraseñas en múltiples sitios diferentes.
- Las infracciones de seguridad del servidor pueden exponer credenciales de red simétricas (contraseñas).
- Las contraseñas están sujetas a ataques de reproducción.
- Los usuarios pueden exponer sus contraseñas por error debido a los ataques de suplantación de identidad.

Esto plantea un riesgo de seguridad significativo, ya que una vez que los malos actores obtienen contraseñas en peligro, pueden iniciar sesión en múltiples sitios. La mayoría de las vulneraciones de seguridad ocurren como resultado de contraseñas vulnerables.

Ahora exploremos cada uno de estos con más detalle.

## Utilice la autenticación multifactor para mejorar la seguridad de la autenticación

La autenticación multifactor (MFA) es un proceso mediante el cual se solicita al usuario durante el proceso de inicio de sesión una forma adicional de identificación, como usar un código emitido desde su teléfono o aportar un escaneo de huellas digitales.

Si solo usa una contraseña para autenticar a un usuario, deja un vector inseguro para el ataque. Si la contraseña es débil o ha sido expuesta en otro lugar, ¿es realmente el usuario el que inicia sesión con el nombre de usuario y la contraseña, o es un atacante? Cuando necesita una segunda forma de autenticación, la seguridad aumenta, ya que este factor adicional no es algo que sea fácil de obtener o duplicar para un atacante.

La autenticación multifactor de Azure exige dos o más de los siguientes métodos de autenticación:

- **Algo que sepa:** normalmente una contraseña
- **Algo que tenga:** por ejemplo, un dispositivo confiable que no se puede duplicar fácilmente, como un smartphone o una clave de hardware
- **Algo que sea:** datos biométricos como una huella digital o un escaneo facial

Azure Multi-Factor Authentication ayuda a proteger el acceso a los datos y las aplicaciones al tiempo que mantiene la simplicidad para los usuarios. Proporciona seguridad adicional, ya que requiere una segunda forma de autenticación y ofrece una autenticación sólida a través de una variedad de métodos de autenticación fáciles de usar. Los usuarios pueden ser desafiados o no por MFA en función de las decisiones de configuración que toma un administrador.

Sus aplicaciones o servicios no necesitan realizar ningún cambio para usar Azure Multi-Factor Authentication. Las solicitudes de verificación forman parte del evento de inicio de sesión de Azure AD, que solicita y procesa automáticamente el desafío de MFA cuando es necesario.

Cuando un usuario inicia sesión en una aplicación o servicio y recibe un mensaje de MFA, puede elegir una de sus formas registradas de verificación adicional. Un administrador podría requerir el registro de estos métodos de verificación de autenticación multifactor de Azure, o el usuario puede acceder a su página [Mi perfil](#) para editar o agregar métodos de verificación.

Las siguientes formas adicionales de verificación se pueden usar con Azure Multi-Factor Authentication:

- Aplicación de Microsoft Authenticator
- sms
- Llamada de voz
- Token de hardware OATH

## Usar la autenticación sin contraseña

Los usuarios quieren ser productivos y, a veces, sienten que las medidas de seguridad hacen mella en la productividad. La autenticación sin contraseña es una forma de autenticación multifactor que reemplaza una contraseña con una alternativa segura. El uso de métodos de autenticación sin contraseña evita la existencia de contraseñas vulnerables, ya que permite que los usuarios se autentiquen usando algo que tengan (como un teléfono inteligente o una insignia), algo que sean (datos biométricos) o algo que sepan (un PIN vinculado a un dispositivo específico).

Autenticación sin contraseña:

- Elimina la mayor vulnerabilidad del perímetro de seguridad: contraseñas débiles que se pueden robar.
- Utiliza el reconocimiento facial y la autenticación biométrica para garantizar que la persona correcta tenga el acceso adecuado.
- Vincula el PIN a su dispositivo para que un hacker tenga que robar ambos.

## Implementar la autenticación sin contraseña con Azure AD

Azure AD admite Fast Identity Online 2 (FIDO2). FIDO2 es un estándar abierto para la autenticación sin contraseña. FIDO2 permite a los usuarios y organizaciones aprovechar el estándar para iniciar sesión en sus recursos sin un nombre de usuario o contraseña utilizando una clave de seguridad externa o una clave de plataforma integrada en un dispositivo.

Los usuarios pueden acceder a un dispositivo según los controles de la organización y autenticarse según un PIN o datos biométricos y utilizando dispositivos como llaves de seguridad USB y tarjetas inteligentes, llaves o dispositivos portátiles con NFC. La autenticación sin contraseña con Azure AD se aplica a equipos compartidos y cuando un teléfono móvil no es una opción viable (como para el personal del servicio de asistencia, el quiosco multimedia público o el equipo del hospital).

Obtenga más información en [Llaves de seguridad FIDO2](#)

## Windows Hello

Windows 10 ahora ofrece una solución sin contraseña a través de la aplicación Windows Hello. Reemplaza las contraseñas con una sólida autenticación en dos fases en PC y dispositivos móviles. Esta autenticación consiste en un nuevo tipo de credencial de usuario que está vinculado a un dispositivo y utiliza un PIN o dato biométrico.

Windows Hello soluciona los siguientes problemas con las contraseñas:

- Las contraseñas seguras pueden ser difíciles de recordar y los usuarios suelen reutilizar las contraseñas en varios sitios.
- Las contraseñas están sujetas a ataques de reproducción.
- Los usuarios pueden exponer sus contraseñas sin darse cuenta debido a ataques de suplantación de identidad (phishing).

Windows Hello permite a los usuarios autenticarse en:

- Una cuenta de Microsoft, Active Directory o Microsoft Azure Active Directory (Azure AD).
- Servicios de un proveedor de identidades o servicios de un usuario de confianza que admiten la autenticación Fast ID Online (FIDO) v2.0

Después de una verificación inicial en dos pasos del usuario durante la inscripción, Windows Hello se configura en el dispositivo del usuario. El usuario proporciona el gesto para comprobar su identidad. A continuación, Windows usa Windows Hello para autenticar a los usuarios.

## Inicio de sesión biométrico

Windows Hello aporta autenticación biométrica confiable y totalmente integrada basada en el reconocimiento facial o la coincidencia de huellas dactilares. Windows Hello utiliza una combinación de software y cámaras especiales de infrarrojos (IR) para aumentar la precisión y protegerse contra la suplantación de identidad. En dispositivos

compatibles con Windows Hello, un sencillo gesto biométrico desbloquea las credenciales de los usuarios.

- **Reconocimiento facial.** Este tipo de reconocimiento biométrico utiliza cámaras especiales que ven con luz infrarroja, lo que les permite diferenciar de manera confiable entre una fotografía o un escaneo y una persona.
- **Reconocimiento de huellas dactilares.** Este tipo de reconocimiento biométrico utiliza un sensor de huellas dactilares capacitivo para escanear su huella dactilar. Los lectores de huellas dactilares han estado disponibles para equipos con Windows durante años, pero la generación actual de sensores es significativamente más confiable y menos propensa a errores.

Windows almacena todos los datos biométricos que se utilizan para implementar Windows Hello de forma segura solamente en el dispositivo local. Los datos biométricos no se trasladan y nunca se envían a dispositivos o servidores externos. Debido a que Windows Hello solo almacena datos de identificación biométrica en el dispositivo, no existe un único punto de recopilación que un atacante pueda comprometer para robar datos biométricos.

Windows Hello ayuda a proteger las identidades y las credenciales de usuario. Debido a que el usuario no especifica una contraseña (excepto durante el aprovisionamiento), ayuda a evitar ataques de phishing y por fuerza bruta.

## Microsoft Authenticator

Es posible que ya esté utilizando la aplicación Microsoft Authenticator como una opción cómoda de autenticación de múltiples factores además de una contraseña. También puede usar la aplicación Authenticator como una opción sin contraseña.



La aplicación Authenticator convierte cualquier teléfono iOS o Android en una credencial segura y sin contraseña. Los usuarios pueden iniciar sesión en cualquier plataforma o explorador al recibir una notificación en su smartphone, hacer coincidir un número que se muestra en la pantalla con el de su smartphone y, luego, usar sus datos biométricos (táctil o facial) o PIN para confirmar.

Antes de que los usuarios puedan iniciar sesión sin contraseña con Microsoft Authenticator, debe asegurarse de que:

- Sus cuentas están habilitadas para Azure MFA
- Inscriben sus dispositivos mediante Microsoft Intune o una solución de administración de puntos de conexión de terceros

**Importante:** La aplicación Microsoft Authenticator funciona con cualquier cuenta que utilice la verificación de dos factores y sea compatible con los estándares de contraseña de un solo uso (TOTP) basada en el tiempo.

La aplicación de Microsoft Authenticator se pueden usar de varias formas, entre las que se incluyen las siguientes:

- Responder a una solicitud de autenticación después de iniciar sesión con su nombre de usuario y contraseña.
- Iniciar sesión sin escribir una contraseña mediante su nombre de usuario, la aplicación autenticadora y su dispositivo móvil con su huella digital, cara o PIN.
- Como un generador de código para cualquier otra cuenta que admita aplicaciones autenticadoras.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Cuál es la teoría que hay detrás del modelo de seguridad de Confianza cero?

- A. Confiar en fuentes verificadas
- B. No confiar nunca, comprobar siempre
- C. Comprobar siempre, confiar una vez

¿Cuáles son los tres elementos clave del acceso condicional?

- A. Señal, decisión, cumplimiento
- B. Señal, decidir, responder
- C. Señal, decisión, responder

¿Dónde puede ir un usuario para administrar sus métodos de verificación?

- A. MyVerifications
- B. MyAccessMethod
- C. MyProfile

# Describir las funcionalidades de protección contra amenazas de Microsoft 365

## Introducción

Las amenazas son de diferentes tipos y tienen muchos objetivos, por lo que es importante comprender las capacidades de protección contra amenazas de Microsoft 365. Microsoft 365 aporta una cartera integral de protección contra amenazas que incluye múltiples herramientas y servicios, e implementa el aprendizaje automático y la inteligencia artificial para proteger su organización.

## Objetivos de aprendizaje

Al finalizar este módulo, habrá realizado lo siguiente:

- Identificar las amenazas comunes de seguridad.
- Descubrir cómo las empresas pueden prevenir, detectar y responder a las amenazas.
- Descubrir su posición de seguridad con Centro de seguridad y Puntuación de seguridad de Microsoft.
- Descubrir el valor que Intelligent Security Graph y Azure Sentinel ofrecen a las organizaciones seguras.

## Identificar las amenazas de seguridad más comunes

Actualmente, el personal de TI enfrenta muchas amenazas de seguridad. Ejemplos de amenazas de seguridad comunes incluyen amenazas a la seguridad de la red y amenazas a la seguridad de los datos.

Las amenazas de seguridad de red comunes incluyen las siguientes:

- Un ataque de espionaje (también conocido como rastreo de red), que ocurre cuando un hacker captura paquetes de red en tránsito en su red.
- Los ataques de denegación de servicio (DoS) limitan la función de una aplicación de red o hace que una aplicación o recurso de red no esté disponible.
- Ataques de escaneo de puertos, que pueden identificar aplicaciones específicas que se ejecutan en servidores.
- Los ataques de intermediario (MITM) son aquellos en los que un hacker usa un equipo para hacerse pasar por un anfitrión legítimo en la red con la que se comunican sus equipos

Las amenazas habituales de seguridad de datos son las siguientes:

- Usuarios no autorizados que acceden a información en un servidor.

- Usuarios no autorizados que acceden a datos desde una unidad extraíble extraviada o robada.
- Filtración de datos que deriva de un portátil perdido o robado, o un medio extraíble que contiene información de la compañía.
- La filtración de datos que surge de los correos electrónicos de los usuarios con contenido confidencial que se envía inadvertidamente a destinatarios no deseados.

Además, los usuarios experimentan amenazas ligadas a los productos básicos y ataques avanzados realizados por humanos. Las amenazas a las mercancías básicas incluyen operaciones de ransomware automatizadas y campañas de phishing a gran escala. Los ataques avanzados operados por humanos son más complejos y generalmente comienzan con exploits, ataques de fuerza bruta (adivinación de contraseñas) o correos electrónicos de phishing personalizados. Si bien muchos ataques avanzados también usan malware para infectar equipos de destino, a menudo usan componentes personalizados y herramientas del sistema indetectables. Recogen credenciales de red y permanecen persistentes en la recopilación de datos durante períodos prolongados.



## Descubrir cómo las empresas pueden prevenir y detectar amenazas y responder a ellas

### Protección contra amenazas de Microsoft

**Importante:** Microsoft 365 Defender es el nuevo nombre de la Protección contra amenazas de Microsoft. [Obtenga más información](#). Pronto actualizaremos nuestros productos y documentos, así que permanezca atento.

Microsoft 365 Defender es un conjunto de aplicaciones de defensa empresarial unificada previa y posteriormente a la vulneración que coordina de forma nativa la detección, la prevención, la investigación y contestación en los puntos de conexión, las identidades, los correos electrónicos y las aplicaciones para ofrecer protección integrada frente a ataques sofisticados. El conjunto de Microsoft 365 Defender protege lo siguiente:

- Identidades con Microsoft Defender for Identity (MSDI): MSDI usa señales de Active Directory para identificar, detectar e investigar amenazas avanzadas, identidades en peligro y acciones internas malintencionadas dirigidas a la organización.
- Puntos de conexión con Microsoft Defender para puntos de conexión (MSDE): MSDE es una plataforma de punto de conexión unificada para la protección preventiva, la detección posterior a la vulneración, la investigación automatizada y la contestación.
- Aplicaciones con Microsoft Cloud App Security (MCAS): MCAS es una solución completa de SaaS cruzada que ofrece visibilidad profunda, controles de datos seguros y protección contra amenazas mejorada para aplicaciones en la nube.
- Correo electrónico y colaboración con Microsoft Defender para Office 365 (MSDO): MSDO protege a su organización frente a amenazas malintencionadas al detectar, investigar y responder a ataques por correo electrónico y otros vectores de colaboración, como Microsoft Teams, SharePoint Online y OneDrive para la Empresa y clientes de Office.

## Microsoft Defender for Identity

[!IMPORTANTE] Microsoft Defender for Identity es el nuevo nombre para Azure Advanced Threat Protection. [Más información](#). Pronto actualizaremos nuestros productos y documentos, así que permanezca atento.

Microsoft Defender for Identity (MSDI) es una solución de seguridad basada en la nube que aprovecha las señales locales de Active Directory para identificar, detectar e investigar amenazas avanzadas, identidades en peligro y acciones internas malintencionadas dirigidas a su organización.

MSDI permite a los profesionales de la seguridad que luchan por detectar ataques avanzados en entornos híbridos:

- Supervisar las actividades y el comportamiento del usuario del perfil: MSDI supervisa y analiza las actividades del usuario y la información a través de la red, como los permisos y la pertenencia a grupos. De este modo, crea una línea base de comportamiento para cada usuario.
- Proteger las identidades de usuario y reducir la superficie expuesta a ataques: MSDI proporciona información muy útil sobre las configuraciones de identidad y las prácticas recomendadas de seguridad sugeridas. A través de informes de seguridad y análisis del perfil de usuario, MSDI permite reducir drásticamente la superficie expuesta a ataques de la organización, lo que dificulta que las credenciales de usuario se pongan en peligro y que se lleve a cabo un ataque.
- Identificar las actividades sospechosas y ataques avanzados a través de la cadena de destrucción de ciberataques: normalmente, los ataques se inician contra cualquier entidad accesible, como un usuario con pocos privilegios, y después se mueven lateralmente hasta que el atacante accede a recursos valiosos, como cuentas confidenciales, los administradores de dominio e

- información muy confidencial. MSDI identifica estas amenazas avanzadas en el origen a lo largo de toda la cadena de terminación del ciberataque.
- Investigar alertas y actividades de usuario: MSDI está diseñado para reducir las alertas sonoras innecesarias al proporcionar solo alertas de seguridad relevantes e importantes en una escala de tiempo simple y en tiempo real del ataque organizativo.

Para obtener más información, consulte [¿Qué es Microsoft Defender for Identity?](#)

## Microsoft Defender para punto de conexión

**Importante:** Microsoft Defender para punto de conexión es el nuevo nombre de la Protección contra amenazas avanzadas de Microsoft Defender.

><a href="https://www.microsoft.com/security/blog/?p=91813" title="" target="\_blank" data-generated="">>Más información</a>. Pronto actualizaremos nuestros productos y documentos, así que permanezca atento.>

Microsoft Defender para punto de conexión (MSDE) es una plataforma diseñada para ayudar a las redes empresariales a proteger los puntos de conexión mediante la prevención, detección, investigación y respuesta a amenazas avanzadas.



Microsoft Defender para punto de conexión (MSDE) tiene siete pilares:

- Administración de amenazas y vulnerabilidades: la administración de amenazas y vulnerabilidades es un enfoque basado en riesgos para la detección, la priorización y la corrección de las vulnerabilidades y configuraciones incorrectas de los puntos de conexión. Utiliza sensores en los dispositivos para evitar la necesidad de agentes o escaneos y prioriza las vulnerabilidades.
- Reducción de la superficie expuesta a ataques: la reducción de la superficie expuesta a ataques reduce los lugares donde su organización es vulnerable a ciberamenazas y ataques. Puede asegurarse de que solo las aplicaciones permitidas puedan ejecutarse y evitar que las aplicaciones accedan a ubicaciones peligrosas.
- Protección de nueva generación: Antivirus de Microsoft Defender es el componente de protección de nueva generación de MSDE. La protección de nueva generación combina el aprendizaje automático, el análisis de macrodatos, la investigación en profundidad de la resistencia a las amenazas y la infraestructura en la nube de Microsoft para proteger los dispositivos de su organización empresarial.

- Detección y respuesta de puntos de conexión: las capacidades de detección y respuesta de puntos de conexión de MSDE proporcionan detecciones de ataque avanzadas que son accionables y casi en tiempo real. Los analistas de seguridad pueden priorizar las alertas, obtener visibilidad del ámbito completo de una vulneración y tomar acciones de respuesta para corregir las amenazas.
- Investigación y corrección automatizadas: la función de investigación automatizada utiliza varios algoritmos de inspección y procesos utilizados por los analistas (como los cuadernos de estrategias) para examinar las alertas y tomar medidas de corrección inmediatas para resolver las infracciones. Esto reduce significativamente el volumen de alertas que deben investigarse de forma individual.
- Expertos en amenazas de Microsoft: Expertos en amenazas de Microsoft es un servicio de búsqueda de amenazas administrada que proporciona a los centros de operaciones de seguridad (SOC) una supervisión y un análisis de nivel experto para ayudarles a garantizar que no se pierdan las amenazas críticas en sus entornos únicos.
- Administración y API: además de aportar una solución de protección de punto de conexión completa y sólida por derecho propio, Microsoft Defender para punto de conexión aporta una serie de API para integrar con otras soluciones.

Para obtener más información, consulte [Integración de Microsoft Defender para punto de conexión](#).

## **Microsoft Cloud App Security**

Microsoft Cloud App Security (MCAS) es un agente de seguridad de acceso a la nube (CASB). Opera como un intermediario entre un usuario de nube y el proveedor de nube, para aportar una amplia visibilidad a sus servicios en la nube, control sobre el viaje de datos y análisis sofisticados para identificar y combatir las ciberamenazas en todos sus servicios en la nube.

MCAS se compila en un marco que aporta las siguientes capacidades:

- Detectar y controlar el uso de Shadow IT: Identifique las aplicaciones en la nube, IaaS y los servicios PaaS que utiliza su organización. Investigue patrones de uso, evaluar los niveles de riesgo y la preparación empresarial de más de 16 000 aplicaciones SaaS frente a más de 80 riesgos.
- Proteger la información confidencial en cualquier lugar de la nube: Comprender, clasificar y proteger la exposición de información confidencial en reposo. Aproveche las directivas listas para usar y los procesos automatizados para aplicar controles en tiempo real en todas sus aplicaciones en la nube.
- Protegerse frente a ciberamenazas y anomalías: Detecte comportamientos inusuales en las aplicaciones en la nube para identificar ransomware, usuarios comprometidos o aplicaciones fraudulentas, analice el uso de alto riesgo y corrija automáticamente para limitar el riesgo para su organización.
- Evaluar el cumplimiento de las aplicaciones en la nube: Evalúe si sus aplicaciones en la nube satisfacen los requisitos de cumplimiento relevantes, incluido el cumplimiento normativo y los estándares de la industria. Evite la

filtración de datos a aplicaciones no compatibles y limite el acceso a datos regulados.

Para obtener más información, lea [información general sobre Microsoft Cloud App Security](#).

## Microsoft Defender para Office 365

**Importante:** *Microsoft Defender para Office 365 es el nuevo nombre para la Protección contra amenazas avanzada de Office 365. [Obtenga más información](#). Pronto actualizaremos nuestros productos y documentos, así que permanezca atento.*

Microsoft Defender para Office 365 (MSDO) protege a su organización frente a amenazas malintencionadas imitando mensajes de correo electrónico, vínculos (direcciones URL) y herramientas de colaboración, entre las que se incluyen Microsoft Teams, SharePoint Online, OneDrive para la Empresa y otros clientes de Office. MSDO incluye:

- Directivas de la protección contra amenazas: Defina directivas de protección contra amenazas para establecer el nivel de protección adecuado para su organización.
- Informes: Vea informes en tiempo real para supervisar el rendimiento de MSDO en su organización.
- Investigación de amenazas y capacidades de respuesta: use las herramientas más avanzadas para investigar, entender, simular y evitar amenazas.
- Capacidades de Investigación y respuesta automatizadas: ahorre tiempo y esfuerzo investigando y mitigando amenazas.

Microsoft Defender para Office 365 está disponible en dos versiones, como se muestra en la siguiente tabla.

- El plan 1 de Microsoft Defender para Office 365 se incluye en Microsoft 365 Empresa Premium.
- El plan 2 de Microsoft Defender para Office 365 se incluye en Office 365 E5, Office 365 A5 y Microsoft 365 E5.
- El plan 1 y el plan 2 de Microsoft Defender para Office 365 están disponibles como complemento para determinadas suscripciones.

Microsoft Defender para Office 365 Plan 1	Microsoft Defender para Office 365 Plan 2
Capacidades de configuración, protección y detección:	Las capacidades de Microsoft Defender para Office 365 Plan 1 y la automatización, investigación, corrección y educación:
<a href="#">Datos adjuntos seguros</a> : comprueba el contenido malintencionado de los archivos adjuntos al correo electrónico.	<a href="#">Rastreadores de amenazas</a> : aporta la información más reciente sobre los problemas de ciberseguridad existentes.

<u>Vínculos seguros</u> : los vínculos se analizan en cada clic: los vínculos seguros siguen siendo accesibles y los malintencionados se bloquean dinámicamente.	<u>Explorador de amenazas</u> : un informe en tiempo real que permite identificar y analizar las amenazas recientes.
<u>ATP para SharePoint, OneDrive y Microsoft Teams</u> : protege a su organización cuando los usuarios colaboran y comparten archivos, al identificar y bloquear los archivos malintencionados en los sitios de equipo y las bibliotecas de documentos.	<u>Investigación y respuesta automatizadas</u> : incluye un conjunto de cuadernos de estrategias de seguridad que pueden lanzarse automáticamente, por ejemplo, cuando se activa una alerta, o manualmente.
<u>ATP de protección contra suplantación de identidad</u> : detecta los intentos de suplantación de sus usuarios y dominios internos o personalizados.	<u>Simulador de ataque</u> : le permite ejecutar escenarios de ataque realistas en su organización para identificar las vulnerabilidades.
<u>Detecciones en tiempo real</u> : un informe en tiempo real que permite identificar y analizar las amenazas recientes.	

Para saber más, consulte [Microsoft Defender para Office 365](#)

## Definir la posición de seguridad con el Centro de seguridad y la Puntuación de seguridad de Microsoft

### Microsoft 365 Defender

Administrar la seguridad de su negocio para protegerse contra un panorama de amenazas en constante evolución ofrece muchos desafíos. Es posible que tenga demasiadas soluciones de seguridad con varios lugares para configurar muchos controles y no sepa qué controles son los más efectivos y cuáles presentarán nuevos desafíos para sus recursos. Para los equipos de seguridad puede resultar difícil encontrar el equilibrio adecuado entre seguridad y productividad.

Entre en Microsoft 365 Defender, el nuevo hogar para supervisar y administrar la seguridad en todas sus identidades, datos, dispositivos, aplicaciones e infraestructura de Microsoft. Aquí puede ver el estado de seguridad de la organización, actuar para configurar dispositivos, usuarios y aplicaciones y, por último, ver alertas de actividad sospechosa. Microsoft 365 Defender está pensado específicamente para que los administradores de seguridad y los equipos de operaciones de seguridad administren y protejan mejor su organización.

Si desea obtener más información, lea [Microsoft 365 Defender introducción](#).

## Puntuación de seguridad de Microsoft

Puntuación de seguridad de Microsoft es una representación de la posición de seguridad de su organización y su oportunidad para mejorarla. Seguir las recomendaciones de Puntuación de seguridad puede proteger a su organización de las amenazas. Desde un panel centralizado en Microsoft 365 Defender, las organizaciones pueden supervisar y mejorar la seguridad de sus identidades, datos, aplicaciones, dispositivos e infraestructura de Microsoft 365.

La Puntuación de seguridad ayuda a las organizaciones a lo siguiente:

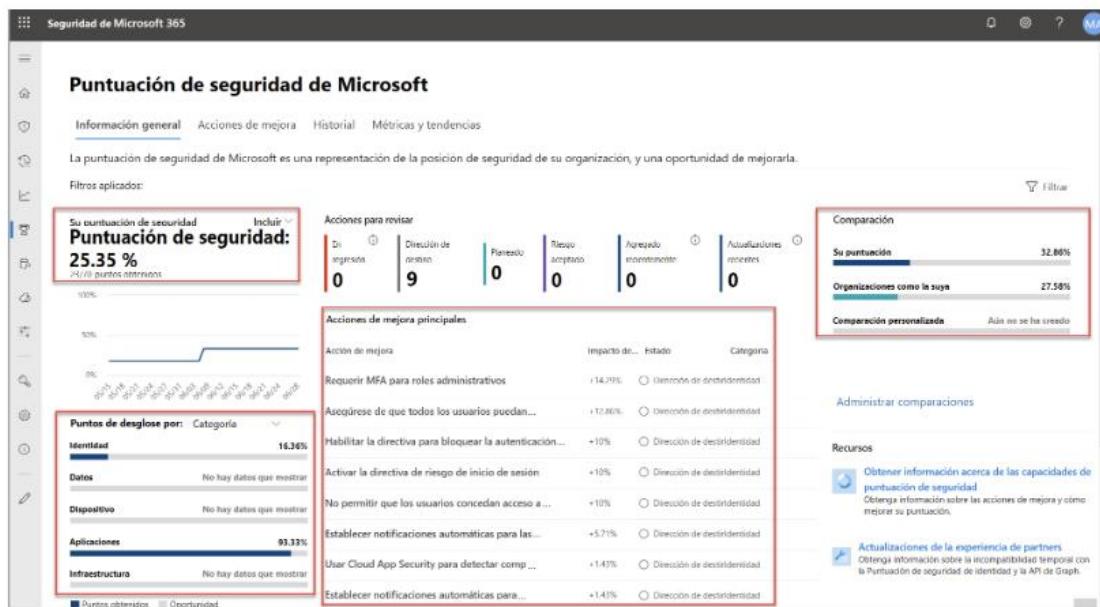
- Informar sobre el estado actual de la posición de seguridad de la organización.
- Mejorar su posición de seguridad al aportar detectabilidad, visibilidad, orientación y control.
- Comparar con puntos de referencia y establecer indicadores clave de rendimiento (KPI).

Los puntos de Puntuación de seguridad se clasifican en identidad, datos, dispositivo, aplicaciones e infraestructura. Se le otorgan puntos por configurar las características de seguridad recomendadas, realizar tareas relacionadas con la seguridad o llevar a cabo la acción de mejora con una aplicación o software de terceros, o una mitigación alternativa.

Puntuación de seguridad de Microsoft muestra el conjunto completo de posibles mejoras, independientemente de la licencia, para que pueda comprender las prácticas recomendadas de seguridad y mejorar su puntuación. Tenga en cuenta que la seguridad

siempre debe equilibrarse con la usabilidad y no todas las recomendaciones funcionarán para su entorno.

En la página de descripción general de Puntuación de seguridad de Microsoft, puede ver cómo se dividen los puntos entre las distintas categorías (identidad, datos, dispositivo, aplicaciones e infraestructura) y qué puntos están disponibles. En la página de descripción general también puede obtener una vista general de la puntuación total, la tendencia histórica de su puntuación de seguridad con comparaciones de referencia y acciones de mejora prioritarias que se pueden tomar para mejorar su puntuación.



Para más información, lea [Puntuación de seguridad de Microsoft](#).

## Tutorial

Siga los siguientes pasos para navegar por Microsoft 365 Defender, con un inquilino de prueba gratuita.

### Tarea 1: Iniciar sesión en el inquilino

1. Abra **Microsoft Edge**.
2. Navegue hasta <https://security.microsoft.com>.
3. Inicie sesión con las credenciales de la cuenta de administrador global de su espacio empresarial de Microsoft 365.

**Nota:** Si todavía no tiene una prueba gratuita de Microsoft 365, siga los pasos que se dan en [Qué es Microsoft 365](#).

### Tarea 2: Explorar Microsoft 365 Defender

1. Desde la página principal de Microsoft 365 Defender, localice la tarjeta de puntuación de seguridad. En la parte superior de la tarjeta, haga clic en **Puntuación de seguridad de Microsoft**.

2. En la parte superior de la página Puntuación de seguridad de Microsoft, observe las pestañas **Acciones de mejora, Historial y Métricas y tendencias**.
3. Seleccione **Acciones de mejora**. Consulte la información disponible para cada acción de mejora.
4. Seleccione una acción de mejora de la lista para ver la información disponible para cada acción.
5. Seleccione la tecla de dirección hacia atrás en el navegador para volver a la página Acciones de mejora.
6. Dedique un momento a explorar la información de las otras pestañas (Historial y Métricas y tendencias).
7. Seleccione **Inicio** en el panel de navegación izquierdo para volver a la página principal de Microsoft 365 Defender.
8. Busque la tarjeta etiquetada como **Usuarios de riesgo** y seleccione **Ver todos los usuarios**.
9. Le llevarán a la página **Usuarios de riesgo** en Microsoft Azure (se abrirá una nueva pestaña en su navegador). Si no tiene usuarios configurados en su espacio empresarial o no tiene usuarios de riesgo, no se enumerará ningún usuario.
10. En el navegador, vuelva a la pestaña **Inicio-Seguridad de Microsoft 365** para regresar a la página principal de Microsoft 365 Defender y explore algunas de las otras tarjetas.
11. Cuando haya terminado, cierre **Microsoft Edge**.

## Describir Microsoft Intelligent Security Graph y Azure Sentinel

Intelligent Security Graph usa análisis avanzados para vincular cantidades masivas de inteligencia sobre amenazas y datos de seguridad de Microsoft y socios para combatir las ciberamenazas. La información detallada de Intelligent Security Graph potencia la protección contra amenazas en tiempo real en los productos y servicios de Microsoft.

## API Microsoft Graph Security

Además de proporcionar información sobre amenazas de los productos y servicios de Microsoft, los datos de Intelligent Security Graph potencian la API Graph Security que los desarrolladores pueden aprovechar para crear servicios de seguridad inteligentes.

La API de Microsoft Graph Security es una API unificada que aporta una interfaz estándar y un esquema uniforme para integrar las alertas de seguridad y la inteligencia sobre amenazas de varias fuentes, enriquecer las alertas y los datos con información contextual y automatizar las operaciones de seguridad.

La API de seguridad forma parte de Microsoft Graph, que es una API REST unificada para integrar datos e inteligencia de Microsoft y servicios y productos de asociados. Con Microsoft Graph, los clientes y partners pueden crear rápidamente soluciones que se autentiquen una sola vez y usar una única llamada a la API para acceder a información de seguridad o bien actuar sobre ella desde diferentes soluciones de seguridad. Al explorar otras entidades de Microsoft Graph (como Azure Active Directory, Intune, etc.), puede descubrir información de seguridad y valor adicional.

Para obtener más información, consulte [Introducción a la API Microsoft Graph Security](#).

## Azure Sentinel

**Importante:** Microsoft 365 Defender es el nuevo nombre de la Protección contra amenazas de Microsoft.

Las soluciones de Microsoft 365 Defender se integran con Azure Sentinel. Microsoft Azure Sentinel es una solución de **administración de eventos de información de seguridad (SIEM) y respuesta automatizada de orquestación de seguridad (SOAR)** que es escalable y nativa de la nube. Azure Sentinel ofrece análisis de seguridad inteligente e inteligencia sobre amenazas en toda la empresa; aporta una única solución para la detección de alertas, la visibilidad de amenazas, la búsqueda proactiva y la respuesta a amenazas.

- Recopile datos a escala de nube de todos los usuarios, dispositivos, aplicaciones y de toda la infraestructura, tanto en el entorno local como en diversas nubes.
- Detecte amenazas que antes no se detectaban y reduzca los falsos positivos mediante el análisis y la inteligencia de amenazas sin precedentes de Microsoft.
- Investigue amenazas con inteligencia artificial y busque actividades sospechosas a escala, aprovechando el trabajo de ciberseguridad que ha llevado a cabo Microsoft durante años.
- Responda a los incidentes rápidamente con la orquestación y la automatización de tareas comunes integradas.



Azure Sentinel permite obtener una vista aérea de toda la empresa, lo que suaviza la tensión de ataques cada vez más sofisticados, volúmenes de alertas cada vez mayores y plazos de resolución largos. Visite [¿Qué es Azure Sentinel?](#) para más información.

# Prueba de conocimientos

**Importante:** Microsoft 365 Defender es el nuevo nombre de la Protección contra amenazas de Microsoft. Además:

- Microsoft Defender para punto de conexión es el nuevo nombre de la Protección contra amenazas avanzada de Microsoft Defender.
- Microsoft Defender para Office 365 es el nuevo nombre para la Protección contra amenazas avanzadas de Office 365.
- Microsoft Defender for Identity es el nuevo nombre para Azure Advanced Threat Protection.

[Obtenga más información](#). Pronto actualizaremos nuestros productos y documentos, así que permanezca atento

Elija la mejor respuesta para cada una de las siguientes preguntas. Despues, seleccione Comprobar las respuestas.

¿Cuál de las siguientes opciones es una solución de seguridad basada en la nube que identifica, detecta e investiga amenazas avanzadas, identidades en peligro y acciones internas malintencionadas dirigidas a su organización?

- A. Microsoft Defender para Office 365 (MSDO)
- B. Microsoft Defender for Identity (MSDI)
- C. Microsoft Cloud App Security

¿Qué categorías se incluyen en el desglose de la puntuación de seguridad?

- A. Identidad, datos, dispositivo, aplicaciones e infraestructura
- B. Malware y phishing
- C. Privacidad de datos y protección contra amenazas

¿Cuál de las siguientes opciones protege a su organización contra las amenazas malintencionadas que plantean los mensajes de correo electrónico, los vínculos (URL) y las herramientas de colaboración?

- A. Microsoft Defender para Office 365 (MSDO)
- B. Microsoft Defender for Identity (MSDI)
- C. Microsoft Cloud App Security

¿Cuál de los siguientes es un agente de seguridad de acceso a la nube que admite varios modos de implementación, incluida la recopilación de registros, los conectores de API y el proxy inverso?

- A. Microsoft Defender para Office 365 (MSDO)
- B. Microsoft Defender for Identity (MSDI)
- C. Microsoft Cloud App Security

# Describir las nuevas funcionalidades de seguridad en la nube de Microsoft 365

## Introducción

A medida que las empresas trasladan una mayor parte de sus cargas de trabajo a la nube, nunca ha sido más importante proteger los recursos en toda la nube. Microsoft, en su posición única como proveedor de nube y proveedor de seguridad, ha creado una seguridad integral en la nube para proteger cada capa de la nube en infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS), independientemente de la nube o las aplicaciones en la nube que use.

En este módulo, podrá hacer lo siguiente:

- Explorar el marco de seguridad de aplicaciones en la nube.
- Descubrir las capacidades de Microsoft Cloud Application Security (MCAS).
- Explorar cómo Microsoft Cloud App Security se integra con las capacidades de protección contra amenazas y seguridad de Microsoft.

## Tome el control de su entorno en la nube con Microsoft Cloud App Security

Pasar a la nube aumenta la flexibilidad para los empleados y el departamento de TI por igual. Sin embargo, también presenta nuevos desafíos y complejidades para mantener la seguridad de su organización. Para obtener el máximo beneficio de las aplicaciones y servicios en la nube, un equipo de TI debe encontrar el equilibrio adecuado entre el acceso de soporte y, al mismo tiempo, mantener el control para proteger los datos críticos. Es crucial obtener visibilidad y control de los datos en las aplicaciones en la nube, dado el número creciente de ataques de ciberseguridad y los requisitos de cumplimiento de las regulaciones clave.

Microsoft Cloud App Security (MCAS) es un servicio de suscripción basado en el usuario que proporciona una gran visibilidad y control sobre el recorrido de los datos y análisis sofisticados para identificar y combatir las ciberamenazas en todos sus servicios en la nube. MCAS, que funciona con integraciones nativas con soluciones de identidad y seguridad líderes en la industria, que incluyen Azure Active Directory, Intune y Azure Information Protection, identifica y combate estas amenazas operando como intermediario, o agente, entre un usuario de la nube y el proveedor de nube.

MCAS es un **agente de seguridad de acceso a la nube** (CASB). Los CASB son soluciones de seguridad basadas en la nube que proporcionan una capa de seguridad para permitir la supervisión y el control de las actividades y la información en las aplicaciones SaaS en la nube públicas y personalizadas y los servicios IaaS. Los CASB se dividen en cuatro áreas de capacidad clave, que incluyen Shadow IT Discovery, protección de la información, protección contra amenazas y cumplimiento. Estas áreas de capacidad representan el marco sobre el que se construye MCAS.

MCAS y el marco de Cloud App Security:

- **Detectar y controlar el uso de Shadow IT:** Identifique las aplicaciones en la nube y los servicios IaaS y PaaS que utiliza su organización, algunos de los cuales pueden ni siquiera ser conocidos o controlados por el departamento de TI. Investigue patrones de uso, evaluar los niveles de riesgo y la preparación empresarial de más de 16 000 aplicaciones SaaS frente a más de 80 riesgos.
- **Proteger la información confidencial en cualquier lugar de la nube:** Comprender, clasificar y proteger la exposición de información confidencial en reposo. Aproveche las directivas listas para usar y los procesos automatizados para aplicar controles en tiempo real en todas sus aplicaciones en la nube.
- **Protegerse frente a ciberamenazas y anomalías:** Detecte comportamientos inusuales en las aplicaciones en la nube para identificar ransomware, usuarios comprometidos o aplicaciones fraudulentas, analice el uso de alto riesgo y corrija automáticamente para limitar el riesgo para su organización.
- **Evalúe el cumplimiento de las aplicaciones en la nube:** Evalúe si sus aplicaciones en la nube satisfacen los requisitos de cumplimiento relevantes, incluido el cumplimiento normativo y los estándares de la industria. Evite la filtración de datos a aplicaciones no compatibles y limite el acceso a datos regulados.

Para más información, consulte la [Guía interactiva: Descubra, proteja y controle sus aplicaciones con Microsoft Cloud App Security](#)

## Explore las capacidades de integración de Microsoft Cloud App Security

### Integración con Microsoft Defender para punto de conexión

**Importante:** Microsoft Defender para punto de conexión es el nuevo nombre de la Protección contra amenazas avanzada de Microsoft Defender.

[Más información](#) Pronto actualizaremos nuestros productos y documentos, así que permanezca atento.

Microsoft Cloud App Security (MCAS) se integra de forma única con Microsoft Defender para punto de conexión (MSDE), una plataforma unificada de seguridad de punto de conexión para protección, detección, investigación y respuesta para mejorar la detección de Shadow IT en su organización.

En este vídeo verá como Microsoft Cloud App Security se integra con Microsoft Defender para punto de conexión.

Para obtener más información, consulte [Microsoft Defender para punto de conexión](#).

### Integración con Azure AD y Azure Information Protection

En el área de trabajo moderna, es fundamental permitir que los usuarios trabajen desde cualquier ubicación y cualquier dispositivo, y concederles acceso a las aplicaciones en la nube. Las crecientes necesidades de colaboración requieren que los datos se compartan con socios y colaboradores externos. Al mismo tiempo, las empresas deben proteger los datos y recursos de su organización.

MCAS permite a las empresas identificar datos confidenciales en las aplicaciones en la nube, supervisar cuando se comparten con entornos de riesgo y tomar las acciones de gobernanza necesarias mediante la clasificación, etiquetado y protección de los datos nuevos y existentes en su entorno.

MCAS se integra con Azure AD y Azure Information Protection para ofrecer estas capacidades en una experiencia holística e integrada. Otorga a las empresas un nivel de granularidad a la hora de definir qué significa el riesgo para su organización, y luego les ofrece control y visibilidad de cualquier sesión de usuario que coincida con esa definición. Por ejemplo, si un empleado intenta acceder a archivos confidenciales desde un equipo personal en una red pública, es posible configurar el sistema para bloquear la descarga por completo o para permitirla. Con Azure Information Protection, el sistema se puede configurar para etiquetar y proteger automáticamente el archivo en tiempo real. Permite a la empresa evitar que la información confidencial se filtre fuera de la organización.



## MCAS e inteligencia avanzada sobre amenazas

Moverse a la nube presenta un nuevo vector de amenaza para las organizaciones. Los ataques pueden introducir ransomware, las cuentas de usuario en peligro realizan actividades malintencionadas y las aplicaciones basadas en OAuth con exceso de privilegios pueden obtener acceso a datos confidenciales o cuentas con privilegios. Los negocios pueden acelerar la adopción segura de aplicaciones en la nube y limitar el impacto en su organización aprovechando análisis de comportamiento sofisticados.

- MCAS aprovecha Intelligent Security Graph con sus miles de millones de señales de seguridad para potenciar su detección de amenazas.
- MCAS se integra con la Puntuación de seguridad para dar visibilidad sobre su posición de seguridad de Microsoft y proporciona una descripción general de las funciones de seguridad disponibles para reducir el riesgo.

MCAS se integra en la puntuación general y le ayuda a proteger su entorno de aplicaciones en la nube.

Para más información, consulte la [Guía interactiva: Detectar amenazas y administrar alertas con Microsoft Cloud App Security](#)

## Integración de MCAS con Power Automate

Power Automate es un servicio que le ayuda a crear un flujo de trabajo automatizado entre sus aplicaciones y servicios favoritos para sincronizar archivos, recibir avisos, recopilar datos y más. Microsoft Cloud App Security se integra con Power Automate para aportar cuadernos de estrategias sobre automatización y orquestación de alertas personalizadas que ayudan a automatizar y orquestar una respuesta, si se activan alertas específicas. Al crear un cuaderno de estrategias en Power Automate con el conector Cloud App Security, su empresa puede crear flujos de trabajo para habilitar opciones de gobierno personalizadas para sus directivas.

Para obtener más información, lea la [Documentación de Power Automate](#).

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Luego seleccione **Comprobar sus respuestas**.

¿Cuáles son las cuatro áreas clave de capacidad de los CASB?

- A. Identidad, confidencialidad, autenticación e integridad de los datos
- B. Shadow IT Discovery, protección de la información, protección contra amenazas y cumplimiento
- C. Red, almacenamiento, aplicaciones y administración

¿Qué servicio se integra con MCAS para descubrir la utilización de aplicaciones en la nube más allá de la red corporativa?

- A. Microsoft Defender para punto de conexión
- B. Power Automate
- C. Azure AD y Azure Information Protection

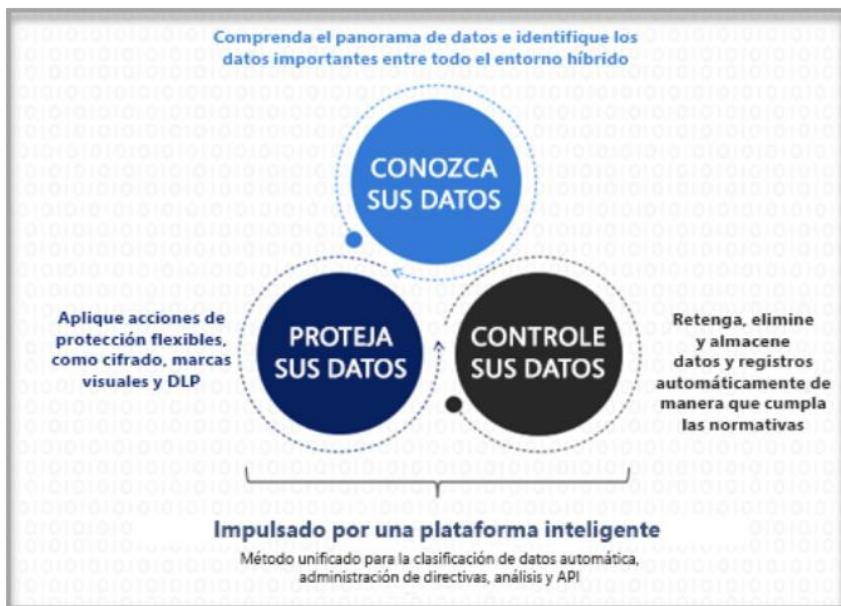
# Describir las funcionalidades de gobernanza y protección de la información de Microsoft 365

## Introducción

Las organizaciones ven que proteger y controlar datos importantes es más desafiante que nunca. Hay varias razones para ello, entre las que se incluyen:

- El crecimiento exponencial de los datos.
- La difuminación de los límites organizativos tradicionales.
- La aceleración de la colaboración entre trabajadores.
- La evolución de los requisitos de cumplimiento.
- Los datos se crean, almacenan y comparten en muchas ubicaciones, incluidos dispositivos, aplicaciones, servicios en la nube y el entorno local.

El conjunto completo de soluciones de Microsoft le permite **conocer, proteger y gobernar sus datos**. La solución de Microsoft es eficaz durante todo el ciclo de vida de los datos, dondequiera que residan y viajen. Este enfoque es posible gracias a una plataforma inteligente que aporta un enfoque unificado para la clasificación automática de datos, la administración de directivas, los análisis y las API.



## Objetivos de aprendizaje

Al final de este módulo, debería ser capaz de hacer lo siguiente:

- Descubrir e identificar información en su entorno
- Comprender cómo puede proteger los datos de su empresa.
- Comprenda cómo puede controlar los datos de su empresa.

# Detectar e identificar información importante en su entorno

Hoy en día, los datos se almacenan en más lugares y en más dispositivos que nunca. Para poder proteger los datos confidenciales, debe conocerlos.

Conocer sus datos consiste en poder descubrir e identificar información importante de todo su entorno. También es posible que deba aclarar qué datos se consideran datos confidenciales en su organización, ya que no se trata de lo mismo para todo el mundo. El conocimiento de sus datos parte de poder identificar qué datos confidenciales tiene en la actualidad para poder clasificarlos de manera adecuada.

## Etiquetas de confidencialidad

Las etiquetas de confidencialidad de Microsoft Information Protection le permiten clasificar y proteger los datos de su organización y, al mismo tiempo, garantizar que la colaboración y la productividad del usuario no se vean obstaculizadas.

Cuando asigna una etiqueta de confidencialidad a un grupo, documento o correo electrónico, funciona como un sello que se aplica al contenido. Esa etiqueta es:

- **Personalizable.** Puede crear categorías para distintos niveles de contenido confidencial de su organización, como Personal, Público, General, Confidencial y Extremadamente confidencial.
- **Texto no cifrado.** Debido a que la etiqueta se almacena como texto no cifrado en los metadatos del contenido, los servicios y las aplicaciones de terceros pueden leerla y, a continuación, aplicar sus propias medidas de protección si es necesario.
- **Persistente.** Después de aplicar una etiqueta de confidencialidad al contenido, esta se almacena en los metadatos de ese correo electrónico o documento. Esto significa que la etiqueta se sincroniza con el contenido, incluida la configuración de protección, y estos datos pasan a ser la base para aplicar las directivas.

Cuando se aplica una etiqueta de confidencialidad a un correo electrónico o documento, la configuración de protección de dicha etiqueta se aplica al contenido. Con las etiquetas de confidencialidad se puede hacer lo siguiente:

- **Cifrar** solo correo electrónico o correo electrónico y documentos. Puede elegir qué usuarios o grupos tienen permisos para realizar las acciones que elija y durante cuánto tiempo. Para obtener más información acerca de la configuración de cifrado al crear o editar una etiqueta de confidencialidad, consulte [Restringir el acceso al contenido mediante el uso de confidencialidad de cifrado](#).
- **Marcar el contenido** cuando se usan aplicaciones de Office al agregar marcas de agua, encabezados o pies de página a correos electrónicos o documentos a los que se aplica la etiqueta. Las marcas de agua se pueden aplicar a los documentos, pero no a los correos electrónicos. Para obtener más información acerca de cuándo se aplican los marcados de contenido,

consulte [Cuando las aplicaciones de Office aplican marcado y cifrado de contenido](#).

- **Aplicar la etiqueta automáticamente** en las aplicaciones de Office o recomendar una etiqueta. Puede elegir qué tipo de información confidencial desea que se etiquete. La etiqueta se puede aplicar automáticamente o, en su lugar, puede pedir a los usuarios que apliquen la etiqueta que recomienda.
- **Proteger el contenido en contenedores como sitios y grupos** al participar en la versión preliminar para el [uso de etiquetas de confidencialidad con Microsoft Teams, los grupos de Microsoft 365 y los sitios de SharePoint](#). Esta configuración de etiqueta no provoca que los documentos se etiqueten automáticamente. En cambio, la configuración de etiqueta protege el contenido al controlar el acceso al contenedor en el que se almacenan los documentos.

Cuando haya creado sus etiquetas de confidencialidad, debe publicarlas y ponerlas a disposición de las personas de su organización, así como de sus servicios. Las etiquetas de confidencialidad se pueden aplicar a documentos y correos electrónicos. Las etiquetas de confidencialidad se publican para usuarios o grupos. Una vez publicadas, las etiquetas de confidencialidad se mostrarán en las aplicaciones de Office para dichos usuarios y grupos.

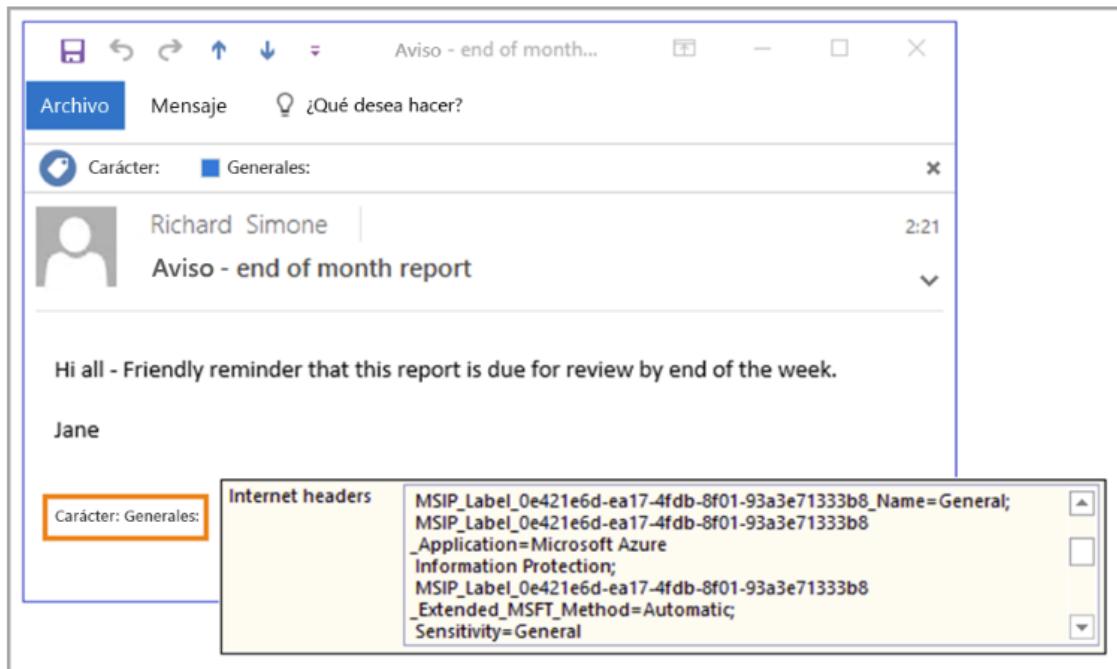
Las etiquetas de confidencialidad usan Azure Information Protection.

## Azure Information Protection

Azure Information Protection (a veces se denomina AIP) es una solución basada en la nube que ayuda a las organizaciones a clasificar y, opcionalmente, proteger sus documentos y correos electrónicos mediante la aplicación de etiquetas. Las etiquetas se pueden aplicar automáticamente por los administradores que definen las reglas y condiciones, manualmente por los usuarios o mediante una combinación de ambas, en cuyo caso los usuarios se guían por las recomendaciones.

Se usan etiquetas de Azure Information Protection para aplicar una clasificación a documentos y correos electrónicos. Al usarlas, la clasificación es identificable independientemente de dónde se almacenen los datos o con quién se compartan. Las etiquetas pueden incluir distintivos visuales, como un encabezado, un pie de página o una marca de agua. Los metadatos se agregan a los archivos y encabezados de correo electrónico en texto no cifrado. El texto no cifrado garantiza que otros servicios, como las soluciones de prevención de pérdida de datos, puedan identificar la clasificación y tomar las medidas adecuadas.

Por ejemplo, el siguiente mensaje de correo electrónico se ha clasificado como "General". La etiqueta ha agregado un pie de página de "Confidencialidad: General" al mensaje de correo electrónico. Este pie de página es un indicador visual para todos los destinatarios y marca los datos empresariales generales que no se deben enviar fuera de la organización. La etiqueta se inserta en los encabezados de correo electrónico para que los servicios de correo electrónico puedan inspeccionar este valor y crear una entrada de auditoría o evitar que se envíe fuera de la organización.



## Clasificación de los datos

Después de aplicar etiquetas de retención y de confidencialidad, las organizaciones querrán ver cómo se usan las etiquetas en el inquilino y qué se hace con esos elementos. El portal de clasificación de datos, al que se accede desde el Centro de cumplimiento de Microsoft 365, aporta instantáneas de cómo se utilizan las etiquetas y la información confidencial en las ubicaciones de la organización.

## Proteger los datos confidenciales durante todo su ciclo de vida

Durante su ciclo de vida, los datos se crearán, compartirán, almacenarán y eliminarán. Los datos deben protegerse en todas las etapas de su ciclo de vida y dondequiera que se encuentren.

## Protección de documentos con etiquetas de confidencialidad

Las etiquetas de confidencialidad no solo sirven para clasificar sus datos. También ayudan a proteger sus datos confidenciales. Como vimos en el módulo anterior, cuando un usuario asigna una etiqueta de confidencialidad a un correo electrónico o documento, la configuración de protección de esa etiqueta se aplica al contenido.

**Aplicar automáticamente una etiqueta de confidencialidad al contenido.** Cuando crea una etiqueta de confidencialidad, puede asignar automáticamente esa etiqueta al contenido cuando coincide con las condiciones que especifique. Como resultado, la protección asociada con esa etiqueta se aplica automáticamente.

La capacidad de aplicar etiquetas de confidencialidad al contenido de forma automática es importante porque no necesita:

- Capacitar a sus usuarios sobre cuándo usar cada una de sus clasificaciones.
- Dependiendo de los usuarios para clasificar todo el contenido correctamente.
- Asegurarse de que los usuarios conozcan sus directivas. En cambio, pueden concentrarse en su trabajo.

Para obtener más información, visite [Aplicar una etiqueta de confidencialidad al contenido automáticamente](#).

**Utilice etiquetas de confidencialidad para aplicar el cifrado.** Puede restringir el acceso al contenido al que se aplique una etiqueta de confidencialidad. Por ejemplo, con la configuración de cifrado de una etiqueta de confidencialidad, puede proteger el contenido para que:

- Solo los usuarios de su organización pueden abrir un correo electrónico o documentos confidenciales.
- Solo los usuarios de un departamento específico pueden editar e imprimir documentos o correos electrónicos, mientras que todos los demás usuarios de su organización solo pueden leerlos.
- Los usuarios no pueden reenviar ni copiar información de un correo electrónico.
- Los usuarios no pueden abrir un documento después de una fecha especificada.

Cuando un documento o correo electrónico está cifrado, el acceso al contenido está restringido, de modo que:

- Solo los usuarios autorizados por la configuración de cifrado de la etiqueta pueden descifrarlo.
- Permanece cifrado sin importar dónde resida, dentro o fuera de su organización, incluso si se cambia el nombre del archivo.
- Está cifrado tanto en reposo (por ejemplo, en una cuenta de OneDrive) como en tránsito (por ejemplo, el correo electrónico mientras atraviesa Internet).

La configuración de cifrado está disponible cuando [crea una etiqueta de confidencialidad](#) en el centro de cumplimiento de Microsoft 365 o en el centro de seguridad de Microsoft 365.

## Cifrado de mensajes de Office 365 (OME)

Las personas suelen utilizar el correo electrónico para intercambiar información confidencial, como datos financieros, contratos legales, información sobre la salud del paciente, etc. Como resultado, los buzones de correo pueden convertirse en depósitos de grandes cantidades de información potencialmente confidencial y la filtración de información puede convertirse en una grave amenaza para su organización.

Con **cifrado de mensajes de Office 365**, su organización puede enviar y recibir mensajes de correo electrónico cifrados entre personas dentro y fuera de su organización. El cifrado de mensajes de Office 365 funciona con Outlook.com, Yahoo!, Gmail y otros servicios de correo electrónico. El cifrado de mensajes de correo electrónico garantiza que solo los destinatarios previstos puedan acceder al contenido del mensaje.

El cifrado de mensajes de Office 365 es un servicio en línea que se basa en **Microsoft Azure Rights Management (Azure RMS)**, que utiliza Azure Information Protection (AIP). OME incluye directivas de cifrado, identidad y autorización para ayudar a proteger su correo electrónico.

Con OME, los usuarios pueden cifrar los mensajes de correo electrónico y una variedad de archivos adjuntos. Para obtener más información consulte [Cifrado de mensajes de Office 365](#).

## Prevención de pérdida de datos (DLP)

La Prevención de pérdida de datos (DLP) se implementa a través de directivas y está diseñada para proteger la información confidencial y evitar su divulgación inadvertida. Con una directiva de prevención de pérdida de datos (DLP), puede identificar, supervisar y proteger automáticamente la información confidencial en Office 365. Las directivas de prevención de pérdida de datos pueden utilizar etiquetas de confidencialidad y [tipos de información confidencial](#) para identificar este tipo de información.

Con una directiva DLP, puede:

- **Identificar información confidencial** en muchos servicios, como Exchange Online, SharePoint Online, OneDrive para la Empresa y Microsoft Teams. Por ejemplo, puede identificar cualquier documento que contenga un número de tarjeta de crédito almacenado en cualquier sitio de OneDrive para la Empresa, o puede supervisar solo los sitios de OneDrive de personas específicas.
- **Impedir el intercambio accidental de información confidencial.** Por ejemplo, puede identificar cualquier documento o correo electrónico que contenga un registro de salud que se comparta con personas externas a su organización y, a continuación, bloquear automáticamente el acceso a ese documento o el envío del correo electrónico.
- **Supervisar y proteger la información confidencial** en las versiones de escritorio de Excel, PowerPoint y Word. Al igual que en Exchange Online, SharePoint Online y OneDrive para la Empresa, estos programas de escritorio de Office incluyen las mismas capacidades para identificar información confidencial y aplicar directivas de DLP. DLP proporciona una supervisión continua relativa al contenido que comparten las personas en estos programas de Office.
- **Ayudar a los usuarios a saber cómo mantener el cumplimiento** sin interrumpir su flujo de trabajo. Por ejemplo, si un usuario intenta compartir un documento que contiene información confidencial, una directiva DLP puede enviarle una notificación por correo electrónico y mostrarle una sugerencia de directiva.
- **Ver informes de DLP** que muestran contenido que coincide con las directivas DLP de su organización. Para evaluar la medida en que su organización cumple con una directiva DLP, puede ver cuántas coincidencias tiene cada directiva y regla a lo largo del tiempo.

DLP detecta información confidencial mediante un análisis de contenido profundo y no solo un simple escaneo de texto. Este análisis de contenido profundo utiliza

coincidencias de palabras clave, coincidencias de diccionario, la evaluación de expresiones regulares, funciones internas y otros métodos para detectar contenido que coincide con sus directivas de DLP. Potencialmente, solo un pequeño porcentaje de sus datos se considera confidencial. Una directiva de DLP puede identificar, supervisar y proteger automáticamente solo esos datos, sin obstaculizar ni afectar a los contactos que trabajan con el resto de su contenido.

Para más información, consulte [Descripción general de la prevención de pérdida de datos](#).

## Windows Information Protection

Windows Information Protection (WIP) es un conjunto de tecnologías que protegen a su organización de fugas de datos accidentales o maliciosas, sin cambios significativos en el entorno o las aplicaciones de su empresa. Aporta esta protección tanto a los dispositivos de propiedad empresarial como a los dispositivos BYOD, y lo hace sin interferir con los flujos de trabajo regulares de los empleados.

Para más información, visite [Proteja los datos de su empresa con Windows Information Protection \(WIP\)](#).

## Controlar los datos mediante Microsoft 365

La gobernanza de la información consiste en poder controlar de forma inteligente los datos en todo su entorno para reducir el riesgo.

Las capacidades de gobernanza de la información en Microsoft 365 incluyen:

- **Administrar datos:** use el [servicio de importación](#) para importar archivos PST de forma masiva a los buzones de correo de Exchange Online o configure el [archivado ilimitado](#) para ofrecer a los usuarios más almacenamiento en el buzón. Utilizar [directivas de retención](#) para simplificar la administración sobre cómo su organización retiene y elimina.
- **Supervisar datos:** el Explorador de actividad de etiquetas, en el Centro de seguridad y cumplimiento, le permite buscar y ver la actividad de etiquetas. Lo que permite ver qué etiquetas se están configurando y garantizar que las etiquetas de datos se apliquen correctamente.
- **Administrar buzones de correo inactivos:** dependiendo de los requisitos de retención de su organización, es posible que deba conservar el contenido del buzón durante unos meses o años después de que finalice el empleo o de forma indefinida. Independientemente del tiempo que tenga que retener el correo electrónico, puede crear [buzones inactivos](#) para mantener el buzón de correo de ex empleados.
- **Administración de registros:** la solución de [administración de registros](#) de Microsoft 365 le ayuda a cumplir con las obligaciones normativas y legales. También ayuda a ser más eficiente al eliminar documentos y datos que ya no son necesarios. La solución de administración de registros de Microsoft 365 incluye lo siguiente:
  - Etiquetar contenido como registro.

- Migrar y administrar sus planes de retención con el administrador de planes de archivos.
- Establecer directivas de retención y eliminación dentro de la etiqueta de registro.
- Activar la retención basada en eventos.
- Revisar y validar la eliminación.
- Comprobar la eliminación de registros.
- Exportar la información sobre elementos eliminados.
- Establecer permisos específicos para las funciones de administrador de registros en su organización.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Qué tipo de directiva se puede utilizar para identificar, supervisar y proteger automáticamente información confidencial en Office 365?

- A. Directivas de alerta
- B. Directivas de prevención de pérdida de datos
- C. Directivas de retención

¿Cómo ayuda la solución de administración de registros de Microsoft 365 a la organización a cumplir con sus obligaciones normativas y legales?

- A. Cifrar información confidencial
- B. Administrar buzones de correo inactivos
- C. Ayudar a las organizaciones a ser más eficientes eliminando documentos y datos que ya no son necesarios.

¿Cuál es el propósito de aplicar etiquetas de confidencialidad a sus datos?

- A. Para identificar en qué carpeta se deben almacenar los datos
- B. Para ejecutar las directivas de protección de datos
- C. Para determinar cuánto tiempo se deben conservar los datos

¿Cuál es la principal ventaja de Azure Information Protection?

- A. Las etiquetas de clasificación de datos se pueden identificar independientemente de dónde se almacenen los datos
- B. Agregar secciones a documentos de Word
- C. Mejora la eficiencia de almacenamiento

# Describir las funcionalidades de administración de cumplimiento de Microsoft

## Introducción

Las organizaciones deben cumplir con los estándares legales y normativos relacionados con el cumplimiento para proteger a sus clientes, a sus socios y a sí mismas. Microsoft aporta herramientas y funcionalidades que permiten a las organizaciones administrar el cumplimiento.

En esta lección, conocerá los diferentes requisitos de cumplimiento comunes a los que deben ajustarse las organizaciones. Sabrá a dónde dirigirse para encontrar la documentación de cumplimiento al explorar el Portal de confianza de servicios. También aprenderá los principios de privacidad de Microsoft. Además, explorará soluciones como el Centro de cumplimiento y el Administrador de cumplimiento de Microsoft 365, que pueden ayudarle a administrar y simplificar las tareas de cumplimiento de una organización.

Después de completar esta lección, podrá hacer lo siguiente:

- Encontrar documentación del cumplimiento.
- Describir los principios de privacidad de Microsoft.
- Explorar el Centro de cumplimiento de Microsoft 365.
- Describir las ventajas del Administrador de cumplimiento.

## Describir las necesidades de cumplimiento comunes

En la actualidad, los datos tienen más importancia que nunca. Las organizaciones, instituciones y sociedades enteras generan datos y dependen de ellos para funcionar diariamente. La manipulación o pérdida de datos puede afectar a organizaciones, instituciones y sociedades por igual. La gran escala de datos que se generan y la creciente dependencia de ellos implica que la administración de datos se haya vuelto fundamental.

Los gobiernos están trabajando duro para proteger a las personas mediante la creación de reglamentos (leyes) que protejan los datos a través de diversas medidas como las siguientes:

- Garantizar el derecho de las personas a acceder a sus datos en cualquier momento.
- Garantizar el derecho de las personas a corregir o eliminar datos suyos si es necesario.
- Introducir períodos de retención que dicten una cantidad mínima o máxima de tiempo para almacenar los datos.
- Conceder a los gobiernos y a las agencias de regulación el derecho a acceder y examinar los datos cuando sea necesario.
- Definir reglas sobre qué datos se pueden procesar y cómo.

Algunos reglamentos también exigen que los datos permanezcan bajo protección incluso aunque se muevan entre diferentes localizaciones geográficas. Por ejemplo, las normativas de algunos países o regiones exigen que cualquier dato personal que se transfiera fuera de sus fronteras cumpla una serie de condiciones, como las siguientes:

- El país o región de destino donde se van a transferir los datos personales debe tener las protecciones de datos adecuadas.
- Las organizaciones deben crear medidas de seguridad adecuadas, como cláusulas específicas que se incluyan en los contratos con las organizaciones u organismos que vayan a administrar los datos personales.

## Reglamentos de cumplimiento común

Estas son algunas de las normativas con las que comúnmente trabajan las organizaciones e instituciones:

- **Ley de portabilidad y responsabilidad de seguros de salud (HIPAA):** establece reglas sobre cómo debe protegerse la información relacionada con la salud.
- **Ley de derechos educativos y privacidad familiar (FERPA):** establece reglas para proteger la información de los estudiantes.
- **ISO 27701:** establece reglas y pautas para administrar la información personal y demostrar su cumplimiento.

Microsoft cubre las necesidades de cumplimiento con herramientas y funciones integradas para ayudarle a proteger la información, administrar la gobernanza de datos y responder a las solicitudes reglamentarias.

## Describir las ofertas del Portal de confianza de servicios

El Portal de confianza de servicios aporta información, herramientas y otros recursos sobre seguridad, privacidad y prácticas de cumplimiento de Microsoft. Inicie sesión con su cuenta de servicios en la nube de Microsoft para acceder a toda la documentación disponible.

Desde el menú principal, puede acceder a estas opciones:

- **Portal de confianza de servicios:** página principal.
- **Administrador de cumplimiento:** mide su progreso en la realización de acciones que ayudan a reducir los riesgos relacionados con la protección de datos y los estándares normativos. Para obtener más información, consulte la documentación del Administrador de cumplimiento de Microsoft en la sección Más información que aparece a continuación.
- **Documentos de confianza:** vínculos a información sobre implementación y diseño de seguridad.
- **Sectores y regiones:** contiene información de cumplimiento sobre los servicios de Microsoft Cloud organizados por sector y región. El vínculo de soluciones del sector actualmente muestra la página principal de servicios financieros. El vínculo de soluciones regionales muestra actualmente

- información para los siguientes países o regiones: Australia, Canadá, República Checa, Dinamarca, Alemania, Polonia, Rumanía, España y el Reino Unido.
- **Centro de confianza:** vínculos al Centro de confianza de Microsoft, que aporta más información sobre la seguridad, el cumplimiento y la privacidad en Microsoft Cloud.
  - **Recursos:** vínculos a recursos, incluidos la información sobre las características y herramientas disponibles para la protección y el gobierno de datos en Office 365, los centros de datos globales de Microsoft y las preguntas más frecuentes.
  - **Mi biblioteca:** le permite agregar documentos y recursos que son relevantes para su organización. Todo está en un solo lugar. También puede optar por que se le envíen notificaciones por correo electrónico cuando se actualice un documento, así como establecer la frecuencia con la que recibirá las notificaciones.

## Describir los principios de privacidad de Microsoft

Los productos y servicios de Microsoft se basan en la confianza. Microsoft se centra en seis principios de privacidad clave a la hora de tomar decisiones sobre los datos. La privacidad consiste en tomar decisiones significativas sobre cómo y por qué se recopilan y utilizan los datos. Se trata de asegurarse de que tiene la información que necesita para tomar las decisiones que más le convienen, en todos los productos y servicios de Microsoft.

Los seis principios de la privacidad son los siguientes:

- **Control:** ponerle a usted, el cliente, en control de su privacidad con herramientas fáciles de usar y opciones claras.
- **Transparencia:** ser transparentes sobre la recopilación y utilización de datos para que todos puedan tomar decisiones informadas.
- **Seguridad:** protección de los datos confiados a Microsoft mediante una seguridad y un cifrado sólidos.
- **Fuertes protecciones legales:** Respetar las leyes locales de privacidad y luchar por la protección legal de la privacidad como derecho humano fundamental.
- **Sin segmentación basada en contenido:** no usar correo electrónico, chat, archivos u otro contenido personal para orientar la publicidad.
- **Ventajas para usted:** Cuando Microsoft recopila datos, los utiliza para beneficiarle a usted, el cliente, y para mejorar su experiencia.

Estos principios conforman la base de la privacidad de Microsoft y determinan el modo en que se diseñan los productos y servicios. Obtenga más información en el **Centro de confianza de Microsoft** en la sección Más información que aparece a continuación.

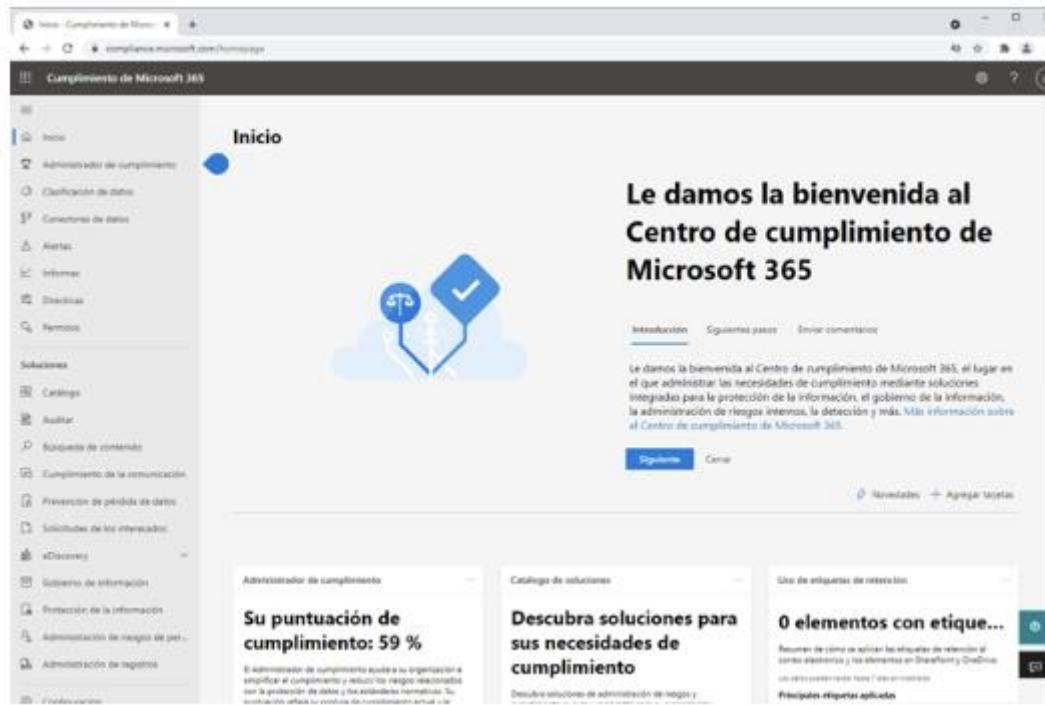
## Describir el Centro de cumplimiento

El Centro de cumplimiento de Microsoft 365 reúne todas las herramientas y datos necesarios para comprender y administrar las necesidades de cumplimiento de una organización.

Pueden acceder al centro de cumplimiento los clientes que tengan SKU de Microsoft 365 con uno de los siguientes roles:

- Administrador global.
- Administrador de cumplimiento.
- Administrador de datos de cumplimiento.

Cuando un administrador inicia sesión en el portal del Centro de cumplimiento de Microsoft 365, tiene una información general de la forma en que la organización está cumpliendo los requisitos de cumplimiento y de las soluciones que puede utilizar para ayudar con el cumplimiento, información sobre alertas activas y más.



La página de inicio predeterminada del Centro de cumplimiento tiene varios tarjetas, entre otras:

- La tarjeta **Puntuación de cumplimiento**. Esta tarjeta muestra la puntuación de cumplimiento y redirige a los administradores al Administrador de cumplimiento, en el que pueden ver un desglose de la puntuación de cumplimiento. La puntuación de cumplimiento mide el progreso a la hora de completar las acciones de mejora recomendadas de los controles. La puntuación ayuda a una organización a comprender su estado actual respecto al cumplimiento. Además, le ayuda a priorizar las acciones en función de su potencial para reducir el riesgo.



- La nueva tarjeta **Catálogo de soluciones** vincula a colecciones de soluciones integradas que se usan para administrar situaciones de cumplimiento de un extremo a otro en tres áreas de soluciones de cumplimiento:
  - La sección **Gobernanza y protección de la información** muestra de forma rápida cómo utilizar las soluciones de cumplimiento de Microsoft 365 para proteger y regir los datos de su organización.
  - La sección **Administración de riesgos internos** de la página de inicio muestra cómo puede la organización identificar, analizar y actuar frente a riesgos internos antes de que causen daños.
  - La sección **Descubrimiento y respuesta** de la página de inicio muestra cómo puede la organización encontrar, investigar y responder de forma rápida a los problemas de cumplimiento con datos relevantes.

Las funcionalidades y herramientas de una solución pueden incluir una combinación de directivas, alertas, informes y más.

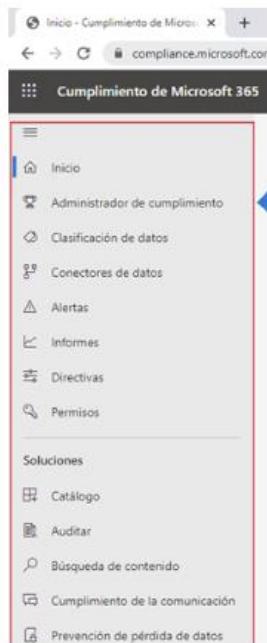


- La tarjeta **Alertas activas** incluye un resumen de la mayoría de las alertas activas y un vínculo donde los administradores pueden ver información más detallada, como gravedad de la alerta, estado, categoría y más.



## Navegación

Además de las tarjetas de la página principal, hay un panel de navegación a la izquierda de la pantalla que facilita el acceso a las alertas, informes, directivas, soluciones de cumplimiento, etc. Para agregar o quitar opciones y obtener un panel de navegación personalizado, puede usar el control **Personalizar navegación** en el panel de navegación para configurar los elementos que aparecen.



# Describir el Administrador de cumplimiento

El Administrador de cumplimiento de Microsoft es una característica del Centro de cumplimiento de Microsoft 365 que ayuda a los administradores a administrar los requisitos de cumplimiento con mayor facilidad y comodidad. El Administrador de cumplimiento realiza labores para ayudar a las organizaciones a mejorar el cumplimiento, como enumerar los riesgos de la protección de datos, administrar las dificultades a la hora de implementar controles, mantenerse al día de las regulaciones y certificaciones y dar parte a los auditores.

El Administrador de cumplimiento ayuda a simplificar el cumplimiento y reducir el riesgo al ofrecer siguiente:

- Evaluaciones predefinidas basadas en regulaciones y estándares regionales e industriales comunes. Los administradores también pueden usar evaluaciones personalizadas para abordar necesidades de cumplimiento específicas de la organización.
- Funcionalidades del flujo de trabajo que permiten a los administradores completar evaluaciones del riesgo de la organización con eficacia.
- Acciones de mejora detalladas paso a paso que los administradores pueden llevar a cabo para cumplir con las regulaciones y estándares relevantes para la organización. Microsoft también administrará algunas acciones en nombre de la organización. Los administradores obtendrán detalles de implementación y resultados de auditoría de dichas acciones.
- La puntuación de cumplimiento es un cálculo que ayuda a una organización a entender su postura general de cumplimiento mediante la medición del progreso en las acciones de mejora.

El panel del Administrador de cumplimiento muestra la puntuación actual de cumplimiento, ayuda a los administradores a ver qué aspectos necesitan atención y les guía hacia las acciones clave de mejora.

The screenshot shows the Microsoft 365 Compliance Center interface. On the left, there's a navigation sidebar with links like 'Inicio', 'Administrador de cumplimiento' (which is selected and highlighted in blue), 'Clasificación de datos', 'Controladores de datos', 'Alertas', 'Informes', 'Directrices', 'Formato', 'Soluciones' (with sub-links like 'Catálogo', 'Audit', 'Búsqueda de contenido', 'Cumplimiento de la comunicación', 'Prevención de pérdida de datos', 'Sustitución de los intercambios', 'eDiscovery', 'Gobierno de información', 'Restricción de la información', 'Administración de riesgos de privacidad', and 'Administración de registros'), and 'Centro de cumplimiento' (with sub-links like 'Puntuación de cumplimiento general', 'Acciones de mejora clave', 'Soluciones', 'Evaluaciones', and 'Plantillas de evaluación').

The main content area is titled 'Administrador de cumplimiento'. It features a 'Información general' card with the heading 'Su puntuación de cumplimiento: 59%' and a gauge meter showing '11682/19571 puntos obtenidos'. Below this, there are two boxes: 'Estatus de ejecución' (with a value of '131 / 8050') and 'Puntuación obtenida administrada por Microsoft' (with a value of '11521 / 11521'). A note below states: 'La puntuación de cumplimiento mide su progreso al completar las acciones recomendadas que minimizan el riesgo de la protección de datos.'

The 'Acciones de mejora clave' section displays a table with three columns: 'No cumplidas' (606), 'Completadas' (6), and 'Fuera del ámbito' (0). Each row in the table provides details about an action item, including its name, points, status (Incomplete, Complete, Out of scope), and a link to 'Ver más'.

El Administrador de cumplimiento utiliza varios elementos de datos para ayudar a administrar las actividades de cumplimiento. A medida que los administradores utilizan el Administrador de cumplimiento para asignar, probar y supervisar las actividades de cumplimiento, es útil tener una comprensión básica de los elementos clave: controles, evaluaciones, plantillas y acciones de mejora.

## Controles.

Un control es el requisito de una regulación, estándar o directiva. Define cómo se evalúa y administra la configuración del sistema, el proceso organizativo y las personas responsables de cumplir con un requisito específico de una regulación, estándar o directiva.

El Administrador de cumplimiento realiza un seguimiento de los siguientes tipos de controles:

- **Controles que administra Microsoft:** controles de servicios en la nube de Microsoft que la propia Microsoft se encarga de implementar.
- **Controles propios:** a veces se denominan “controles que administra el cliente” y los implementa y administra la organización.
- **Controles compartidos:** la organización y Microsoft comparten la responsabilidad de implementarlos.

El Administrador de cumplimiento evalúa continuamente los controles escaneando en su entorno de Microsoft 365 y detectando la configuración de su sistema, actualizando continua y automáticamente su estado de acción técnica.

## Evaluaciones

Una evaluación es una serie de controles de una regulación, estándar o directiva específica. Completar las acciones de una evaluación sirve para cumplir con los requisitos de un estándar, regulación o ley. Por ejemplo, una organización puede tener una evaluación que, cuando el administrador complete todas las acciones que contiene, sirva para alinear la configuración de Microsoft 365 de la organización con los requisitos de ISO 27001.

Las evaluaciones tienen varios componentes:

- **Servicios en el ámbito:** el conjunto específico de servicios de Microsoft aplicables a la evaluación.
- **Controles que administra Microsoft:** controles de servicios en la nube de Microsoft que la propia Microsoft implementa para la organización.
- **Controles propios:** a veces se denominan “controles que administra el cliente” y los implementa y administra la organización.
- **Controles compartidos:** la organización y Microsoft comparten la responsabilidad de implementarlos.
- **Puntuación de evaluación:** muestra el progreso de cara a lograr todos los puntos posibles a partir de acciones de la evaluación que administran la organización y Microsoft.

Al crear evaluaciones, un administrador las asignará a un grupo. El administrador puede configurar los grupos de la forma más lógica para la organización. Por ejemplo, pueden agrupar las evaluaciones por año de auditoría, región, solución, equipos en la organización, o de alguna otra manera. Una vez que el administrador ha creado los grupos, puede [filtrar la vista de panel](#) para ver la puntuación por uno o más grupos.

## Plantillas

El Administrador de cumplimiento aporta plantillas para que los administradores puedan crear evaluaciones rápidamente. Pueden modificarlas para crear evaluaciones que se ajusten a sus necesidades. Los administradores también pueden elaborar plantillas con sus propios controles y acciones para crear evaluaciones personalizadas. Por ejemplo, puede que el administrador quiera una plantilla para abordar un control interno de los procesos de negocio o un estándar regional de protección de datos que ninguna de las más de 150 plantillas de evaluación predefinidas de Microsoft contempla.

## Acciones de mejora

Las acciones de mejora ayudan a centralizar las actividades de cumplimiento. Cada acción de mejora aporta orientación recomendada con la intención de ayudar a las organizaciones a alinearse con las regulaciones y estándares de protección de datos. Las acciones de mejora pueden asignarse a usuarios de la organización para que lleven a cabo labores de implementación y pruebas. Los administradores también pueden almacenar documentación, notas y actualizaciones del estado del registro de la acción de mejora.

## Beneficios del Administrador de cumplimiento

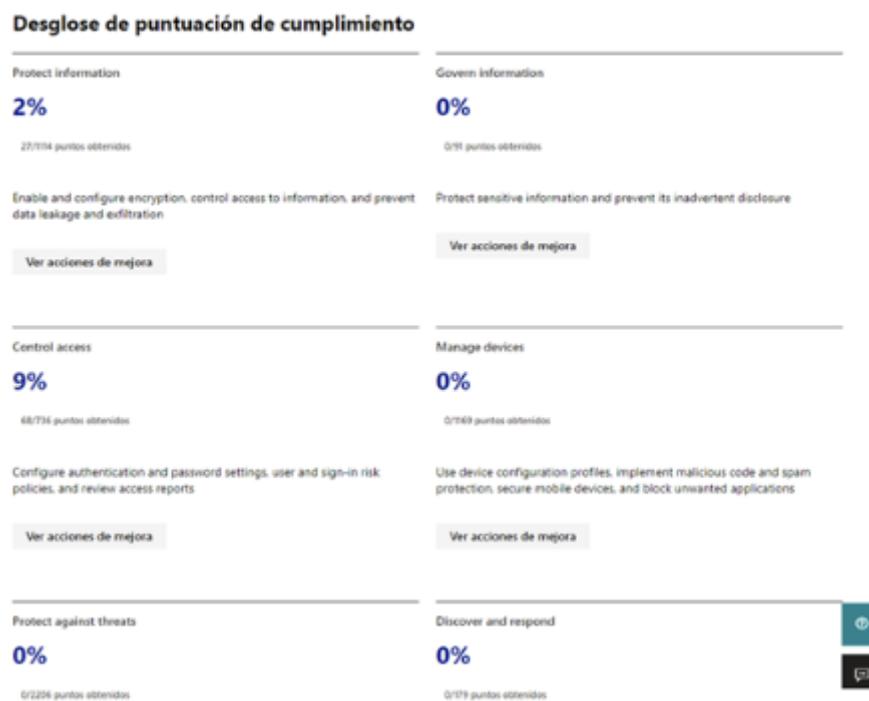
El Administrador de cumplimiento tiene muchos beneficios, entre los que se incluyen los siguientes:

- Traducir a un lenguaje sencillo reglamentos, normas, directivas empresariales u otros marcos de control complejos.
- Dar acceso a una amplia variedad de evaluaciones listas para usar y evaluaciones personalizadas para ayudar a las organizaciones con sus necesidades únicas de cumplimiento.
- Asignar los controles reglamentarios con las acciones de mejora recomendadas.
- Dar orientación paso a paso sobre cómo implementar las soluciones para cumplir los requisitos reglamentarios.
- Ayudar a los administradores y usuarios a priorizar las acciones que tendrán un mayor impacto en el cumplimiento de su organización, asociando una puntuación a cada acción.

# Describir el uso y las ventajas de la puntuación de cumplimiento

La puntuación de cumplimiento mide el progreso a la hora de completar las acciones de mejora recomendadas en los controles. La puntuación puede servir para que una organización conozca su estado actual respecto al cumplimiento. También ayuda a las organizaciones a priorizar las acciones en función de su potencial para reducir el riesgo.

Los administradores pueden obtener un desglose de la puntuación de cumplimiento en el panel de información general del Administrador de cumplimiento:



## ¿Cuál es la diferencia entre el Administrador de cumplimiento y la puntuación de cumplimiento?

El Administrador de cumplimiento es una solución de un extremo a otro del centro de cumplimiento de Microsoft 365 que permite a los administradores administrar y llevar un seguimiento de las actividades de cumplimiento. La puntuación de cumplimiento es un cálculo del estado general de la organización respecto al cumplimiento. La puntuación de cumplimiento está disponible a través del Administrador de cumplimiento.

El Administrador de cumplimiento da a los administradores las funcionalidades para comprender y aumentar su puntuación de cumplimiento de cara a mejorar el estado de su organización respecto al cumplimiento, de forma que se alinee con los requisitos de cumplimiento.

## Cómo conocer la puntuación de cumplimiento

La puntuación de cumplimiento general se calcula a partir de las puntuaciones que se asignan a las acciones. Hay dos tipos de acciones:

- **Sus acciones de mejora:** acciones que debe administrar la organización.
- **Acciones de Microsoft:** acciones que administra Microsoft por la organización.

Este tipo de acciones llevan asignados unos puntos que cuentan para la puntuación de cumplimiento. Las acciones también pueden considerarse técnicas o no técnicas, lo cual también afecta a la puntuación de cumplimiento general. También se asigna un valor de puntuación a las acciones en función de si son obligatorias, discretionales, de prevención, de detección o de corrección:

- **Obligatorias:** son acciones que no deben eludirse. Por ejemplo, crear una directiva para establecer requisitos de longitud o caducidad de las contraseñas.
- **Discretionales:** son acciones que dependen de la comprensión de los usuarios de una directiva y de su adhesión a ella. Por ejemplo, una directiva que establezca que los usuarios tengan que asegurarse de que bloquean sus dispositivos antes de dejarlos.

Las siguientes subcategorías de acciones pueden clasificarse como obligatorias o discretionales:

- Las acciones **preventivas** están diseñadas para hacer frente a riesgos específicos, como proteger los datos en reposo a través del cifrado en caso de vulneraciones o ataques.
- Las acciones **de detección** supervisan activamente los sistemas para identificar irregularidades que puedan representar un riesgo o que puedan usarse para detectar vulneraciones o infracciones. Algunos ejemplos de este tipo de acciones son las auditorías de acceso a sistemas o de cumplimiento de regulaciones.
- Las acciones **correctivas** ayudan a los administradores a minimizar los efectos adversos de los incidentes de seguridad a través de las medidas correctivas que reducen su efecto inmediato o posiblemente incluso revertir el daño.

¿Cómo se calcula la puntuación de cumplimiento?			
	Prevención	De detección	Correctiva
▶ Obligatoria	+27 puntos	+3 puntos	+3 puntos
● Discrecional	+9 puntos	+1 puntos	+1 puntos

Las acciones obligatorias y de prevención suponen el mayor valor de puntos de cara a la puntuación de cumplimiento (27 puntos). Las organizaciones acumulan puntos con cada acción que completan. Y la puntuación de cumplimiento se muestra en forma de un porcentaje que representa todas las acciones completadas en comparación con las que quedan pendientes:



## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Luego seleccione **Comprobar sus respuestas**.

Al explorar la documentación del cumplimiento de Microsoft en el Portal de confianza de servicios, ha encontrado varios documentos específicos de su sector. ¿Cuál es la mejor manera de asegurarse de que se mantiene al día con las actualizaciones más recientes?

- A. Guardar los documentos en Mi biblioteca.
- B. Imprimir cada documento para poder consultarlos fácilmente.
- C. Descargar cada documento.

Ha entrado un nuevo administrador en el equipo y necesita poder acceder al Centro de cumplimiento de Microsoft 365. ¿Cuál de los siguientes roles podría utilizar el administrador para acceder al Centro de cumplimiento?

- A. Rol de administrador de cumplimiento
- B. Rol de administrador del departamento de soporte técnico
- C. Rol de administrador de usuarios

Sus nuevos compañeros del equipo de administración no están familiarizados con el concepto de los controles compartidos en el Administrador de cumplimiento. ¿Cómo se lo explicaría?

- A. Son controles que deben implementar tanto los reguladores externos como Microsoft.
- B. Son controles que deben implementar tanto su organización como los reguladores externos.
- C. Son controles que deben implementar tanto su organización como Microsoft.

Un cliente ha pedido una presentación sobre cómo puede el Centro de cumplimiento de Microsoft 365 mejorar el estado del cumplimiento en su organización. La presentación tendrá que hablar del Administrador de cumplimiento y la puntuación de cumplimiento. ¿Cuál es la diferencia entre el Administrador de cumplimiento y la puntuación de cumplimiento?

- A. El Administrador de cumplimiento es una solución de un extremo a otro del Centro de cumplimiento de Microsoft 365 que permite a los administradores administrar y hacer un seguimiento de las actividades de cumplimiento. La puntuación de cumplimiento es un cálculo del estado general de la organización respecto al cumplimiento.
- B. El Administrador de cumplimiento es una solución de un extremo a otro del Centro de cumplimiento de Microsoft 365 que permite a los administradores administrar y llevar un seguimiento de las actividades de cumplimiento. La puntuación de cumplimiento es la puntuación que los reguladores dan a la organización por un cumplimiento correcto.
- C. El Administrador de cumplimiento es el regulador que administrará sus actividades de cumplimiento. La puntuación de cumplimiento es un cálculo del estado general de la organización respecto al cumplimiento.

# Reducir el riesgo y simplificar el proceso de detección y auditoría

## Introducción

Para seguir abordando los desafíos legales, empresariales y de cumplimiento normativo, las empresas deben poder conservar y proteger la información importante y encontrar rápidamente lo que es relevante. Mantener y proteger información importante se extiende no solo a cómo las entidades externas ven y usan sus datos, sino que también se aplica a cómo sus empleados usan y acceden a los datos de su organización. Microsoft 365 proporciona una serie de herramientas, servicios y características que pueden ayudar a las empresas a mitigar o prevenir el riesgo interno.

Otro aspecto de los requisitos regulatorios que cambian rápidamente a los que deben enfrentarse las organizaciones es la capacidad de encontrar información relevante. Examinar manualmente millones de archivos para encontrar el pequeño número que es relevante simplemente no es una opción. Ya sea respondiendo a investigaciones, litigios o solicitudes regulatorias, las organizaciones deben poder encontrar rápidamente lo que es relevante. Auditoría avanzada y eDiscovery avanzado son herramientas para ayudar a su organización a encontrar datos relevantes de forma rápida y rentable.

Al final de este módulo, podrá hacer lo siguiente:

- Explorar las capacidades de Microsoft 365 para administrar el riesgo interno.
- Describir las herramientas disponibles para ayudar a las organizaciones a encontrar datos relevantes de forma rápida y rentable.

## Administrar el riesgo interno

La administración de riesgos internos es una solución en Microsoft 365 que ayuda a minimizar los riesgos internos al permitirle detectar e investigar las actividades de riesgo en su organización, y tomar medidas sobre ellas.

La administración y minimización del riesgo en su organización comienza con la comprensión de los tipos de riesgos ligados al área de trabajo moderna. Algunos riesgos están ligados a factores y eventos externos y no se pueden controlar de forma directa. Otros riesgos derivan de eventos internos y actividades de los empleados que pueden eliminarse y evitarse. Algunos ejemplos son los riesgos de comportamientos y acciones ilegales, inapropiados, no autorizados o poco éticos por parte de empleados y gerentes. Estos comportamientos incluyen una amplia gama de riesgos internos de los empleados:

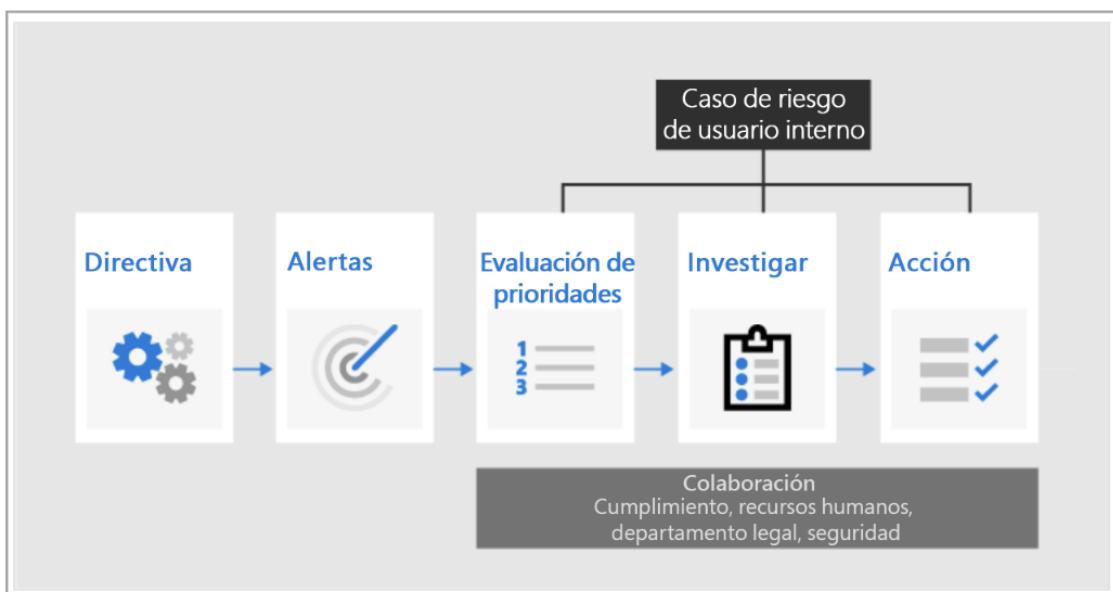
- Filtraciones de datos confidenciales y pérdida de datos
- Infracciones a la confidencialidad
- Robo de propiedad intelectual (PI)
- Fraude
- Tráfico de información privilegiada
- Infracciones de cumplimiento normativo

Los empleados del lugar área de trabajo moderna pueden crear, administrar y compartir datos en un amplio espectro de plataformas y servicios. En la mayoría de los casos, las organizaciones tienen recursos y herramientas limitados para identificar y mitigar los riesgos de toda la organización y al mismo tiempo cumplir con los estándares de privacidad de los empleados.

## Flujo de trabajo de la administración de riesgo interno

La administración de riesgo interno le ayuda a identificar, investigar y abordar los riesgos internos de su organización. Con plantillas de directivas enfocadas, la señalización de la actividad integral en todo el servicio de Microsoft 365 y flujo de trabajo flexible, puede usar información útil para identificar y resolver comportamientos de riesgo rápidamente.

La identificación y resolución de actividades de riesgo interno y los problemas de cumplimiento con la administración de riesgo interno en Microsoft 365 utiliza el siguiente flujo de trabajo:



- Directivas: las directivas de administración de riesgo interno se crean mediante plantillas predefinidas y condiciones de directivas que definen qué indicadores de riesgo se examinan en las áreas de características de Microsoft 365. Estas condiciones incluyen cómo se usan los indicadores para las alertas, qué usuarios se incluyen en la directiva, qué servicios se priorizan y el período de tiempo de supervisión. Para obtener más información, consulte [Insider risk management policies](#).
- Alertas: las alertas se generan automáticamente mediante indicadores de riesgo que coinciden con las condiciones de la directiva y se muestran en el **Panel de alertas**. Este panel permite una vista rápida de todas las alertas que necesitan repaso, alertas abiertas a lo largo del tiempo y estadísticas de alertas para su organización. Para más información, consulte [Alertas de la administración de riesgo interno](#).
- Evaluación de prioridades: las nuevas actividades que necesitan investigación generan de forma automática alertas a las que se les asigna el

estado de *Necesita revisión*. Los revisores pueden identificar rápidamente estas alertas y desplazarse por cada una para evaluar y clasificar las prioridades. Las alertas se resuelven abriendo un nuevo caso, asignando la alerta a un caso existente o descartando la alerta. Como parte del proceso de evaluación de prioridades, los revisores pueden ver los detalles de la alerta de la coincidencia de la directiva, ver la actividad del usuario asociada con la coincidencia, ver la gravedad de la alerta y revisar la información de perfil del usuario.

- Investigar: se crean casos para alertas que requieren una revisión e investigación más profunda de los detalles y circunstancias en torno a la coincidencia de las directivas. El **Panel de control del caso** proporciona una vista completa de todos los casos activos, los casos abiertos a lo largo del tiempo y las estadísticas de casos para su organización. Al seleccionar un caso en el panel de casos, se abre el caso para su investigación y revisión. Para obtener más información, consulte [Casos de administración de riesgo interno](#).
- Acción: después de que se investigan los casos, los revisores pueden tomar medidas rápidamente para resolver el caso o colaborar con otras partes interesadas del riesgo en su organización.
  - Las acciones pueden ser tan simples como enviar una notificación cuando los empleados cometen una infracción en las condiciones de la directiva de manera accidental o inadvertida. Para obtener más información, consulte [Plantillas de avisos de administración de riesgo interno](#).
  - En casos más graves, es posible que deba compartir la información del caso de administración de riesgo interno con otros revisores de su organización. Escalar un caso para su investigación le permite transferir datos y la administración del caso a eDiscovery avanzado en Microsoft 365. Para obtener más información sobre los casos de eDiscovery avanzado, consulte [Descripción general de eDiscovery avanzado en Microsoft 365](#).

## Situaciones

A continuación se presentan algunos ejemplos de cómo la administración de riesgos internos puede ayudar a las empresas a administrar los riesgos internos en su organización:

- Robo de datos por parte de los empleados: cuando los empleados abandonan una organización, ya sea voluntariamente o como resultado de un despido, a menudo existe una preocupación legítima de que los datos de la empresa, los clientes y los empleados estén en riesgo. Las directivas de administración de riesgo interno que utilizan la plantilla de la directiva [Robo de datos por empleado que se va](#) detectan en forma automática las actividades típicamente asociadas con este tipo de robo.
- Filtraciones intencionales o no intencionales de información sensible o confidencial: en la mayoría de los casos, los empleados hacen todo lo posible para gestionar adecuadamente la información sensible o confidencial. A veces, los empleados pueden filtrar o compartir

- intencionalmente información sensible y confidencial de forma malintencionada y para un beneficio personal potencial. Las directivas de administración de riesgo interno creadas utilizando la plantilla de directiva [Pérdidas de datos](#) detectan de forma automática las actividades típicamente asociadas con el intercambio de información sensible o confidencial.
- Acciones y comportamientos que infringen las directivas corporativas: las comunicaciones de empleado a empleado suelen ser una fuente de infracciones involuntarias o malintencionadas de las directivas corporativas. Estas infracciones pueden incluir el lenguaje ofensivo, las amenazas y el ciberacoso entre empleados. Este tipo de actividad contribuye a un ambiente de trabajo hostil y puede resultar en acciones legales tanto contra los empleados como contra la organización en general. La administración de riesgo interno utiliza nuevos clasificadores integrados de Microsoft 365 y la plantilla de la directiva [Lenguaje ofensivo en el correo electrónico](#).

## Administrar el cumplimiento de comunicaciones

El cumplimiento de comunicaciones forma parte de la nueva solución de riesgo interno establecida en Microsoft 365 que ayuda a minimizar los riesgos de comunicación al ayudarle a detectar y capturar mensajes inapropiados en su organización, y tomar medidas de corrección para ellos. Las directivas predefinidas y personalizadas le permiten escanear las comunicaciones internas y externas en busca de coincidencias de directivas para que puedan ser examinadas por revisores designados. Los revisores pueden investigar los correos electrónicos escaneados, Microsoft Teams, Yammer o las comunicaciones con terceros de su organización y tomar las acciones de corrección adecuadas para asegurarse de que cumplen con los estándares de mensajes de su organización.

Las directivas de cumplimiento de comunicaciones en Microsoft 365 lo ayudan a superar muchos desafíos modernos asociados con el cumplimiento y las comunicaciones internas y externas, que incluyen:

- Exploración de tipos de canales de comunicación en aumento.
- El volumen creciente de datos de mensajes.
- Cumplimiento normativo y riesgo de multas

Como puede ver, el Cumplimiento de comunicaciones es una herramienta poderosa que puede ayudar a supervisar y detectar comunicaciones anómalas e indeseables entre su personal o entre su personal y terceros. El cumplimiento de las comunicaciones no está habilitado de forma predeterminada y se puede encontrar en el catálogo de soluciones, en Administración de riesgo interno.

Una vez habilitado, puede utilizar el aprendizaje automático avanzado para realizar un seguimiento de los correos electrónicos y las conversaciones del equipo en busca de sentimientos de mensajes inapropiados, blasfemias, currículos, código fuente, acoso dirigido y amenazas. Además, puede utilizarlo para identificar casos de uso indebido de información privilegiada al buscar detalles de la cuenta, valores monetarios y detalles de la cuenta bancaria o de crédito.

Cumplimiento de comunicaciones es una herramienta potente que puede ayudar a mantener y proteger a su personal, sus datos y su organización.

## Restringir las comunicaciones con barreras de información

Los servicios en la nube de Microsoft incluyen potentes capacidades de comunicación y colaboración. Sin embargo, es posible que las empresas quieran restringir las comunicaciones entre dos grupos para evitar que ocurra un conflicto de intereses en su organización o restringir las comunicaciones entre ciertas personas para salvaguardar la información interna. Con las barreras de información, Microsoft 365 permite a las empresas restringir las comunicaciones entre grupos específicos de usuarios cuando sea necesario.

Las barreras de información (IB) son directivas que un administrador puede configurar para evitar que las personas o los grupos se comuniquen entre sí. Cuando existen directivas de barrera de información, las personas que no deberían comunicarse con otros usuarios específicos no podrán encontrar, seleccionar, chatear o llamar a esos usuarios. Con las barreras de información, se realizan controles para evitar comunicaciones no autorizadas.

### Escenarios

La necesidad de barreras de información puede aplicarse a diferentes segmentos y sectores empresariales. Algunas situaciones comunes son:

- Servicios financieros: Un impulsor principal de las barreras de información, la Autoridad Reguladora del Sector Financiero (FINRA) repasa las barreras de información y los conflictos de interés dentro de las empresas miembro y ofrece orientación sobre cómo administrar dichos conflictos.
- Educación: Los alumnos de una escuela no pueden buscar los datos de contacto de los alumnos de otros centros educativos.
- Aviso legal: Mantener la confidencialidad de los datos obtenidos por el abogado de un cliente para que no acceda a ellos un abogado de la misma firma que representa a un cliente diferente.
- Gobierno: El acceso a la información y el control de esta son limitados entre departamentos y grupos
- Servicios profesionales: Un grupo de personas en una compañía solo puede chatear con un cliente o un cliente específico a través de una federación o acceso de invitado durante una interacción con el cliente.

### Barreras de información en Teams

Inicialmente, las barreras de información se aplican solo a los chats y canales de Microsoft Teams. En Microsoft Teams, las directivas de barrera de información determinan y previenen los siguientes tipos de comunicaciones no autorizadas:

- Buscar a un usuario
- Agregar un miembro a un equipo
- Iniciar una sesión de chat con alguien

- Iniciar un chat de grupo
- Invitar a alguien a unirse a una reunión
- Compartir una pantalla
- Hacer una llamada

Si las personas involucradas están incluidas en una directiva de barrera de información para prevenir la actividad, no podrán continuar. Para más información, consulte [Barreras de información en Microsoft Teams](#).

## Controlar el acceso de administrador privilegiado

Privileged Access Management permite un control de acceso granular sobre las tareas de administración privilegiadas en Microsoft 365. Puede proteger a su organización de las infracciones que utilizan cuentas de administrador privilegiadas existentes con acceso permanente a datos confidenciales o acceso a configuraciones críticas.

Habilitar Privileged Access Management en Microsoft 365 permite que su organización opere con un **acceso de cero permanencia**; esto significa que los usuarios que necesitan acceso privilegiado deben solicitar permisos de acceso y que, una vez recibido, es un acceso en el momento y que otorga el tiempo suficiente para realizar el trabajo en cuestión. El acceso de cero permanencia aporta una capa de defensa contra las vulnerabilidades del acceso administrativo permanente.

Privileged Access Management requiere que los usuarios soliciten acceso en el momento para completar tareas elevadas y privilegiadas a través de un flujo de trabajo de aprobación de gran alcance y con un límite de tiempo.

En un nivel alto, los pasos para configurar y usar el acceso privilegiado son:

1. Crear un grupo de aprobadores: antes de comenzar a utilizar el acceso con privilegios, determine quién necesita autoridad de aprobación para las solicitudes entrantes de acceso a tareas elevadas y privilegiadas. Cualquier usuario que forme parte del grupo de aprobadores puede aprobar solicitudes de acceso.
2. Habilitar el acceso privilegiado: el acceso privilegiado debe habilitarse explícitamente en Office 365 con el grupo de aprobadores predeterminado, incluido un conjunto de cuentas del sistema que desea excluir del control de acceso de Privileged Access Management.
3. Crear una directiva de acceso: la creación de una directiva de aprobación le permite definir los requisitos de aprobación específicos dentro del ámbito de las tareas individuales.
4. Enviar y aprobar solicitudes de acceso privilegiado: una vez habilitado, el acceso privilegiado requiere aprobaciones para cualquier tarea que tenga definida una directiva de aprobación asociada. Para las tareas incluidas en una directiva de aprobación, los usuarios deben solicitar y obtener la aprobación de acceso para tener los permisos necesarios para ejecutar la tarea.

Una vez concedida la aprobación, el usuario solicitante puede ejecutar la tarea prevista y el acceso con privilegios autorizará y ejecutará la tarea en su nombre. La aprobación sigue siendo válida durante la duración solicitada (la duración predeterminada es de 4

horas), durante las cuales el solicitante puede ejecutar la tarea prevista varias veces. Todas estas ejecuciones se registran y están disponibles para auditorías de seguridad y cumplimiento.

## Aumentar el control con Caja de seguridad del cliente

La Caja de seguridad del cliente admite solicitudes para acceder a datos en Exchange Online, SharePoint Online y OneDrive para la Empresa. La Caja de seguridad del cliente garantiza que Microsoft no pueda acceder a su contenido para realizar una operación de servicio sin su aprobación explícita. La Caja de seguridad del cliente lo lleva al flujo de trabajo de aprobación de solicitudes para acceder a su contenido.

De vez en cuando, los ingenieros de Microsoft ayudan en la solución de problemas y corrigen los problemas informados por los clientes en el proceso de soporte técnico. Por lo general, los problemas se solucionan a través de amplias herramientas de depuración y telemetría que Microsoft tiene implementadas para sus servicios. Sin embargo, algunos casos requieren que un ingeniero de Microsoft acceda al contenido del cliente para determinar la causa y solucionar el problema. La Caja de seguridad del cliente requiere que el ingeniero solicite acceso al cliente como paso final en el flujo de trabajo de aprobación. Lo que da a las organizaciones la opción de aprobar o rechazar estas solicitudes y aportar control de acceso directo al cliente.

## Flujo de trabajo de la Caja de seguridad del cliente

Los siguientes pasos describen el flujo de trabajo típico cuando un ingeniero de Microsoft inicia una solicitud de Caja de seguridad del cliente:

1. Alguien en una organización experimenta un problema con su buzón de correo electrónico de Microsoft 365. Una vez que el usuario utiliza la solución de problemas pero no logra corregirlo, abre una solicitud de soporte técnico con el Soporte técnico de Microsoft.
2. Un ingeniero de soporte técnico de Microsoft revisa la solicitud de servicio y determina la necesidad de acceder al inquilino de la organización para reparar el problema en Exchange Online.
3. El ingeniero de soporte técnico de Microsoft inicia sesión en la herramienta de solicitud de Caja de seguridad del cliente y realiza una solicitud de acceso a datos que incluye el nombre del inquilino de la organización, el número de solicitud de servicio y el tiempo estimado que el ingeniero necesita acceder a los datos.
4. Una vez que un administrador de soporte técnico de Microsoft aprueba la solicitud, la Caja de seguridad del cliente envía al aprobador designado en la organización una notificación por correo electrónico sobre la solicitud de acceso pendiente de Microsoft.
5. El aprobador inicia sesión en el Centro de administración de Microsoft 365 y aprueba la solicitud. Este paso desencadena la creación de un registro de auditoría disponible al buscar en el registro de auditoría. Si el cliente rechaza la solicitud o no la aprueba dentro de las 12 horas, la solicitud caduca y no se concede acceso al ingeniero de Microsoft.
6. Una vez que el aprobador de la organización aprueba la solicitud, el ingeniero de Microsoft recibe el mensaje de aprobación, inicia sesión en el

inquilino en Exchange Online y corrige el problema del cliente. Los ingenieros de Microsoft tienen la duración solicitada para solucionar el problema, después de lo cual el acceso se revoca automáticamente.



Todas las acciones realizadas por un ingeniero de Microsoft se registran en el registro de auditoría. Puede buscar y repasar estos registros de auditoría.

## Investigar con Auditoría avanzada

La auditoría avanzada en Microsoft 365 aporta nuevas capacidades de auditoría que pueden ayudar a su organización con investigaciones forenses y de cumplimiento.

**Nota:** Auditoría avanzada está disponible para organizaciones con una suscripción a Microsoft 365 Enterprise E5. Además, se puede asignar una licencia complementaria de Cumplimiento de Microsoft 365 E5 a los usuarios cuando se requiera una licencia por usuario para las características de auditoría avanzada, como es el caso de la retención a largo plazo de los registros de auditoría y el acceso a eventos cruciales para las investigaciones.

Auditoría avanzada incluye estas capacidades:

- Retención a largo plazo de los registros de auditoría: Auditoría avanzada conserva todos los registros de auditoría de Exchange, SharePoint y Azure Active Directory durante un año. Esto se logra mediante una directiva de retención de registros de auditoría predeterminada que retiene cualquier registro de auditoría que contenga el valor de **Exchange**, **SharePoint** o **AzureActiveDirectory** para la propiedad **Carga de trabajo**.
- Directivas de retención de registros de auditoría: todos los registros de auditoría generados en otros servicios que no están cubiertos por la directiva de retención de registros de auditoría predeterminada se conservan durante 90 días. Sin embargo, ahora puede crear directivas de retención de registros de auditoría personalizadas para conservar otros registros de auditoría hasta por un año.
- Acceso a eventos cruciales para las investigaciones: el primer evento crucial que vamos a publicar es la acción de auditoría del buzón *MailItemsAccessed*. Esta acción se activa cuando los protocolos y clientes de correo electrónico acceden a los datos de correo. La acción *MailItemsAccessed* puede ayudar a los investigadores a identificar filtraciones de datos y determinar el alcance de los mensajes que pueden haberse visto en peligro.
- Acceso de ancho de banda elevado a la API de Actividad de administración de Office 365: con el lanzamiento de Auditoría avanzada, cada organización

obtendrá su propia cuota de ancho de banda totalmente asignada para acceder a sus datos de auditoría.

## Administrar el cumplimiento y las investigaciones legales con eDiscovery avanzado

La solución de eDiscovery avanzado de Microsoft aporta un flujo de trabajo de un extremo a otro para preservar, recopilar, revisar, analizar y exportar contenido que responde a las investigaciones internas y externas de su organización. También permite a los equipos legales administrar todo el flujo de trabajo de notificación de suspensión legal para comunicarse con los custodios involucrados en un caso.

El flujo de trabajo integrado de eDiscovery avanzado se alinea con el proceso de eDiscovery descrito por el modelo de referencia de descubrimiento electrónico (EDRM), que aporta recursos globales prácticos para mejorar el eDiscovery, la privacidad, la seguridad y el gobierno de información.

En un nivel alto, así es como eDiscovery avanzado admite el flujo de trabajo de EDRM:

- **Identificación.** Después de identificar a las potenciales personas de interés en una investigación, puede agregarlas como custodios (también llamado *custodios de datos*, porque pueden poseer información que sea relevante para la investigación) a un caso de eDiscovery avanzado. Una vez que los usuarios se agregan como custodios, es fácil conservar, recopilar y repasar los documentos de custodia.
- **Conservación.** Para conservar y proteger los datos que son relevantes para una investigación, eDiscovery avanzado le permite aplicar una suspensión legal a las fuentes de datos asociadas con los custodios en un caso. También puede poner en suspensión los datos que no son de custodia. eDiscovery avanzado tiene también un flujo de trabajo de comunicaciones integrado para que pueda enviar notificaciones de suspensión legal a los custodios y realizar un seguimiento de sus reconocimientos.
- **Recopilación.** Una vez que haya identificado (y conservado) los orígenes de datos relevantes para la investigación, puede utilizar la herramienta de búsqueda incorporada en la búsqueda de eDiscovery avanzado y recopilar datos en directo de los orígenes de datos de custodia (y de los orígenes de datos sin custodia, si corresponde) que puedan ser relevantes para el caso.
- **Procesamiento.** Una vez que haya recopilado todos los datos relevantes para el caso, el siguiente paso es procesarlos para su posterior revisión y análisis. En eDiscovery avanzado, los datos locales que identificó en la fase de recopilación se copian en una ubicación de Azure Storage (denominada *conjunto de revisión*), que le proporciona una vista estática de los datos del caso.
- **Revisión.** Una vez que se han agregado datos a un conjunto de revisión, puede ver documentos específicos y ejecutar otras consultas para reducir los datos a lo más relevante para el caso. Además, puede anotar y etiquetar documentos específicos.
- **Análisis.** eDiscovery avanzado aporta una herramienta de análisis integrada que ayuda a eliminar datos del conjunto de revisión que usted determine que

no son relevantes para la investigación. Además de reducir el volumen de datos relevantes, eDiscovery avanzado también le ayuda a ahorrar en costes de inspección por motivos legales al permitirle organizar el contenido para que el proceso de inspección sea más fácil y eficiente.

- **Producción y presentación.** Cuando haya terminado, puede exportar documentos de un conjunto de revisión para la revisión legal. Puede exportar documentos en su formato nativo o en un formato especificado por EDRM para que se puedan importar a aplicaciones de revisión de terceros.

## Prueba de conocimientos

Elija la mejor respuesta para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

¿Cuáles son las fases del flujo de trabajo de administración de riesgo interno en Microsoft 365?

- A. Directiva, alertas, evaluación de prioridades, investigación y acción
- B. Escanear, modificar y eliminar
- C. Descubrir, clasificar y explorar

¿Cómo se define el acceso permanente cero?

- A. No se obtienen permisos de seguridad de forma predeterminada
- B. Acceso en función del rol
- C. Acceso otorgado por privilegio

¿Qué son las barreras de información (IB)?

- A. Firewalls entre su organización e Internet
- B. Directivas que un administrador puede configurar para evitar que individuos o grupos se comuniquen entre sí
- C. Filtros para evitar el correo no deseado