



# Microsoft 365 Fundamentals

Exam Ref MS-900

Craig Zacker

# Contenido

1) Portada

2) Pagina del titulo

3) La página de derechos de autor

4) Contenido de un vistazo

5) Contenido

6) Introducción

1) Organización de este libro.

2) Certificaciones de Microsoft

3) Erratas, actualizaciones y soporte de libros

4) Mantente en contacto

7) Importante: cómo usar este libro para estudiar para el examen

8) Sobre el Autor

9) Capítulo 1. Comprender los conceptos de la nube

1) Habilidad 1.1: Detallar y comprender los beneficios y

consideraciones sobre el uso de servicios en la nube

2) Habilidad 1.2: Comprender los diferentes tipos de servicios en la nube

disponible

3) Resumen

4) Experimento mental

5) Respuesta de experimento de pensamiento

10) Capítulo 2. Comprender los servicios principales de Microsoft 365 y

conceptos

1) Habilidad 2.1: Describir los componentes principales de Microsoft 365

2) Habilidad 2.2: Compare los servicios principales en Microsoft 365 con  
servicios locales correspondientes

3) Habilidad 2.3: Comprender el concepto de gestión moderna

- 4) **Habilidad 2.4: Comprender Office 365 ProPlus**
- 5) **Habilidad 2.5: Comprender la colaboración y la movilidad con Microsoft 365**
- 6) **Habilidad 2.6: Describir las capacidades de análisis en Microsoft 365**
- 7) **Resumen**
- 8) **Experimento mental**
- 9) **Respuesta de experimento de pensamiento**
- 11) **Capítulo 3. Comprender la seguridad, el cumplimiento, la privacidad y confiar en Microsoft 365**
- 1) **Habilidad 3.1: Comprender los conceptos de seguridad y cumplimiento con Microsoft 365**
- 2) **Habilidad 3.2: Comprender la protección de identidad y administración**
- 3) **Habilidad 3.3: Comprender la necesidad de un punto final unificado gestión, escenarios de uso de seguridad y servicios**
- 4) **Habilidad 3.4: Comprender el Portal de confianza del servicio y Gerente de Cumplimiento**
- 5) **Resumen**
- 6) **Experimento mental**
- 7) **Respuesta de experimento de pensamiento**
- 12) **Capítulo 4. Comprenda los precios y el soporte de Microsoft 365**
- 1) **Habilidad 4.1: Comprender las opciones de licencia disponibles en Microsoft 365**
- 2) **Habilidad 4.2: planificar, predecir y comparar precios**
- 3) **Habilidad 4.3: Describir las ofertas de soporte para Microsoft 365 servicios**
- 4) **Habilidad 4.4: Comprender el ciclo de vida del servicio en Microsoft 365**
- 5) **Resumen**
- 6) **Experimento mental**
- 7) **Respuesta de experimento de pensamiento**
- 13) **Índice**
- 14) **Fragmentos de código**

1) yo \_\_\_\_\_

2) ii \_\_\_\_\_

3) iii \_\_\_\_\_

4) iv \_\_\_\_\_

5) v \_\_\_\_\_

6) vi \_\_\_\_\_

7) vii \_\_\_\_\_

8) viii \_\_\_\_\_

9) ix \_\_\_\_\_

10) X \_\_\_\_\_

11) xi \_\_\_\_\_

12) xii \_\_\_\_\_

13) xiii \_\_\_\_\_

14) xiv \_\_\_\_\_

15. xv \_\_\_\_\_

dieciséis. xvi \_\_\_\_\_

17) 1 \_\_\_\_\_

18) 2 \_\_\_\_\_

19) 3 \_\_\_\_\_

20) 4 4 \_\_\_\_\_

21) 5 5 \_\_\_\_\_

22) 6 6 \_\_\_\_\_

23) 7 7 \_\_\_\_\_

24) 8 \_\_\_\_\_

25) 9 \_\_\_\_\_

26) 10 \_\_\_\_\_

27) 11 \_\_\_\_\_

28) 12 \_\_\_\_\_

29) 13 \_\_\_\_\_

30) 14 \_\_\_\_\_

31) 15 \_\_\_\_\_

32) dieciséis \_\_\_\_\_

33) 17 \_\_\_\_\_

34) 18 años \_\_\_\_\_

35) 19 \_\_\_\_\_

36) 20 \_\_\_\_\_

**37) 21** \_\_\_\_\_

**38) 22** \_\_\_\_\_

**39) 23** \_\_\_\_\_

**40) 24** \_\_\_\_\_

**41) 25** \_\_\_\_\_

**42) 26** \_\_\_\_\_

**43) 27** \_\_\_\_\_

**44) 28** \_\_\_\_\_

**45) 29** \_\_\_\_\_

**46) 30** \_\_\_\_\_

**47) 31** \_\_\_\_\_

**48) 32** \_\_\_\_\_

**49) 33** \_\_\_\_\_

**50 34** \_\_\_\_\_

**51) 35** \_\_\_\_\_

**52) 36** \_\_\_\_\_

**53) 37** \_\_\_\_\_

**54) 38** \_\_\_\_\_

**55) 39** \_\_\_\_\_

**56) 40** \_\_\_\_\_

**57) 41** \_\_\_\_\_

**58) 42** \_\_\_\_\_

**59) 43** \_\_\_\_\_

**60 44** \_\_\_\_\_

**61) 45** \_\_\_\_\_

**62) 46** \_\_\_\_\_

**63) 47** \_\_\_\_\_

**64) 48** \_\_\_\_\_

**sesenta y cinco. 49**

**66 50** \_\_\_\_\_

**67) 51** \_\_\_\_\_

**68) 52** \_\_\_\_\_

**69) 53** \_\_\_\_\_

**70) 54** \_\_\_\_\_

**71) 55** \_\_\_\_\_

**72) 56** \_\_\_\_\_

73) 57 \_\_\_\_.

74) 58 \_\_\_\_.

75) 59 \_\_\_\_.

76) 60 60 \_\_\_\_.

77) 61 \_\_\_\_.

78) 62 \_\_\_\_.

79) 63 \_\_\_\_.

80 64 \_\_\_\_.

81) sesenta y cinco

82) 66 \_\_\_\_.

83) 67 \_\_\_\_.

84) 68 \_\_\_\_.

85) 69 \_\_\_\_.

86) 70 \_\_\_\_.

87) 71 \_\_\_\_.

88) 72 \_\_\_\_.

89) 73 \_\_\_\_.

90 74 \_\_\_\_.

91) 75 \_\_\_\_.

92) 76 \_\_\_\_.

93) 77 \_\_\_\_.

94) 78 \_\_\_\_.

95) 79 \_\_\_\_.

96) 80 \_\_\_\_.

97) 81 \_\_\_\_.

98) 82 \_\_\_\_.

99 83 \_\_\_\_.

100 84 \_\_\_\_.

101) 85 \_\_\_\_.

102 86 \_\_\_\_.

103) 87 \_\_\_\_.

104) 88 \_\_\_\_.

105) 89 \_\_\_\_.

106) 90 \_\_\_\_.

107) 91 91 \_\_\_\_.

108) 92 \_\_\_\_.

**109** **93** \_\_\_\_\_.

**110** **94** \_\_\_\_\_.

**111)** **95** \_\_\_\_\_.

**112** **96** \_\_\_\_\_.

**113)** **97** \_\_\_\_\_.

**114)** **98** \_\_\_\_\_.

**115)** **99** \_\_\_\_\_.

**116)** **100** \_\_\_\_\_.

**117)** **101** \_\_\_\_\_.

**118)** **102** \_\_\_\_\_.

**119)** **103** \_\_\_\_\_.

**120** **104** \_\_\_\_\_.

**121)** **105** \_\_\_\_\_.

**122)** **106** \_\_\_\_\_.

**123** **107** \_\_\_\_\_.

**124)** **108** \_\_\_\_\_.

**125** **109** \_\_\_\_\_.

**126)** **110** \_\_\_\_\_.

**127)** **111** \_\_\_\_\_.

**128** **112** \_\_\_\_\_.

**129)** **113** \_\_\_\_\_.

**130** **114** \_\_\_\_\_.

**131** **115** \_\_\_\_\_.

**132)** **116** \_\_\_\_\_.

**133)** **117** \_\_\_\_\_.

**134)** **118** \_\_\_\_\_.

**135)** **119** \_\_\_\_\_.

**136)** **120** \_\_\_\_\_.

**137)** **121** \_\_\_\_\_.

**138** **122** \_\_\_\_\_.

**139.** **123** \_\_\_\_\_.

**140** **124** \_\_\_\_\_.

**141** **125** \_\_\_\_\_.

**142** **126** \_\_\_\_\_.

**143)** **127** \_\_\_\_\_.

**144)** **128** \_\_\_\_\_.

145. 129 129

146. 130

147 131

148 132

149 133

150 134

151) 135

152) 136

153 137

154. 138

155 139

156) 140

157. 141

158. 142

159. 143

160 144

161. 145

162 146

163 147

164 148

165. 149

166. 150

167. 151

168 152

169 153

170 154

171 155

172) 156

173 157

174) 158

175 159

176 160

177. 161

178) 162

179. 163

180 164

**181. 165** \_\_\_\_\_  
**182 166** \_\_\_\_\_  
**183 167** \_\_\_\_\_  
**184 168** \_\_\_\_\_  
**185 169** \_\_\_\_\_  
**186 170** \_\_\_\_\_  
**187 171** \_\_\_\_\_  
**188. 172** \_\_\_\_\_  
**189 173** \_\_\_\_\_  
**190 174** \_\_\_\_\_  
**191 175** \_\_\_\_\_  
**192. 176** \_\_\_\_\_  
**193 177** \_\_\_\_\_  
**194. 178** \_\_\_\_\_  
**195. 179** \_\_\_\_\_  
**196 180** \_\_\_\_\_  
**197 181** \_\_\_\_\_  
**198. 182** \_\_\_\_\_  
**199 183** \_\_\_\_\_  
**200 184** \_\_\_\_\_  
**201 185** \_\_\_\_\_  
**202. 186** \_\_\_\_\_  
**203. 187** \_\_\_\_\_  
**204 188** \_\_\_\_\_  
**205. 189** \_\_\_\_\_  
**206 190** \_\_\_\_\_  
**207. 191** \_\_\_\_\_  
**208. 192** \_\_\_\_\_  
**209. 193** \_\_\_\_\_  
**210 194** \_\_\_\_\_  
**211 195** \_\_\_\_\_  
**212 196** \_\_\_\_\_  
**213 197** \_\_\_\_\_  
**214 198** \_\_\_\_\_  
**215. 199** \_\_\_\_\_  
**216 200** \_\_\_\_\_

**217** **201** \_\_\_\_.  
**218** **202** \_\_\_\_.  
**219** **203** \_\_\_\_.  
**220** **204** **204** \_\_\_\_.  
**221.** **205** \_\_\_\_.  
**222** **206** \_\_\_\_.  
**223.** **207** \_\_\_\_.  
**224** **208** \_\_\_\_.  
**225** **209** \_\_\_\_.  
**226.** **210** \_\_\_\_.  
**227.** **211** \_\_\_\_.  
**228** **212** \_\_\_\_.  
**229.** **213** \_\_\_\_.  
**230.** **214** \_\_\_\_.  
**231.** **215** \_\_\_\_.  
**232.** **216** \_\_\_\_.  
**233.** **217** \_\_\_\_.  
**234.** **218** \_\_\_\_.  
**235.** **219** \_\_\_\_.  
**236.** **220** \_\_\_\_.  
**237.** **221** \_\_\_\_.  
**238.** **222** \_\_\_\_.  
**239.** **223** \_\_\_\_.  
**240** **224** \_\_\_\_.

**Examen Ref MS-900**

**Fundamentos de**

**Microsoft 365**

**Craig Zacker**



# **Examen Ref MS-900 Fundamentos de Microsoft 365**

Publicado con la autorización de Microsoft Corporation por Pearson Education, Inc.

Copyright © 2020 por Pearson Education, Inc.

Todos los derechos reservados. Esta publicación está protegida por derechos de autor y se debe obtener el permiso del editor antes de cualquier reproducción prohibida, almacenamiento en un sistema de recuperación o transmisión en cualquier forma o por cualquier medio, electrónico, mecánico, fotocopiado, grabación o similar. Para obtener información sobre permisos, formularios de solicitud y los contactos apropiados dentro del Departamento de Derechos y Permisos Globales de Pearson Education, visite [www.pearson.com/permissions/](http://www.pearson.com/permissions/).

No se asume ninguna responsabilidad de patente con respecto al uso de la información aquí contenida.

Aunque se han tomado todas las precauciones en la preparación de este libro, el editor y el autor no asumen ninguna responsabilidad por errores u omisiones. Tampoco se asume ninguna responsabilidad por daños resultantes del uso de la información aquí contenida. ISBN-13: 978-0-13-648487-5 ISBN-10: 0-13-648487-5

Número de control de la Biblioteca del Congreso: 2019956209

ScoutAutomatedPrintCode

## **MARCAS COMERCIALES**

Microsoft y las marcas registradas enumeradas en <http://www.microsoft.com> en la página web "Marcas comerciales" son marcas comerciales del grupo de empresas Microsoft. Todas las demás marcas son propiedad de sus respectivos dueños.

## **ADVERTENCIA Y DESCARGO DE RESPONSABILIDAD**

Se ha hecho todo lo posible para que este libro sea lo más completo y preciso posible, pero no se implica ninguna garantía o idoneidad. La información proporcionada

está en una base "tal cual". El autor, el editor y Microsoft Corporation no tendrán responsabilidad ni responsabilidad ante ninguna persona o entidad con respecto a cualquier pérdida o daño que surja de la información contenida en este libro.

## VENTAS ESPECIALES

Para obtener información sobre la compra de este título en grandes cantidades o para oportunidades de ventas especiales (que pueden incluir versiones electrónicas, diseños de portadas personalizadas y contenido específico para su negocio, objetivos de capacitación, enfoque de marketing o intereses de marca), comuníquese con nuestro departamento de ventas corporativo. a

[corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) o (800) 382-3419. Para consultas de

ventas del gobierno, comuníquese con

[governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

Para preguntas sobre ventas fuera de los EE. UU., Comuníquese con

[intlcs@pearson.com](mailto:intlcs@pearson.com).

## CRÉDITOS

EDITOR EN JEFE Brett

Bartow

EDITOR EJECUTIVO Loretta

Yates

ASISTENTE EDITOR PATROCINADOR Charvi

Arora

EDITOR DE DESARROLLO Rick

Kughen

EDITOR DIRECTIVO Sandra

Schroeder

EDITOR DE PROYECTO MAYOR Tracey

Croom EDITOR DE COPIA Rick Kughen

INDEXADOR

Erika Millen CORRECTOR

Charlotte Kughen EDITOR

TÉCNICO

J. Boyd Nolan

ASISTENTE EDITORIAL Cindy

Teeters

DISEÑADOR DE CUBIERTA

Twist Creative, código de

COMPOSICIÓN SeattleMantra

# Contenido de un vistazo

*Introducción*

*Importante: cómo usar este libro para estudiar para el  
examen*

**CAPÍTULO 1 Comprender los conceptos de la nube**

**CAPÍTULO 2 Comprender los servicios principales de Microsoft 365  
y conceptos**

**CAPÍTULO 3 Comprender la seguridad, el cumplimiento,  
privacidad y confianza en Microsoft 365**

**CAPÍTULO 4 Comprender los precios de Microsoft 365 y  
apoyo**

*Índice*

# Contenido

## Introducción

*Organización de este libro Certificaciones de*

*Microsoft Erratas, actualizaciones y soporte de libros*

*Manténgase en contacto*

## Importante: Cómo usar este libro para

**estudia para el examen**

## Capítulo 1 Comprender los conceptos de la nube

Habilidad 1.1: detallar y comprender los beneficios

y consideraciones sobre el uso de servicios en la nube

Comprender los servicios en la nube Ventajas de la

computación en la nube Habilidad 1.2: Comprender los

diferentes tipos de

servicios en la nube disponibles

Arquitecturas en la nube Modelos

de servicios en la nube

## Resumen

Experimento de pensamiento Respuesta de

experimento de pensamiento

## Capítulo 2 Comprender el núcleo de Microsoft 365

### servicios y conceptos

Habilidad 2.1: Describir el núcleo de Microsoft 365

componentes

Windows 10 Enterprise

Exchange Online SharePoint

Online Equipo de Microsoft

Enterprise Mobility + Security Skill 2.2: Compare los

servicios principales en Microsoft

365 con los servicios locales correspondientes

Costo de

actualizaciones de

implementación

Administración de

seguridad

Servicio de comparaciones

Habilidad 2.3: Comprender el concepto de moderno

administración

Transición a la administración moderna Windows como  
servicio Uso de los portales de Microsoft 365  
Comprendión del modelo de implementación y  
lanzamiento de Microsoft Habilidad 2.4: Comprenda  
Office 365 ProPlus

---

Comparación de Office 365 ProPlus con Office  
local Implementación de Office

---

Habilidad 2.5: Comprender la colaboración y  
movilidad con Microsoft 365

Herramientas de colaboración de Microsoft 365  
Colaborando en la movilidad de Microsoft 365  
Enterprise

Habilidad 2.6: Describir las capacidades analíticas en  
Microsoft 365

Microsoft Advanced Threat Analytics Microsoft  
365 Usage Analytics MyAnalytics Workplace  
Analytics Resumen

---

Experimento de pensamiento Respuesta de  
experimento de pensamiento

## **Capítulo 3 Comprender la seguridad, el cumplimiento,**

### **privacidad y confianza en Microsoft 365**

Habilidad 3.1: Comprender la seguridad y

conceptos de cumplimiento con Microsoft 365

Gestión de riesgos Pilares

clave de seguridad

Habilidad 3.2: Comprender la protección de identidad y

administración

Identidad Autenticación

Protección de documentos

Habilidad 3.3: Comprender la necesidad de unificar

gestión de puntos finales, escenarios de uso de

seguridad y servicios

Microsoft 365 y Directory Services SCCM e Intune

cogestión Escenarios de uso de seguridad Abordar

amenazas comunes Habilidad 3.4: Comprender el

Portal de Service Trust

y gerente de cumplimiento

Service Trust Portal Compliance

Manager Adopción en la nube

showstoppers Resumen

Experimento de pensamiento Respuesta de

experimento de pensamiento

## Capítulo 4 Comprender los precios de Microsoft 365 y

apoyo

Habilidad 4.1: Comprender las opciones de licencia

disponible en Microsoft 365

Suscripciones a Microsoft 365 Venta de licencias de

Microsoft 365 Microsoft 365 Implementación de mejores

prácticas Habilidad 4.2: Planificar, predecir y comparar

precios

Análisis de costo-beneficio para redes en la nube versus

redes locales Licencias por volumen Facturación y

administración de facturas Habilidad 4.3: Describa las ofertas

de soporte para

Servicios de Microsoft 365

Acuerdos de nivel de servicio Crear solicitudes de

soporte Determinar el estado del servicio Habilidad 4.4:

Comprender el ciclo de vida del servicio en

Resumen de

Microsoft 365

Experimento de pensamiento Respuesta de

experimento de pensamiento

*Índice*

# Introducción

---

La certificación Microsoft 365 Certified Fundamentals es el punto de entrada inicial en una jerarquía de certificaciones de Microsoft 365. El examen MS-900 Microsoft 365 Fundamentals prueba el conocimiento del candidato de los componentes y capacidades de los productos Microsoft 365 sin profundizar en procedimientos administrativos específicos. Con la certificación de Fundamentos establecida, los profesionales de TI pueden pasar a las certificaciones de nivel Asociado que se concentran en áreas específicas de la administración de Microsoft 365, como mensajería, seguridad, escritorio y trabajo en equipo. El pináculo supremo en la jerarquía es la certificación de Expertos del Administrador de la empresa, que se puede lograr aprobando los exámenes MS-100 y MS101.

Este libro cubre todas las habilidades medidas por el examen MS900, con cada una de las cuatro áreas principales cubiertas en un capítulo separado. Cada capítulo se divide en secciones de habilidades individuales, que cubren todos los temas sugeridos para cada habilidad. Se recomienda que acceda a una versión de prueba de Microsoft 365 mientras trabaja a su manera

a través de este libro. Nada puede reemplazar la experiencia práctica real, y Microsoft proporciona una plataforma de evaluación totalmente funcional de Microsoft 365 Enterprise, cuyos componentes son accesibles en la nube y no requieren otro hardware que no sea una computadora con acceso a Internet. Microsoft también proporciona una gran cantidad de documentación para todos los componentes de Microsoft 365 en

[docs.microsoft.com](https://docs.microsoft.com) . Con estas herramientas, además de algo de tiempo y dedicación, puede prepararse para el examen MS-900 y el primer paso hacia su carrera en Microsoft 365.

## ORGANIZACIÓN DE ESTE LIBRO

---

Este libro está organizado por la lista "Habilidades medidas" publicada para el examen. La lista "Habilidades medidas" está disponible para cada examen en el sitio web de Microsoft Learn:

[http://microsoft.com/learn](https://microsoft.com/learn) . Cada capítulo de este libro corresponde a un área temática principal en la lista, y las tareas técnicas en cada área temática determinan la organización de un capítulo. Si un examen cubre cuatro áreas temáticas principales, por ejemplo, el libro contendrá cuatro capítulos.

## CERTIFICACIONES DE MICROSOFT

---

Las certificaciones de Microsoft lo distinguen al demostrar su dominio de un amplio conjunto de habilidades y experiencia con

Productos y tecnologías actuales de Microsoft. Los exámenes y las certificaciones correspondientes se desarrollan para validar su dominio de las competencias críticas a medida que diseña y desarrolla, o implementa y respalda, soluciones con productos y tecnologías de Microsoft tanto en las instalaciones como en la nube. La certificación brinda una variedad de beneficios para el individuo y para los empleadores y las organizaciones.

**Más información: Todas las certificaciones de Microsoft**

Para obtener información sobre las certificaciones de Microsoft, incluida una lista completa de certificaciones disponibles, vaya a  
<http://www.microsoft.com/learn>.

## **ERRATA, ACTUALIZACIONES Y RESERVA DE APOYO**

---

Hemos hecho todo lo posible para garantizar la precisión de este libro y su contenido complementario. Puede acceder a las actualizaciones de este libro, en forma de una lista de erratas enviadas y sus correcciones relacionadas, en:

[MicrosoftPressStore.com/ExamRefMS900/errata](http://MicrosoftPressStore.com/ExamRefMS900/errata)

---

Si descubre un error que aún no figura en la lista, envíenoslo en la misma página.

Para obtener asistencia e información adicional sobre libros, por favor

visitar [\*http://www.MicrosoftPressStore.com/Support\*](http://www.MicrosoftPressStore.com/Support).

---

Tenga en cuenta que el soporte del producto para el software y hardware de Microsoft no se ofrece a través de las direcciones anteriores. Para obtener ayuda con el software o hardware de Microsoft, vaya a [\*http://support.microsoft.com\*](http://support.microsoft.com).

---

## MANTENTE EN CONTACTO

---

¡Sigamos con la conversación! Estamos en Twitter

[\*http://twitter.com/MicrosoftPress\*](http://twitter.com/MicrosoftPress).

---

# **Importante: cómo usar este libro para estudiar para el examen**

Los exámenes de certificación validan su experiencia en el trabajo y conocimiento del producto. Para evaluar su preparación para tomar un examen, use esta Referencia del examen para ayudarlo a verificar su comprensión de las habilidades evaluadas por el examen. Determine los temas que conoce bien y las áreas en las que necesita más experiencia. Para ayudarlo a actualizar sus habilidades en áreas específicas, también le proporcionamos "¿Necesita más revisión?" punteros, que lo dirigen a información más detallada fuera del libro.

El examen de referencia no es un sustituto de la experiencia práctica. Este libro no está diseñado para enseñarle nuevas habilidades.

Le recomendamos que complete la preparación de su examen utilizando una combinación de materiales de estudio y cursos disponibles. Obtenga más información sobre la capacitación en el aula disponible y encuentre cursos en línea gratuitos y eventos en vivo en <http://microsoft.com/learn>. Las pruebas de práctica oficiales de Microsoft están disponibles para muchos exámenes en

<http://aka.mspracticetests>.

Este libro está organizado por la lista "Habilidades medidas" publicada para el examen. La lista de "Habilidades medidas" para cada examen está disponible en el sitio web de Microsoft Learn:

<http://aka.ms/examlist>.

Tenga en cuenta que esta referencia de examen se basa en esta información disponible públicamente y en la experiencia del autor. Para salvaguardar la integridad del examen, los autores no tienen acceso a las preguntas del examen.

# Sobre el Autor

**Craig Zacker** es autor o coautor de docenas de libros, manuales, artículos y sitios web sobre temas informáticos y de redes. También ha sido profesor de inglés, editor técnico y de copia, administrador de red, webmaster, entrenador corporativo, ingeniero de soporte técnico, operador de minicomputadora, estudiante de literatura y filosofía, empleado de biblioteca, técnico de cuarto oscuro fotográfico, un empleado de envío, y un chico de periódico. Vive en una casita con su bella esposa y un gato neurótico.

# Capítulo 1. Comprender los conceptos de la nube

La nube es una de las palabras de moda más grandes que ha surgido de la industria de TI, pero es un término que es difícil de definir en cualquiera de los términos más generales. Para una definición simple, puede decir que el *nube* es un recurso basado en Internet que brinda a los suscriptores varios tipos de servicios de TI a pedido. Para los usuarios, la nube les permite ejecutar aplicaciones, transmitir videos, descargar música, leer correos electrónicos y realizar cualquier cantidad de otras tareas, todo sin tener que preocuparse sobre dónde están ubicados los servidores, qué recursos utilizan, cuántos datos están involucrados y, en la mayoría de los casos, si el servicio está operativo. Al igual que la electricidad o el agua en su casa, la enciende y está allí, la mayor parte del tiempo. Sin embargo, para los profesionales de TI, definir la nube puede ser más difícil.

## Habilidades en este capítulo:

- Detallar y comprender los beneficios y consideraciones del uso de servicios en la nube
- Comprender los diferentes tipos de servicios en la nube disponibles

# HABILIDAD 1.1: DETALLE Y ENTIENDA LOS BENEFICIOS Y LAS CONSIDERACIONES DEL USO DE LOS SERVICIOS EN LA NUBE

---

Los administradores de sistemas, los desarrolladores de software, los administradores de bases de datos y el personal de soporte al usuario ven la nube de una manera diferente y la usan para diferentes propósitos. Los proveedores de la nube, como Microsoft, Google y Amazon, suelen ofrecer una amplia variedad de recursos y servicios. Pueden proporcionar hardware virtualizado, como servidores, almacenamiento y redes; software en forma de servidor de fondo y aplicaciones de usuario; así como herramientas para mensajería, gestión de contenido, colaboración, gestión de identidad, análisis y otros. Los servicios se proporcionan en un *a la carta* base, con los suscriptores solo pagando por lo que usan.

## Esta sección cubre cómo:

- Comprender los servicios en la nube
- Comprender las ventajas de la computación en la nube

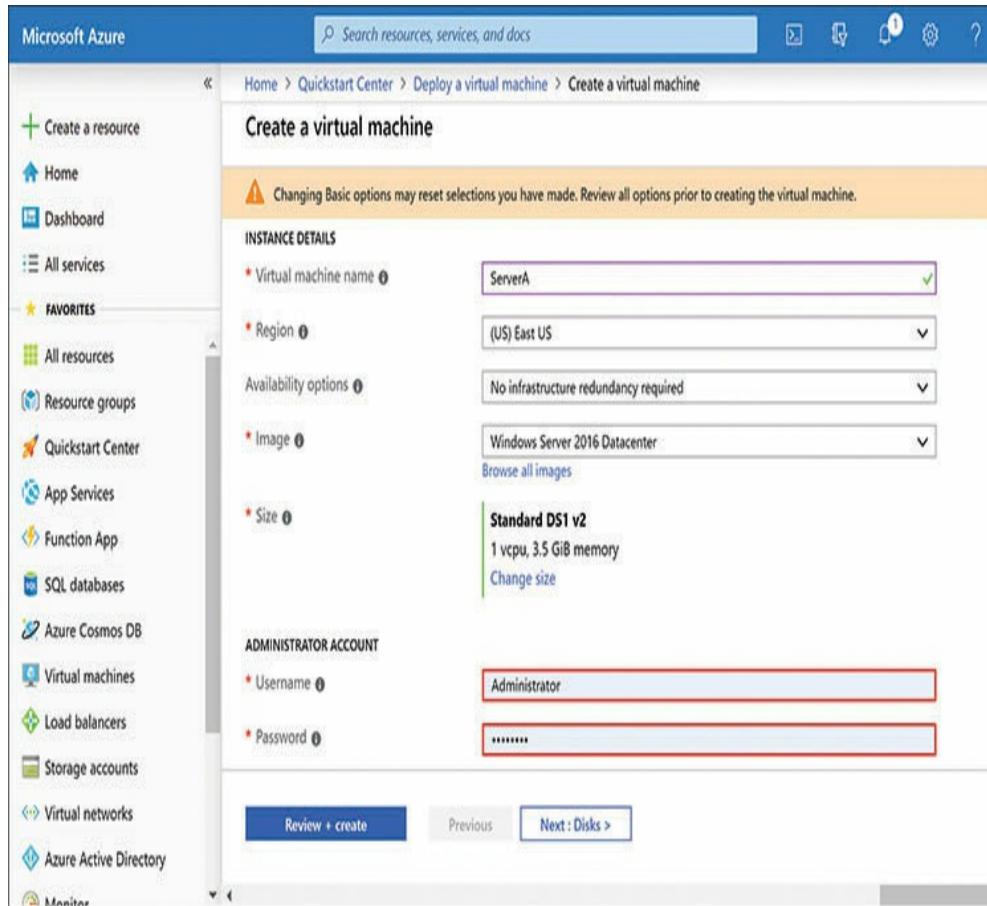
## Comprender los servicios en la nube

Los diferentes tipos de profesionales de TI entienden la nube de diferentes maneras. Para un administrador del sistema, la nube puede proporcionar máquinas virtuales que funcionan como servidores, en

lugar o junto a servidores físicos en el centro de datos de la organización. Para los desarrolladores de software, la nube puede proporcionar una variedad de plataformas preconfiguradas y entornos de desarrollo para la implementación y prueba de aplicaciones. Para un administrador de base de datos, la nube puede proporcionar arquitecturas de almacenamiento complejas y soluciones de administración de bases de datos preconfiguradas. Los servicios en la nube pueden organizar los datos y usar inteligencia artificial para desarrollar nuevos usos para ellos. Para los técnicos de soporte al usuario, la nube puede proporcionar aplicaciones de productividad y otro software, como Office 365, que se implementan más fácilmente que las aplicaciones independientes, se actualizan automáticamente de forma regular y son accesibles en cualquier plataforma de dispositivo.

En cada una de estas especializaciones, los servicios en la nube pueden eliminar los tediosos procesos de configuración que los administradores a menudo tienen que realizar antes de ponerse a trabajar. Por ejemplo, el proceso de agregar un nuevo servidor físico a un centro de datos puede requerir muchas tareas separadas, que incluyen evaluar las necesidades de hardware, seleccionar un proveedor, esperar la entrega, ensamblar el hardware e instalar y configurar el sistema operativo y las aplicaciones. Estas tareas pueden resultar en días o semanas desperdiciados incluso antes de que el servidor esté listo para su uso. Con un proveedor en la nube, el proceso de agregar un nuevo servidor virtual lleva solo unos minutos. Una interfaz de administración remota, como Windows Azure

portal mostrado en Figura 1-1 , permite al suscriptor seleccionar los recursos de hardware virtual deseados para el servidor y, en unos minutos, el nuevo servidor se está ejecutando y listo para usar.



**FIGURA 1-1** La interfaz Crear una máquina virtual en el Portal de Windows Azure

## Ventajas de la computación en la nube

Cuando una organización está construyendo una nueva infraestructura de TI o expandiendo una existente, el

La cuestión de si utilizar recursos locales o servicios en la nube basados en suscriptores es una decisión crítica en estos días. Los servicios basados en la nube pueden no ser preferibles para todos los escenarios informáticos, pero pueden proporcionar muchas ventajas sobre los centros de datos locales. Al diseñar una estrategia de TI, una empresa debe considerar tanto las necesidades prácticas de la organización, incluida la seguridad de los datos y otros factores comerciales, como los costos relativos de los servicios requeridos.

Algunas de las ventajas que puede proporcionar la computación en la nube se analizan en las siguientes secciones.

## Economía

Los servicios en la nube incurren en cargos regulares, pero los cargos generalmente se basan únicamente en las necesidades de los suscriptores y en lo que usan en un momento determinado. Los ahorros monetarios que resultan del uso de servicios en la nube pueden ser significativos. Algunos de los gastos que se pueden reducir o eliminar mediante el uso de servicios en la nube incluyen los siguientes:

- **Hardware** El hardware de servidor de alta gama utilizado por una gran empresa, además de los componentes informáticos estándar, puede incluir arreglos de almacenamiento elaborados y otro hardware que es un gasto inicial costoso antes de que comience cualquier trabajo real. Las tarifas por hardware virtualizado equivalente en la nube se amortizan durante la vida del proyecto para el que se utiliza.
  
- **Actualizaciones** En una gran empresa, los servidores y otros componentes de hardware tienen una esperanza de vida documentada, después de lo cual deben reemplazarse. El hardware en la nube es virtual, por lo que el suscriptor está aislado de los costos de mantenimiento del proveedor físico.

hardware. Esos costos, por supuesto, se tienen en cuenta en el precio del servicio, pero eliminan otro gasto sustancial de hardware para el suscriptor.

- **Software** Las licencias de software son un gasto significativo, especialmente para productos basados en servidor. Además de los sistemas operativos y las aplicaciones, el software de utilidad para firewalls, protección antivirus y copias de seguridad aumenta el gasto. Al igual que con el hardware, el software suministrado por suscripción por un proveedor de la nube requiere poco o ningún desembolso inicial. Por lo general, el software basado en la nube también incluye actualizaciones aplicadas por el proveedor de manera regular.
- **Ambiente** Equipar un gran centro de datos a menudo implica mucho más gasto que el costo del hardware de la computadora solo. Además del costo de los pies cuadrados, un centro de datos generalmente necesita aire acondicionado y otros controles ambientales, equipos de regulación de electricidad y energía, racks y otro hardware de montaje, equipos de conectividad de red y una infraestructura de seguridad física. Dependiendo de las necesidades de la organización, estos costos pueden variar de significativos a astronómicos. Ninguno de estos gastos son necesarios para los servicios basados en la nube, aunque sus costos ciertamente se tienen en cuenta en las tarifas pagadas por el suscriptor.
- **Red** Un centro de datos requiere una conexión a Internet y también puede requerir conexiones cruzadas entre ubicaciones dentro del centro de datos. El tamaño y la funcionalidad del centro de datos determinan cuánto rendimiento se requiere y qué tecnología puede suministrarlo mejor. Más velocidad cuesta más dinero, por supuesto. Los recursos basados en la nube eliminan este gasto porque la conectividad es parte del servicio. Todavía se requiere acceso a Internet para administrar los recursos de la nube, pero la cantidad de datos transferidos es relativamente pequeña.
- **Redundancia** Dependiendo de las necesidades de la organización, la tolerancia a fallas puede tomar la forma de fuentes de alimentación de respaldo, servidores redundantes o incluso centros de datos redundantes en diferentes ciudades, lo que puede hacer que los costos operativos crezcan exponencialmente. Por lo general, los proveedores de la nube pueden proporcionar estos diversos tipos de tolerancia a fallas con un ahorro sustancial. Un contrato con un proveedor de la nube puede incluir un

acuerdo de nivel de servicio (SLA) con un porcentaje de disponibilidad de tiempo de actividad que aísla al suscriptor de los mecanismos de tolerancia a fallas reales empleados y simplemente garantiza que los servicios contratados no sufrirán más que una cantidad específica de tiempo de inactividad. Por ejemplo, un contrato que especifica un tiempo de actividad del 99 por ciento (coloquialmente llamado

*contrato de dos nueves*) permite 3.65 días de tiempo de inactividad por año. Un 99.9 por ciento (o *tres nueves*) El contrato permite 8,76 horas de tiempo de inactividad por año. Las estipulaciones del contrato aumentan a partir de ahí, y el costo aumenta a medida que disminuye el tiempo de inactividad permitido. Un 99.9999 por ciento (o *seis nueves*)

El contrato permite solo 31.5 segundos de tiempo de inactividad por año. Por lo general, si el proveedor no cumple con el porcentaje de tiempo de actividad especificado en el SLA, el contrato solicita un crédito para parte de la tarifa mensual.

- **Personal** Un centro de datos requiere personas capacitadas para instalar, configurar y mantener todo el equipo. Si bien los equivalentes de servicios basados en la nube requieren configuración y mantenimiento realizados a través de una interfaz remota, la eliminación de la necesidad de mantenimiento de hardware reduce en gran medida los requisitos de mano de obra.

Los costos de los servicios basados en la nube no son insignificantes, pero la naturaleza de la inversión financiera es tal que muchas organizaciones consideran que son más prácticos que construir y mantener un centro de datos físico. El desembolso inicial de los servicios en la nube es mínimo, y los costos actuales son fácilmente predecibles.

## Consolidación

Originalmente, los departamentos de TI brindaban servicios a los usuarios mediante la construcción y el mantenimiento de centros de datos que contenían servidores y otros equipos. Uno de los problemas con este modelo era que los servidores a menudo eran

subutilizado Para acomodar la mayor carga de trabajo de la "temporada alta", los servidores a menudo se construían con

recursos que excedieron con creces sus necesidades cotidianas. Esos recursos caros, por lo tanto, permanecieron inactivos la mayor parte del tiempo. Las máquinas virtuales (VM), como las que los administradores pueden crear utilizando productos como Microsoft Hyper-V y VMware ESX, son una solución a este problema. Las máquinas virtuales permiten consolidar múltiples servidores en una computadora física. Los administradores pueden escalar máquinas virtuales agregando o restando recursos virtualizados, como memoria y almacenamiento, o pueden mover las máquinas virtuales de una computadora física a otra, según sea necesario.

Los proveedores de la nube usan esta misma técnica de consolidación para proporcionar a los suscriptores máquinas virtuales. Por ejemplo, cuando un suscriptor de Microsoft Azure crea un nuevo servidor, lo que realmente sucede es que la interfaz de Azure crea una nueva máquina virtual en uno de los servidores físicos de Microsoft. El suscriptor no tiene acceso a la computadora física subyacente que aloja la VM, ni tampoco sabe dónde se encuentra físicamente la computadora. Las máquinas virtuales en el servidor físico están completamente aisladas entre sí, por lo que incluso si los competidores más feroces tuvieran máquinas virtuales ejecutándose en la misma computadora host, nunca lo sabrían. El proveedor puede, y probablemente lo hace, mover máquinas virtuales de una computadora host a otra cuando sea necesario, pero este proceso es completamente invisible para los suscriptores.

El resultado final de este modelo de consolidación es que cada VM recibe exactamente los recursos de hardware virtual que necesita en un momento determinado. Los suscriptores pagan solo por los recursos virtualizados que están utilizando. Nada se desperdicia.

## **Escalabilidad**

Los requisitos comerciales cambian. Pueden aumentar o disminuir en el transcurso de los años, y también pueden experimentar ciclos regulares de actividad que son estacionales, mensuales, semanales o incluso diarios. Un centro de datos físico debe estar diseñado para soportar el nivel de actividad pico para los ciclos comerciales regulares y también anticipar un grado de crecimiento esperado durante varios años. Como se mencionó anteriormente, esto puede significar comprar más equipos de los que la empresa necesita durante la mayor parte de su tiempo operativo, dejando que el exceso de capacidad a menudo se subutilice.

Los servicios basados en la nube evitan estos períodos de subutilización al ser fácilmente escalables. Debido a que el hardware en una máquina virtual está virtualizado, un administrador puede modificar sus recursos a través de un simple cambio de configuración. Una máquina virtual local (es decir, no en la nube) obviamente está limitada por el hardware físico en la computadora que lo aloja y los recursos utilizados por otras máquinas virtuales en el mismo host. Sin embargo, en una máquina virtual basada en la nube, estas limitaciones no

aplicar. Los recursos de hardware físico son invisibles para el suscriptor de la nube, por lo que si los recursos que el suscriptor desea para una VM no están disponibles en su computadora host actual, el proveedor puede mover invisiblemente la VM a otro host que tenga suficientes recursos.

Un servicio basado en la nube es escalable de dos maneras:

- **Escala vertical** También conocido como *ampliar*, El escalado vertical es la suma o resta de hardware virtual en una máquina virtual, como memoria, almacenamiento o CPU. El proceso de escalado es una simple cuestión de ajustar los parámetros de la VM en una interfaz remota; incluso se puede automatizar para acomodar ciclos comerciales regulares. Por lo tanto, el suscriptor paga solo por los recursos que las máquinas virtuales realmente están utilizando en un momento dado.
- **Escala horizontal** También conocido como *escalando*, El escalado horizontal es la suma o resta de máquinas virtuales a un grupo de servidores que ejecutan una aplicación en particular. Por ejemplo, en el caso de una granja de servidores web basada en la nube, las solicitudes de usuarios entrantes se pueden compartir entre varias máquinas virtuales. Si el tráfico web aumenta o disminuye, los administradores pueden agregar o restar máquinas virtuales del clúster, según sea necesario.

## Fiabilidad

En un centro de datos local, la copia de seguridad de datos, la recuperación ante desastres y la tolerancia a fallas son servicios caros que requieren hardware adicional, tiempo de implementación y administración. Una pequeña empresa puede requerir solo un medio de almacenamiento de respaldo y software. Sin embargo, para las empresas con requisitos de TI muy críticos, estos servicios pueden solicitar cualquier cosa hasta duplicar centros de datos en diferentes ciudades con datos de alta velocidad

conexiones que los unen.

Sin embargo, en el caso de un proveedor de nube a gran escala, esto es exactamente lo que implica su infraestructura. Por lo tanto, los proveedores de la nube están en una excelente posición para proporcionar estos servicios elaborados sin la necesidad de actualizaciones de infraestructura, y a menudo pueden hacerlo por tarifas que son mucho menos de lo que se requeriría para que las empresas los brinden ellos mismos.

Por ejemplo, Microsoft Azure proporciona los siguientes mecanismos de confiabilidad para sus servicios basados en la nube:

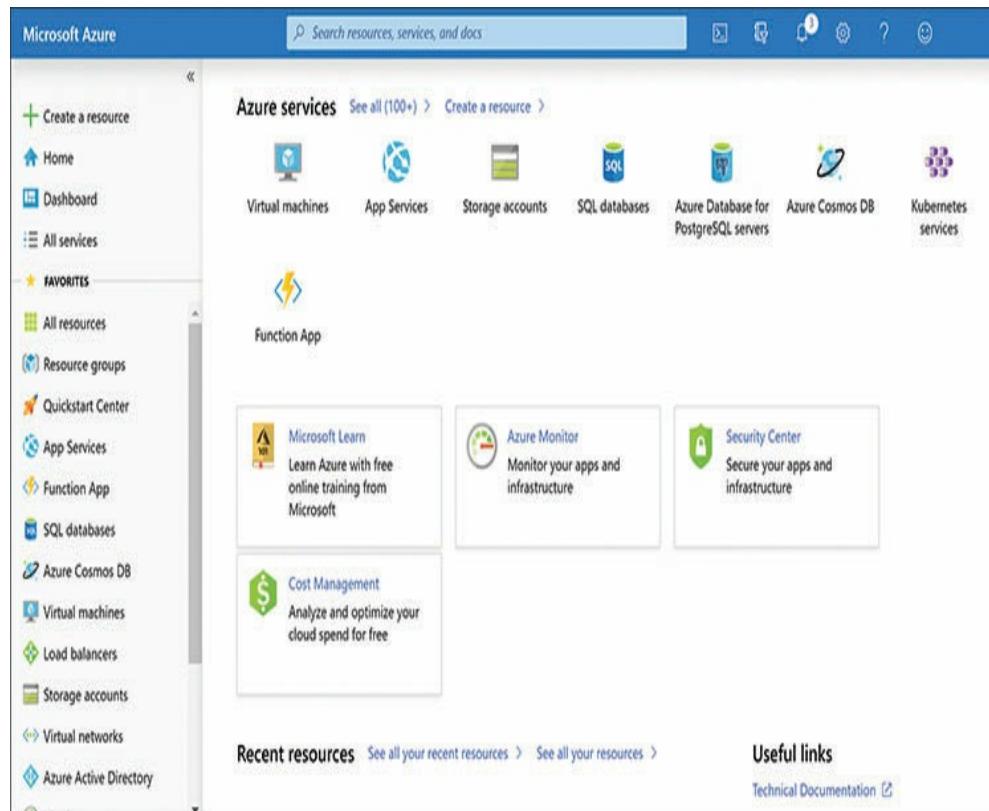
- Azure mantiene tres copias redundantes de todos los datos, con una de esas copias ubicadas en un centro de datos separado.
- Azure proporciona comutación por error automática a un servidor de respaldo para minimizar el tiempo de inactividad en caso de una interrupción.
- Azure aloja todas las aplicaciones en dos instancias de servidor separadas para minimizar el tiempo de inactividad causado por una falla de hardware.

## Manejabilidad

Debido a que los suscriptores no tienen acceso físico a los servidores que alojan sus servicios en la nube, deben acceder a ellos de forma remota. Esto también es común para las organizaciones con servidores locales, particularmente aquellas con grandes centros de datos. A menudo es mucho más conveniente para los administradores acceder a los servidores desde sus escritorios que viajar a un centro de datos que podría estar en otro piso, en otro edificio o incluso en otra ciudad. La gestión remota de hoy por lo general proporciona una solución integral

y acceso confiable a todas las funciones del servidor.

Hay varias herramientas de administración remota disponibles para recursos en la nube y locales, pero los grandes proveedores de servicios de nube externos suelen proporcionar un portal seguro basado en la web que permite a los administradores acceder a todos sus servicios de suscripción utilizando una interfaz, como la de Microsoft Azure se muestra en Figura 1-2 .



**FIGURA 1-2** La interfaz de administración en el Portal de Windows Azure

Un portal basado en la web permite a los administradores acceder a sus servicios desde cualquier ubicación, incluso desde casa o

mientras viajaba.

## Seguridad

La seguridad es un problema importante para cualquier centro de datos, que los administradores suelen abordar al preocuparse por problemas como la pérdida de datos y el acceso no autorizado. Estas son preocupaciones importantes si el centro de datos es local o virtual. Sin embargo, en el caso de un centro de datos local, existe otro vector de ataque potencial: el físico. Los servidores y otros equipos pueden ser robados directamente, dañados por incendios u otros desastres o los intrusos pueden acceder físicamente a ellos. Por lo tanto, existen medidas de seguridad adicionales que pueden ser necesarias, como cerraduras de puertas, equipos de vigilancia, credenciales de acceso o incluso puestos de control de seguridad tripulados.

Los servicios basados en la nube eliminan la necesidad de seguridad física, que es proporcionada por el proveedor. Sin embargo, todavía existe el problema de la seguridad basada en software, y los proveedores de la nube casi siempre proporcionan una variedad de controles y servicios que le permiten fortalecer la seguridad de sus servidores y aplicaciones para satisfacer sus necesidades comerciales.

*Nota:*

**Siempre eres**

**Responsable de sus datos**

**Las organizaciones que usan recursos en la nube para implementar sus servidores deben ser conscientes del hecho de que aún son responsables de la seguridad y privacidad de sus datos. Por ejemplo, si una organización almacena registros médicos de pacientes en un servidor de archivos basado en la nube, la organización sigue siendo responsable de cualquier violación de datos que ocurra. Por lo tanto, los contratos con los proveedores de la nube deben estipular las políticas de seguridad que deben mantener.**

## Infraestructura

En un centro de datos local, los administradores son responsables de todos los aspectos de los servidores y otros equipos, incluida la instalación y el mantenimiento del hardware, la configuración y las actualizaciones del sistema operativo, y la implementación y administración de la aplicación. Los servicios basados en la nube permiten a los suscriptores especificar qué elementos de la infraestructura son responsables de mantener.

Por ejemplo, un suscriptor puede contratar con un proveedor una máquina virtual que ejecute un sistema operativo de servidor, de modo que el suscriptor sea responsable de toda la operación y mantenimiento del servidor. El suscriptor no tiene acceso directo al hardware físico del sistema host, por supuesto, pero sí tiene control sobre el hardware virtual en el que se ejecuta el servidor, así como todo el software que se ejecuta en el servidor, incluido el funcionamiento sistema. En algunas situaciones, esto es deseable, o incluso esencial.

En otras situaciones, los servicios basados en la nube pueden adoptar la forma de plataformas o aplicaciones de servidor preinstaladas. En este caso, el suscriptor podría tener acceso limitado al servidor o no tener ningún acceso. En el caso de que un suscriptor contrate Microsoft Exchange Online, el proveedor otorga al suscriptor acceso administrativo a la aplicación Exchange Server, pero no le otorga acceso al suscriptor al sistema operativo subyacente en el que se ejecuta la aplicación del servidor. Para un suscriptor de Office 365, el proveedor solo otorga acceso a las aplicaciones de Office. El suscriptor no sabe nada sobre los servidores en los que se ejecutan las aplicaciones o sus sistemas operativos.

Estas opciones permiten a los suscriptores del servicio en la nube ejercer la responsabilidad administrativa sobre componentes específicos solo en situaciones en que sus requisitos comerciales lo exijan. Para los elementos administrados por el proveedor de servicios, los contratos generalmente estipulan requisitos de mantenimiento de hardware y políticas de actualización de software. El resultado final puede ser un ahorro sustancial en tiempo y capacitación para el personal interno de TI del suscriptor.

### **Presuntas desventajas de la computación en la nube**

Hay algunos profesionales de TI que persisten en afirmar que los servicios basados en la nube son inferiores a los servicios locales. Podrían decir que un centro de datos local

es más seguro, más confiable, proporciona un mayor acceso al equipo o sufre menos tiempo de inactividad. Si bien no se puede decir que la nube es siempre una solución preferible, estos argumentos datan principalmente de un momento en que la nube era una tecnología nueva e inmadura. Ahora han sido desacreditados en gran medida por años de rendimiento comprobado.

Todavía hay razones por las cuales las empresas pueden y deben mantener centros de datos locales. Por ejemplo, podrían tener requisitos especiales de seguridad, o podrían haber hecho una gran inversión en instalaciones y equipos. Sin embargo, cada año se observa un mayor porcentaje de servidores implementados en la nube y clientes que acceden a servicios basados en la nube. Microsoft 365 es el siguiente paso para llevar la nube al entorno de productividad de escritorio.

## **HABILIDAD 1.2: ENTENDER LOS DIFERENTES TIPOS DE SERVICIOS EN LA NUBE DISPONIBLES**

---

La flexibilidad es un aspecto importante de la computación en la nube, y Microsoft 365 puede acomodar una amplia variedad de entornos de TI. Mientras que algunas organizaciones pueden estar construyendo una implementación de Microsoft 365 desde cero, otras pueden tener una infraestructura existente que desean incorporar en una solución de Microsoft 365. Antes de que sea posible explorar cómo se puede hacer esto, es importante

comprender los diversos tipos de arquitecturas en la nube y modelos de servicio.

### Esta sección cubre cómo:

- Posicione Microsoft 365 en un escenario SaaS, IaaS, PaaS, Público, Privado e Híbrido

## Arquitecturas en la nube

Las organizaciones de hoy usan los recursos de la nube de diferentes maneras y por varias razones. Una nueva empresa o división de una empresa podría decidir construir una infraestructura de TI completamente nueva utilizando solo recursos basados en la nube. Mientras tanto, una empresa que ya ha invertido en una infraestructura de TI tradicional podría usar la nube para expansiones o para la adición de servicios seleccionados. Las organizaciones que planean sus infraestructuras pueden usar cualquiera de las tres permutaciones de arquitectura de nube descritas en las siguientes secciones.

## Nube pública

UNA *nube pública* es una red de servidores propiedad de un proveedor de servicios de terceros en una ubicación remota, que brinda a los suscriptores acceso a máquinas virtuales o servicios a través de Internet, a menudo por una tarifa. Los precios se basan en los recursos o servicios que utiliza. Microsoft Azure, Amazon Web Services y Google Cloud son todos

Ejemplos de proveedores de servicios de nube pública que las organizaciones utilizan para alojar sus máquinas virtuales y acceder a otros servicios.

**Nota:**

**Público no**

**Media sin protección**

**El término *nube pública* es una especie de nombre inapropiado; no significa que las máquinas virtuales que crea una organización en la nube de un proveedor sean públicas, es decir, abiertas al acceso por cualquier persona. Solo significa que el proveedor proporciona servicios al público por suscripción, a los que se puede acceder desde cualquier lugar en cualquier momento a través de Internet.**

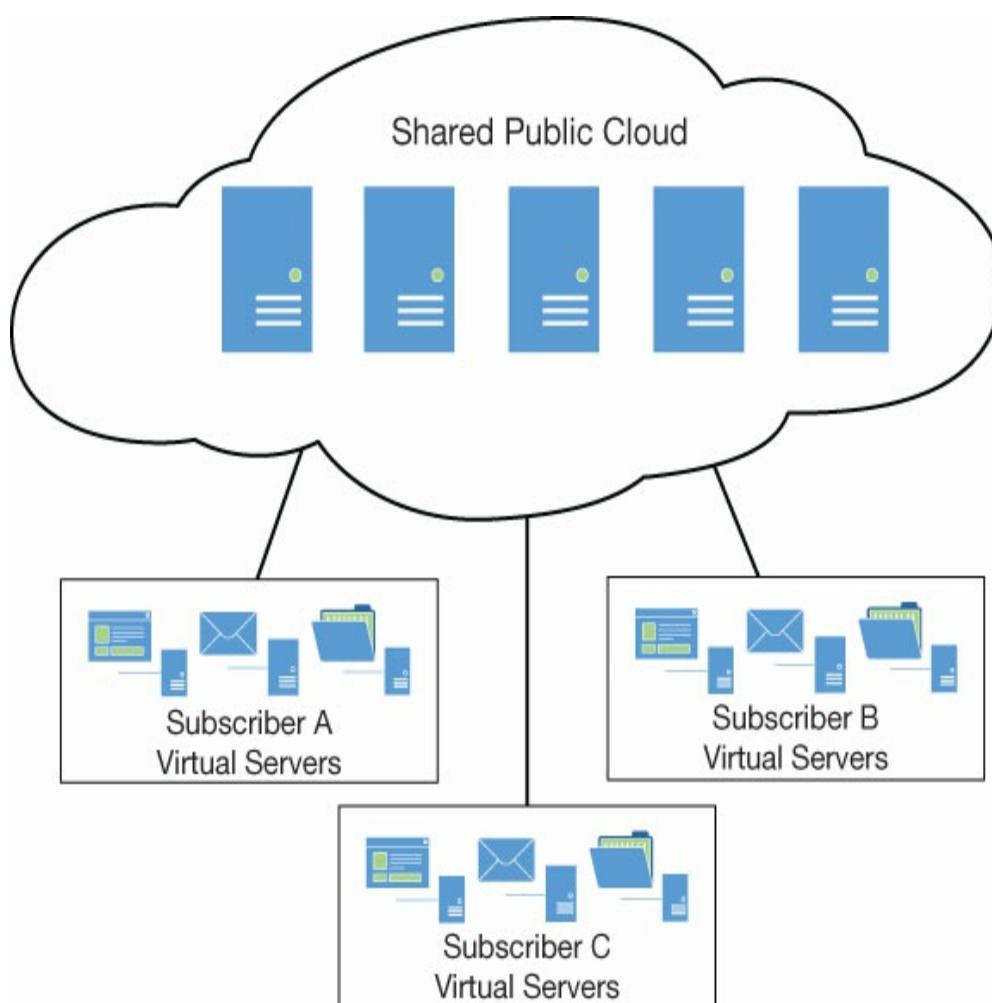
Estos actores principales en la industria de la nube pública mantienen miles de servidores en centros de datos ubicados en todo el mundo. Pueden acomodar clientes de grandes empresas al proporcionar servicios a escala global. Hay otros proveedores de nube más pequeños que ofrecen los mismos servicios, que podrían no funcionar a una escala tan masiva, pero estos también pueden tener sus ventajas. Debido a que los proveedores de servicios en la nube son responsables de administrar y mantener los servidores físicos, los suscriptores ahorran una gran cantidad de tiempo, gastos y recursos humanos.

Existen dos tipos básicos de implementación en la nube pública que las organizaciones pueden usar, como sigue:

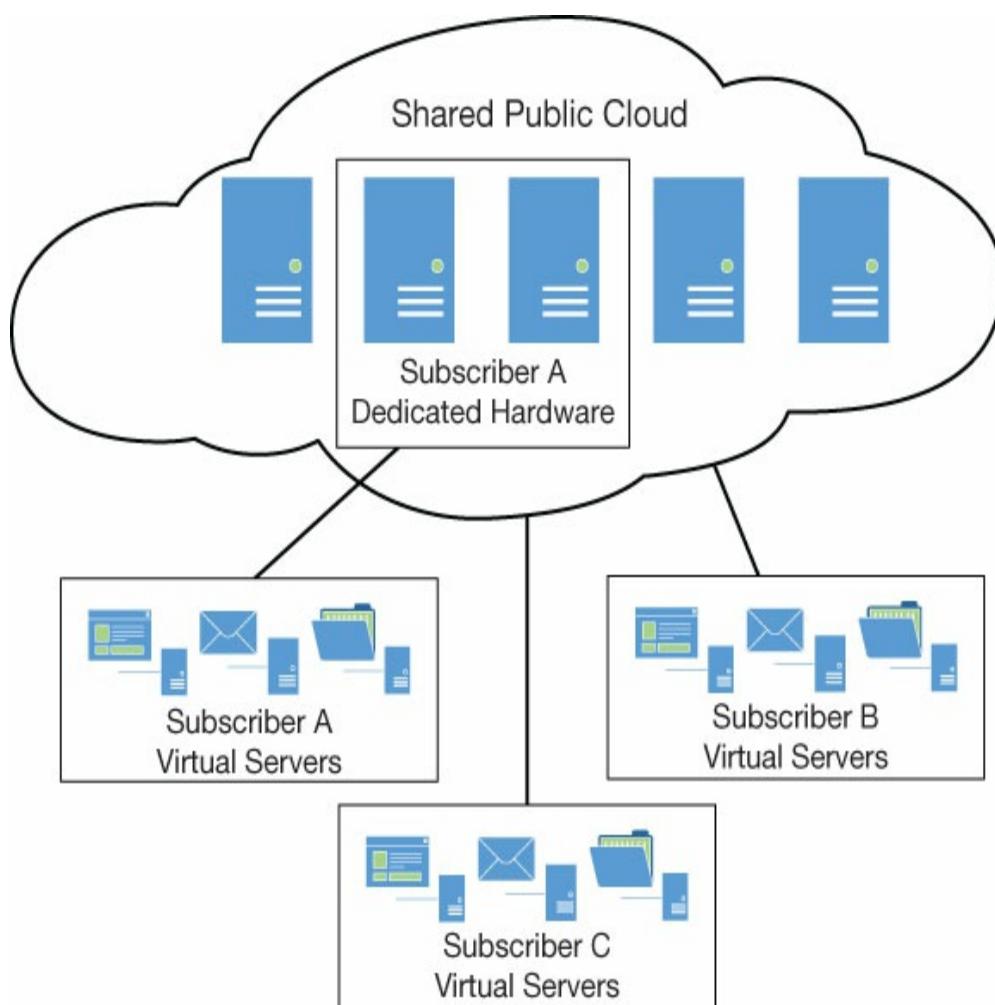
- **Nube pública compartida** Los suscriptores acceden a servicios que un proveedor externo implementa en hardware que podría ser utilizado por otros

suscriptores al mismo tiempo. Por ejemplo, un servidor host físico en el sitio de un proveedor puede ejecutar máquinas virtuales que pertenecen a diferentes suscriptores simultáneamente, como se muestra en Figura 1-3 . Las máquinas virtuales están aseguradas individualmente y funcionalmente aisladas unas de otras. Esto es lo que normalmente se entiende por una nube pública.

- **Nube pública dedicada** Los suscriptores contratan a un proveedor externo para una infraestructura de hardware dedicada a su uso exclusivo. (Ver Figura 1-4 .) Los servicios prestados son los mismos que en una nube pública compartida; La única diferencia es el hardware que utiliza el proveedor para proporcionar los servicios. Obviamente, este arreglo es más costoso que una nube pública compartida, pero algunas organizaciones necesitan la seguridad adicional y la tolerancia a fallas proporcionadas por tener hardware dedicado a su propio uso.



**FIGURA 1-3** Servidores virtuales que se ejecutan en una nube pública compartida



**FIGURA 1-4** Servidores virtuales que se ejecutan en una nube pública dedicada

Por lo tanto, el término *nube pública* puede referirse a un proveedor que permite a las empresas construir sus redes de TI prácticamente en lugar de hacerlo físicamente. Los suscriptores de Microsoft 365 pueden hacer uso de estos servicios para

implementar toda o parte de su productividad infraestructura. Sin embargo, esta no es la única función de la nube pública. Cuando las personas transmiten películas a sus televisores, usan servicios bancarios basados en la web, acceden a su correo electrónico en línea o usan las aplicaciones de productividad de Office 365, están usando proveedores de nube pública. La diferencia en estos casos es que el proveedor está proporcionando servicios específicos en lugar de una infraestructura de TI.

## Nube privada

UNA *nube privada* es una red de servidores propiedad y operada por una empresa únicamente para su propio uso. Si bien los servicios pueden ser los mismos y parecer idénticos a sus usuarios finales, la principal diferencia es que la organización también tiene control sobre el hardware físico.

En una implementación en la nube pública de una infraestructura de TI, el suscriptor crea máquinas virtuales en los servidores del proveedor y las usa para instalar y ejecutar aplicaciones específicas o contrata con el proveedor para acceder a los servicios que se ejecutan en las propias máquinas virtuales del proveedor. Una implementación en la nube privada generalmente funciona de la misma manera. La organización todavía crea y utiliza máquinas virtuales para ejecutar sus aplicaciones en la mayoría de los casos, pero crea esas máquinas virtuales en servidores host físicos que posee.

Otra variación en la nube privada es el *nube privada alojada*, en el cual el hardware que es propiedad o arrendado por una organización es alojado y administrado por un proveedor externo. La organización tiene un uso exclusivo del hardware y evita los gastos de construcción y administración de un centro de datos. Tienen que pagar tarifas continuas al proveedor, y este acuerdo podría no satisfacer todas las estipulaciones de almacenamiento de datos, pero es probable que el costo general sea menor que una nube privada local.

*Nota:*

## Nubes privadas y

### Tráfico de internet

El término *nube privada* puede ser algo así como un oxímoron. Por lo general, la definición de la nube incluye el acceso a los servicios a través de Internet. En una nube pública, el acceso administrativo y de usuario a los recursos de la nube se realiza a través de Internet. Si bien una nube privada puede proporcionar a los usuarios y administradores acceso a los servicios a través de Internet, por lo general no utiliza Internet cuando los administradores y usuarios se encuentran en el mismo sitio que el centro de datos que alberga la nube.

Cuando una gran empresa mantiene instalaciones en múltiples ubicaciones, los usuarios de todas esas instalaciones pueden acceder a una nube privada a través de Internet. Sin embargo, una organización pequeña o mediana que ejecuta Microsoft 365 Business en una sola ubicación puede ejecutar lo que técnicamente se llama una nube privada sin la necesidad de que el tráfico de usuarios y administradores abandone la instalación.

La arquitectura de nube privada puede proporcionar un nivel de

seguridad y privacidad que un proveedor de nube pública podría no ser capaz de cumplir. Una organización puede tener estipulaciones contractuales del gobierno o requisitos legales que los obliguen a mantener su propio hardware y almacenar datos confidenciales en el sitio en lugar de usar hardware de terceros que no esté sujeto a las mismas estipulaciones o requisitos. Por ejemplo, la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA) dicta cómo deben protegerse y protegerse los datos médicos en los Estados Unidos. Ya sea que esté involucrado un proveedor externo de la nube, una empresa es legalmente responsable de todos los datos almacenados en sus servidores. Es posible que una organización también necesite ejecutar una aplicación heredada que requiera una configuración específica de hardware o software que un proveedor externo no pueda suministrar.

Una nube privada también proporciona un mayor grado de personalización que los recursos de la nube pública. Los proveedores de la nube pública tienen éxito debido a la escala de sus negocios; sus servicios son configurables utilizando las opciones que más desean sus clientes. No es probable que proporcionen acceso a oscuras opciones de software que solo necesitarán unos pocos de sus clientes. En el caso de una nube privada, una organización tiene acceso a todas y cada una de las opciones de personalización proporcionadas por el software que elige instalar.



### **Consejo de examen**

La diferencia entre una nube privada y una nube pública dedicada es quién posee y opera el hardware. Los candidatos al examen deben saber que parte de la documentación utiliza el término **nube privada**, en vez de **nube pública dedicada**, para describir el hardware propiedad y operado por un proveedor externo para el uso exclusivo de un suscriptor.

---

Las ventajas de una nube privada también son sus desventajas. El propietario del hardware es responsable de comprar, alojar, implementar y mantener ese hardware, lo que puede aumentar en gran medida el gasto general, como se describió anteriormente en este capítulo. No hay tarifas de suscriptor continuas para una nube privada, como las hay con un proveedor de nube pública, pero hay tarifas continuas para operar un centro de datos, que incluye espacio, energía, seguros y personal.

La organización también es responsable de comprar y mantener licencias para todos los productos de software necesarios para proporcionar los servicios necesarios. Esto puede incluir licencias de sistema operativo, licencias de servidor de aplicaciones y licencias de usuario, así como el costo de utilidades de software adicionales. Por lo general, los costos generales de una infraestructura de nube privada son más altos que los de una nube pública y pueden ser enormemente más altos. Depende de la organización determinar si las ventajas de la nube privada valen el gasto adicional.

## Nube híbrida

UNA *nube híbrida* combina la funcionalidad de una nube pública y una privada, permitiendo que una organización disfrute de lo mejor de ambas arquitecturas. Hay una variedad de escenarios en los que una organización podría preferir implementar una arquitectura de nube híbrida.

Si una organización tiene servicios existentes implementados en su propio hardware físico, es posible que desee mantener esos servicios mientras agrega otros de un proveedor de nube pública. Por ejemplo, la organización podría haber alcanzado la capacidad física de su propio centro de datos y no desea invertir en una expansión importante de las instalaciones.

Una organización también puede usar recursos de la nube pública para ampliar la capacidad de su nube privada o de su red interna durante períodos temporales de mayor necesidad, como los aumentos estacionales de negocios. Esta técnica, llamada *estallido de nubes*, elimina la necesidad de que la organización pague por hardware y otros recursos que solo se requieren por breves períodos de tiempo. Debido a que es posible conectar los servicios públicos y privados, los recursos pueden interactuar de cualquier manera que sea necesaria. Por ejemplo, una empresa con un sitio web de comercio electrónico implementado en una nube privada puede agregar servidores públicos basados en la nube a su granja de servidores web para acomodar el aumento del tráfico durante la temporada alta de Navidad.

Otra posibilidad es que una organización pueda estar sujeta al tipo de almacenamiento de datos u otros requisitos de seguridad descritos en la sección anterior, pero no desean construir toda su infraestructura en una nube privada. En este escenario, la organización podría desplegar una base de datos que contenga los datos confidenciales en una nube privada y utilizar un proveedor de nube pública para la implementación de un sitio web vinculado a la base de datos. De esta manera, la red puede cumplir con los requisitos de almacenamiento sin tener que ir a expensas de implementar servidores web y otros servicios en la nube privada. Lo mismo es cierto para una variedad de otros servicios; Las organizaciones pueden mantener sus datos y servicios confidenciales en la nube privada y utilizar la nube pública para los servicios no sensibles.

Algunos proveedores de la nube proporcionan herramientas que permiten a los administradores administrar sus recursos de la nube pública y privada a través de una única interfaz. Microsoft Azure proporciona Azure Active Directory, por ejemplo, que permite a un suscriptor usar el mismo servicio de directorio para recursos de nube públicos y privados, de modo que los administradores puedan acceder a ambos con un inicio de sesión único. Azure también proporciona interfaces de administración y seguridad, las cuales tienen soporte incorporado para

arquitecturas de nube híbrida.

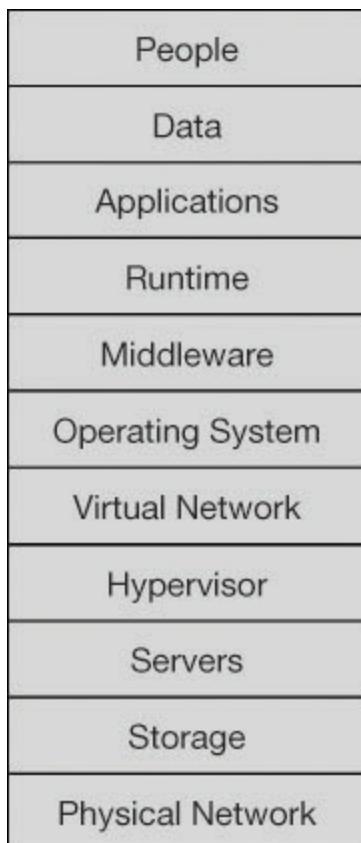
## Modelos de servicio en la nube

Las ofertas de los proveedores de servicios en la nube generalmente se dividen en modelos de servicio, que especifican qué elementos de la infraestructura de la nube se incluyen con cada producto. Existen tres modelos principales de servicios en la nube, denominados Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS).

Una infraestructura en la nube se puede dividir en capas formando una pila, como se muestra en Figura 1-5 . Las funciones de las capas son las siguientes:

- **Personas** Los usuarios que trabajan con la aplicación.
- **Datos** La información que la aplicación crea o utiliza
- **Solicitud** El programa de software de nivel superior que se ejecuta en una máquina virtual
  
- **Tiempo de ejecución** Una capa de software intermedia, como .NET o Java, que proporciona el entorno en el que se ejecutan las aplicaciones
- **Middleware** Un componente de software que proporciona servicios intermedios entre un sistema operativo y aplicaciones.
- **Sistema operativo** El software que proporciona las funciones básicas de una máquina virtual.
  
- **Red virtual** Las conexiones lógicas entre máquinas virtuales que se ejecutan en servidores
- **Hipervisor** El componente de software en los servidores físicos que permite que las máquinas virtuales compartan los recursos físicos del servidor.

- **Servidores** Las computadoras físicas que alojan las máquinas virtuales que brindan servicios en la nube
- **Almacenamiento** Los discos duros y otros componentes físicos que forman el subsistema que proporciona almacenamiento de datos para los servidores físicos.
- **Red física** Los cables, enruteadores y otros equipos que conectan físicamente los servidores entre sí y a Internet.



**FIGURA 1-5** Las capas de la infraestructura de la nube.

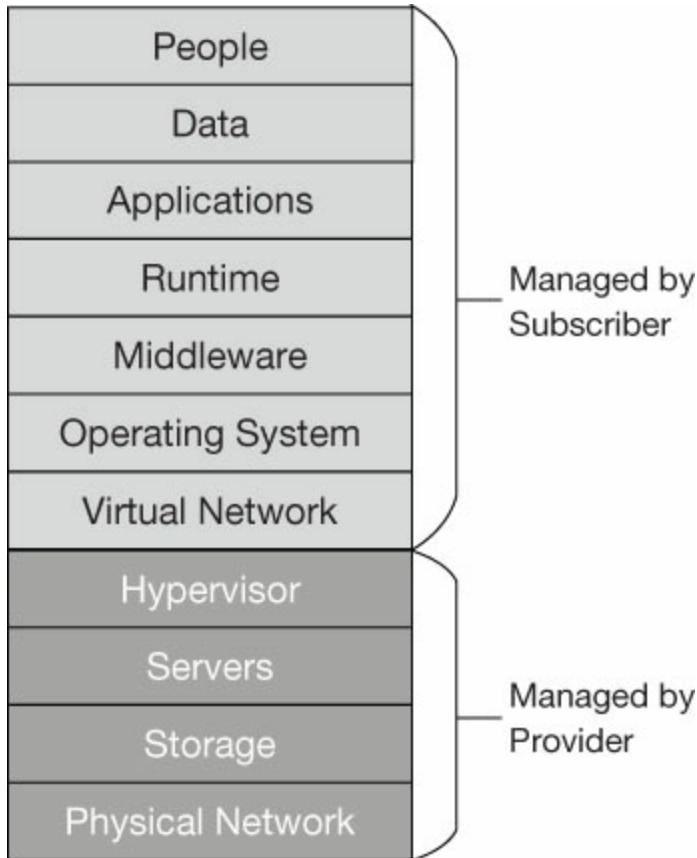
En una organización que utiliza sus propios servidores locales para todo, no hay ninguna nube involucrada, y la organización es obviamente responsable de administrar todas las capas de la pila. Sin embargo, cuando una organización usa servicios basados en la nube, el servicio en la nube

el proveedor gestiona algunas capas de la pila y la organización gestiona el resto. Esto se llama un *modelo de responsabilidad compartida*. Las capas que administra la organización y las que administra el proveedor dependen del modelo de servicio utilizado para proporcionar el producto en la nube. Los tres modelos básicos de servicios en la nube se describen en las siguientes secciones.

## IaaS

*Infraestructura como servicio (IaaS)* es un modelo de computación en la nube en el que un proveedor de servicios en la nube proporciona al cliente los elementos de computación física: la red, el subsistema de almacenamiento, los servidores físicos y el hipervisor que se ejecuta en los servidores. Esto proporciona a los suscriptores todo lo que necesitan para crear sus propias máquinas virtuales y administrarlas por sí mismos. Por lo tanto, todas las capas de infraestructura de la nube sobre el hipervisor son responsabilidad del suscriptor, como se muestra en Figura 1-6 .

---



**FIGURA 1-6** El modelo de responsabilidad compartida para IaaS

Por ejemplo, cuando un suscriptor usa Microsoft Azure para crear una máquina virtual, el proveedor proporciona acceso a un servidor físico con un software de hipervisor, presumiblemente Microsoft Hyper-V, que se ejecuta en él. El servidor tiene un subsistema de almacenamiento físico y está conectado a una red física que le proporciona acceso a los otros servidores del proveedor y a Internet. Con las herramientas de administración que proporciona Azure, el suscriptor puede crear una máquina virtual que contenga una cantidad específica de memoria y almacenamiento,

y una serie de CPU, todas las cuales se realizan prácticamente.

*¿Necesita más revisión ?:*

**Nube**

## **Computación con Microsoft Azure**

Para obtener más información sobre la computación en la nube realizada en Microsoft Azure, vea <https://azure.microsoft.com/en-ca/overview/what-is-cloud-computing>

El resultado final es una máquina virtual que el suscriptor puede instalar, configurar y usar para ejecutar aplicaciones como una VM que se ejecuta en un servidor local. La diferencia es que el suscriptor no tiene que equipar un centro de datos, construir una red, adquirir una computadora física e instalar el hipervisor. En cambio, el suscriptor paga una tarifa regular por los recursos reales que usa la VM. El suscriptor puede agregar memoria, almacenamiento y CPU a la VM o eliminarlos, según sea necesario, y el suscriptor puede configurar muchas otras configuraciones a través de una interfaz de administración remota. Los recursos adicionales incurren en tarifas adicionales, pero el proceso de construcción de un nuevo servidor lleva unos minutos en lugar de días o semanas.

Con el modelo IaaS, el proveedor es responsable de los servidores físicos y la red física, pero el suscriptor es responsable de administrar y mantener sus máquinas virtuales y la red virtual en la que

corren, como se muestra anteriormente en [Figura 1-6](#). Por lo tanto, el proveedor instala actualizaciones del sistema operativo en los servidores físicos, pero el suscriptor debe instalar cualquier sistema operativo y actualizaciones de aplicaciones necesarias en las máquinas virtuales. Cualquier otro software de VM, mantenimiento y problemas de administración que surjan también son responsabilidad del suscriptor.

**Nota:**

**Actualización de VM**

**administración**

**Por una tarifa adicional, Microsoft Azure puede proporcionar una solución de administración de actualizaciones que automatiza la instalación de actualizaciones y parches en las máquinas virtuales de un suscriptor.**

De todos los modelos de servicios en la nube, IaaS asigna la mayor responsabilidad al suscriptor y, en muchos casos, así es como los administradores lo desean. Al crear y configurar sus propias máquinas virtuales, los administradores pueden duplicar el entorno de sus servidores locales, creando una infraestructura híbrida de nube que puede manejar el tráfico de desbordamiento durante una temporada alta.

Las organizaciones con sitios web de alto tráfico a menudo utilizan un proveedor de servicios de alojamiento web dedicado para ejecutar sus sitios. Sin embargo, construir el sitio usando máquinas virtuales proporcionadas por un proveedor de servicios en la nube usando el modelo IaaS a menudo puede ser una propuesta mucho menos costosa.

Los suscriptores también pueden usar IaaS para crear un entorno de prueba y desarrollo para aplicaciones. La rápida implementación y modificación de las máquinas virtuales permite a los administradores crear múltiples plataformas temporales de evaluación y prueba y eliminarlas con la misma facilidad.

IaaS también puede proporcionar a los suscriptores máquinas virtuales que contengan cantidades masivas de recursos de hardware virtual que serían poco prácticos para implementar en servidores locales. Los grandes conjuntos de datos y la informática de alto rendimiento pueden requerir grandes cantidades de memoria y potencia de procesamiento para realizar las tareas requeridas para las aplicaciones, como el diseño del clima, la minería de datos y el modelado financiero. Los recursos de un proveedor de servicios en la nube de alta gama hacen que sea mucho menos costoso equipar las máquinas virtuales con el hardware virtual necesario que construir servidores físicos equivalentes.

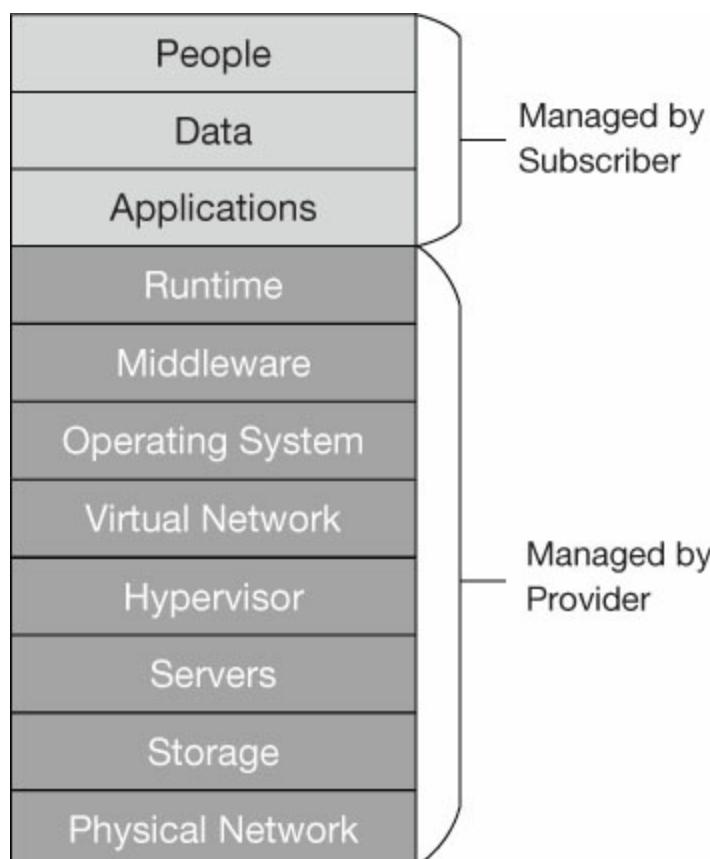
## PaaS

En lo que a veces se conoce como *nube escalonada* infraestructura de modelo de servicio, *Plataforma como servicio (PaaS)* es el segundo nivel, ya que se basa en las responsabilidades del proveedor del primer nivel (IaaS). PaaS está diseñado para proporcionar a los suscriptores una plataforma de desarrollo lista para usar que les permite evitar perder tiempo construyendo repetidamente la infraestructura de hardware y software para un sistema de prueba antes de que puedan

ejecutar una nueva aplicación

Debido a que la plataforma es accesible a través de Internet como todos los servicios en la nube, una organización con múltiples desarrolladores que trabajan en el mismo proyecto puede proporcionarles a todos acceso al entorno de prueba, incluso si están ubicados en diferentes sitios.

El modelo PaaS amplía la responsabilidad del proveedor de servicios en la nube sobre el modelo IaaS al agregar la red virtual, el sistema operativo, el middleware y las capas de tiempo de ejecución, como se muestra en Figura 1-7 . Cuanto mayor es la responsabilidad del proveedor, menor es la del suscriptor.



## **FIGURA 1-7 El modelo de responsabilidad compartida para PaaS**

A diferencia de las máquinas virtuales en el modelo IaaS, el proveedor de la nube es completamente responsable del sistema operativo VM, aplicando actualizaciones y parches y realizando el mantenimiento según sea necesario. La plataforma también puede incluir (por una tarifa adicional) componentes adicionales especificados por el suscriptor, como herramientas de desarrollo, middleware y sistemas de administración de bases de datos. El objetivo del modelo PaaS es eliminar la necesidad de que los desarrolladores de software hagan cualquier cosa que no sea desarrollar, construir, personalizar, probar e implementar sus aplicaciones.

### **Sin servidor**

Las tarifas para las máquinas virtuales PaaS e IaaS generalmente se basan en los recursos que están configurados para usar y el tiempo de ejecución. Sin embargo, existe otro modelo de servicio en la nube para el desarrollo de aplicaciones, relacionado con PaaS, denominado *Computación sin servidor*. En informática sin servidor (a veces conocida como *Funcionar como un servicio*,

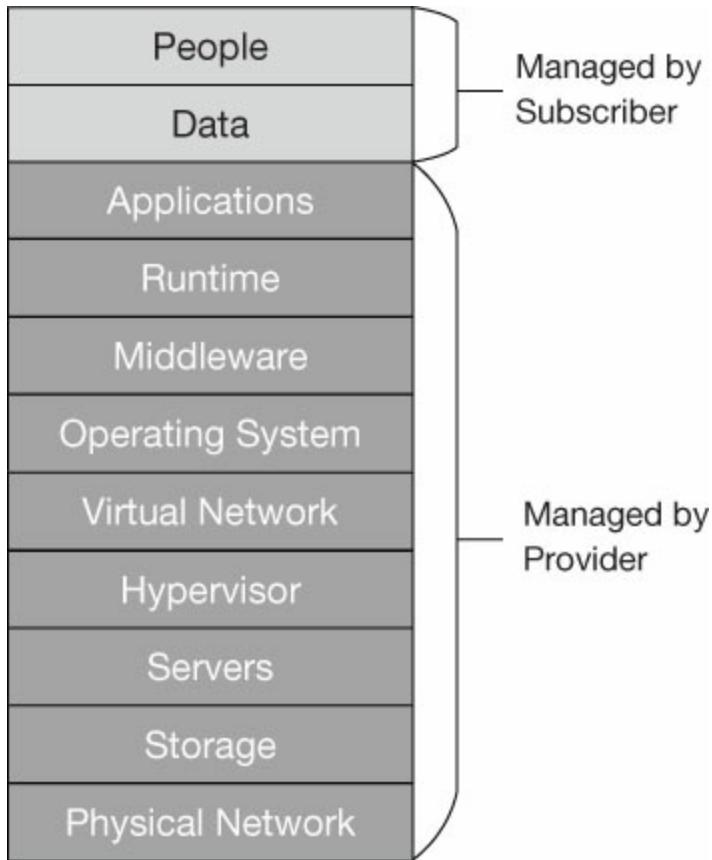
o FaaS), el proveedor de la nube asume aún más la responsabilidad de la administración del servidor al asignar dinámicamente los recursos de la máquina virtual en respuesta a las solicitudes o eventos de la aplicación.

El precio se basa en los recursos de la máquina virtual tal como se utilizan realmente. Por lo tanto, este modelo puede ser menos costoso que una VM PaaS que está incurriendo en cargos

El tiempo se está ejecutando. El término *sin servidor*, en este caso, no significa que no haya un servidor involucrado; el nombre deriva del hecho de que el suscriptor de la nube no tiene que aprovisionar una máquina virtual en la que se ejecutará el código del desarrollador.

## SaaS

*Software como servicio (SaaS)* es el tercer nivel de la infraestructura del modelo de servicio en la nube, y en este modelo, el proveedor de la nube es responsable de casi todas las capas. Solo las personas y las capas de datos se dejan al suscriptor, como se muestra en Figura 1-8 . Esto significa que el proveedor es responsable de las aplicaciones, así como de todas las capas debajo.



**FIGURA 1-8** El modelo de responsabilidad compartida para SaaS

El modelo SaaS permite a los usuarios finales acceder a aplicaciones basadas en la nube utilizando una interfaz web u otra interfaz de cliente ligero, sin la necesidad de instalar primero las aplicaciones. Office 365 es un ejemplo de un producto SaaS, como lo son los equipos de Microsoft y otros componentes de Microsoft 365. Si bien Office 365 permite instalar sus aplicaciones de productividad en una computadora cliente, no es necesario que el usuario lo haga. Se puede acceder a las aplicaciones directamente a través de un navegador web, con todo menos los archivos de datos propios del usuario.

a través de la nube



---

### ***Consejo de examen***

El examen MS-900 requiere que comprenda el papel de las arquitecturas públicas, privadas e híbridas, así como los modelos de servicio IaaS, PaaS y SaaS, en la computación en la nube. Sin embargo, asegúrese de comprender también cómo encajan estos elementos con el producto Microsoft 365.

---

---

## **RESUMEN**

---

- La computación en la nube puede proporcionar a las organizaciones muchos beneficios, que incluyen escalabilidad económica, confiabilidad, capacidad de administración y seguridad. Hay tres arquitecturas básicas
- en la nube:
  - **Público** Los recursos en la nube son proporcionados por un proveedor externo en Internet.
  - **Privado** Una organización proporciona sus propios recursos en la nube.
  - **Híbrido** Las arquitecturas públicas y privadas se combinan. Existen tres modelos de servicios en la nube: IaaS, PaaS y SaaS, que especifican qué parte de la administración de recursos es responsabilidad del proveedor de la nube y cuánto es responsabilidad del suscriptor.

---

## **EXPERIMENTO MENTAL**

---

En este experimento mental, demuestre sus habilidades y

conocimiento de los temas tratados en este capítulo. Puede encontrar la respuesta a este experimento mental en la siguiente sección.

Wingtip Toys tiene un sitio web en el que venden sus productos a clientes de todo el mundo; Es la principal fuente de ventas de la empresa. El sitio web está alojado en una granja de servidores en el centro de datos de la compañía, que es una pequeña habitación en el sótano del edificio. El tráfico entrante se distribuye entre los servidores mediante un conmutador de equilibrio de carga. Richard, el administrador del sitio, monitorea regularmente el tráfico del sitio web y, a medida que se acerca la temporada de vacaciones, ve que el nivel de tráfico aumenta casi hasta el punto en que los servidores están abrumados.

No hay presupuesto para la compra de computadoras de servidor web adicionales, y tampoco hay espacio para más servidores en el centro de datos. Al leer sobre las opciones de la nube, Richard piensa que podría haber una solución allí. ¿Cómo puede Richard expandir la granja de servidores web para manejar el aumento del tráfico con el menor gasto utilizando la nube?

## PENSAMIENTO RESPUESTA DEL EXPERIMENTO

---

Por un gasto mínimo, Richard puede crear servidores web adicionales utilizando máquinas virtuales basadas en la nube y agregarlos a su granja de servidores web, formando una arquitectura de nube híbrida. Los servidores basados en la nube pueden

ayuda a manejar el tráfico web de la temporada alta, y cuando los niveles de tráfico bajan, Richard puede eliminar las máquinas virtuales de la granja de servidores hasta que se necesiten nuevamente.

# Capítulo 2. Comprender los servicios y conceptos básicos de Microsoft 365

En el nivel más básico, el producto Microsoft 365 está documentado como consistente en los siguientes componentes:

- Office 365 Enterprise Windows 10
- Enterprise Enterprise Movilidad +
- Seguridad

El objetivo del producto es proporcionar a los usuarios un flujo de trabajo integral que combine servicios basados en la nube, inteligencia artificial y capacidades de aprendizaje automático. Para hacer esto, estos tres componentes en realidad consisten en una variedad de aplicaciones y servicios front-end y back-end, como se describe en las secciones de este capítulo.

## Habilidades en este capítulo:

- Describir los componentes principales de Microsoft 365.
- Compare los servicios principales en Microsoft 365 con los servicios locales correspondientes.

- Comprender el concepto de administración moderna Comprender
- Office 365 ProPlus
- Comprenda la colaboración y la movilidad con Microsoft 365 Describa las capacidades analíticas en Microsoft 365

## HABILIDAD 2.1: DESCRIBA LOS COMPONENTES PRINCIPALES DE MICROSOFT 365

---

Microsoft 365 no es solo una colección de aplicaciones de estaciones de trabajo; Está diseñado más para ser una solución integral de productividad para los usuarios, así como una solución de administración para los administradores. Para los usuarios, el elemento más visible de Microsoft 365 es Office 365 Pro Plus, con las mismas aplicaciones familiares de Outlook, Word, Excel y PowerPoint que probablemente han estado usando durante años. Sin embargo, hay muchos componentes de Microsoft 365 que funcionan debajo de las aplicaciones inmediatamente visibles, que ayudan a proteger a los usuarios y sus datos y les proporcionan servicios inteligentes de comunicación y colaboración.

### Windows 10 Enterprise

Windows 10 es el sistema operativo que permite a los usuarios acceder tanto a las aplicaciones de productividad de Office 365 como a los servicios proporcionados por los otros componentes de Microsoft 365. El producto Microsoft 365 Enterprise

los planes incluyen la edición Enterprise de Windows 10. La edición Enterprise de Windows 10 incluye medidas de seguridad, herramientas de implementación y funciones de administración que van más allá de las de Windows 10 Pro, brindando a los administradores de redes empresariales protección y control centralizados y automatizados sobre flotas de estaciones de trabajo

Algunas de las características adicionales incluidas en Windows 10 Enterprise se describen en las siguientes secciones.

## Seguridad

Todas las ediciones de Windows 10 incluyen Windows Defender, que protege el sistema operativo de varios tipos de ataques de malware. Sin embargo, en comparación con Windows 10 Pro, Windows 10 Enterprise incluye varias mejoras en el software Windows Defender, incluidas las siguientes funciones:

- **Protector de aplicaciones de Windows Defender** Esto permite a los administradores empresariales crear listas de sitios de Internet confiables, recursos en la nube y redes de intranet. Cuando un usuario accede a un sitio no confiable utilizando Microsoft Edge o Internet Explorer, Windows 10 crea automáticamente un contenedor de Hyper-V y abre el recurso no confiable dentro del entorno protegido que proporciona el contenedor. El resultado es que si el recurso no confiable resulta ser malicioso, el atacante está aislado dentro del contenedor y la computadora host permanece protegida.
- **Control de aplicaciones de Windows Defender (WDAC)** Esto proporciona defensa contra aplicaciones maliciosas al revertir el modelo de confianza estándar en el que se supone que las aplicaciones son confiables hasta que

se prueban lo contrario. WDAC evita que un sistema ejecute aplicaciones, complementos, complementos y otros módulos de software que no se hayan identificado como confiables utilizando una política creada con Microsoft Intune o la Política de grupo.

- **Protección contra amenazas avanzada (ATP) de Microsoft Defender**

Windows 10 incluye los componentes del lado del cliente de ATP, un motor privado de prevención, detección y respuesta de amenazas basado en la nube. Windows 10 incluye sensores de comportamiento de punto final, que recopilan información de comportamiento del sistema operativo y la reenvían a los servidores back-end ATP en la nube privada de la empresa para su análisis. ATP también protege los archivos en carpetas clave del sistema contra modificaciones no autorizadas o encriptación por ransomware y otros ataques, aplica técnicas de mitigación de vulnerabilidades para proteger contra amenazas conocidas, mejora la protección de red proporcionada por Windows Defender SmartScreen y realiza una investigación automatizada en tiempo real y remediación de brechas de seguridad.

## Actualizaciones

Windows 10 realiza las actualizaciones del sistema de manera diferente a las versiones anteriores de Windows, reemplazando los principales paquetes de servicio lanzados cada pocos años con actualizaciones de características semestrales. El proceso de actualización de Windows está automatizado de manera predeterminada para el usuario típico de Windows, pero los administradores de red aún pueden intervenir en el proceso con el fin de probar las versiones de actualización antes de que generalmente se implementen.

Microsoft proporciona las siguientes herramientas para la administración de actualizaciones:

- **Windows Update para empresas** Este es un servicio gratuito basado en la nube que permite a los administradores diferir, programar y pausar implementaciones de actualizaciones en estaciones de trabajo específicas. Los administradores pueden usar el

servicio para permitir la instalación de actualizaciones solo en sistemas de prueba designados, y luego implementar las actualizaciones más adelante si no surgen problemas. Si hay problemas con actualizaciones particulares, los administradores pueden pausar sus implementaciones indefinidamente.

- **Servicio de actualización de Windows Server (WSUS)** Este es un servicio gratuito y descargable que permite a los administradores administrar las actualizaciones del sistema internamente descargando versiones a un servidor WSUS a medida que estén disponibles, probándolas según sea necesario y luego implementándolas en estaciones de trabajo en un horario específico. WSUS no solo permite a los administradores ejercer un control completo sobre el proceso de implementación de la actualización, sino que también reduce el ancho de banda de Internet utilizado por el proceso de actualización al descargar versiones solo una vez y luego distribuirlas utilizando la red interna. Los administradores pueden instalar varios servidores WSUS y distribuir las preferencias de actualización y los cronogramas de lanzamiento entre ellos, haciendo que el sistema sea altamente escalable.

Si bien los administradores pueden usar estas herramientas para administrar actualizaciones en estaciones de trabajo que ejecutan cualquier versión de Windows, existen mejoras adicionales para las estaciones de trabajo Windows 10 Enterprise, incluida su capacidad de administración con la herramienta Desktop Analytics. *Analítica de escritorio* es un servicio mejorado que incorpora toda la compatibilidad de actualización y la funcionalidad de monitoreo de actualización de Windows Analytics, junto con una integración más profunda en las herramientas de administración de Microsoft, como System Center Configuration Manager (SCCM) y una interfaz de "panel único" que proporciona a los administradores con una vista completa del estado de actualización de Windows 10 y Office 365.

Algunas de las funciones de monitoreo de actualizaciones compatibles con Desktop Analytics son las siguientes:

- **Preparación de actualización** Desktop Analytics recopila información sobre Windows, Office 365 y otras aplicaciones y controladores, y la analiza para identificar cualquier problema de compatibilidad que pueda interferir con una actualización.
- **Actualización de cumplimiento** Desktop Analytics recopila información de Windows 10 sobre el progreso de las implementaciones de actualizaciones del sistema operativo, así como la firma de Antivirus de Windows Defender y los datos de resultados, la configuración de Windows Update para empresas y los datos de uso de Optimización de entrega. Después de analizar la información, Desktop Analytics informa sobre cualquier problema de cumplimiento de actualizaciones que pueda necesitar atención administrativa.
- **Salud del dispositivo** Una solución de Desktop Analytics que utiliza los datos de diagnóstico mejorados generados por Windows 10 para identificar dispositivos y controladores que causan bloqueos regulares. La herramienta también proporciona soluciones potenciales, como versiones alternativas de controladores o reemplazos de aplicaciones.

*Readeraid:*

## Ventanas

### **Analytics se convierte en Desktop Analytics**

La preparación de actualizaciones, el cumplimiento de actualizaciones y el estado del dispositivo son parte de la herramienta de análisis de Windows disponible en Microsoft Azure. Desktop Analytics es una versión mejorada de la herramienta que se integra con SCCM y proporciona estas mismas funciones para estaciones de trabajo Windows 10 Enterprise.

Windows 10 Enterprise también es compatible con Windows 10 LTSC Access. El canal de servicio a largo plazo (LTSC), anteriormente denominado rama de servicio a largo plazo (LTSB), es un modelo de actualización que los administradores empresariales pueden usar para sistemas de propósito especial que realizan una sola tarea, como los quioscos. Los sistemas LTSC reciben estándar

actualizaciones de calidad mensuales, pero no reciben las actualizaciones semestrales de funciones. Hay actualizaciones de funciones de LTSC disponibles cada dos o tres años, pero los administradores pueden elegir cuándo o si instalarlas. Esto permite que el sistema LTSC mantenga un conjunto de características consistentes a lo largo de su ciclo de vida, de modo que cumpla con su función designada.

## administración

Microsoft 365 proporciona muchas mejoras en el entorno de administración empresarial que permiten a los administradores simplificar el proceso de implementación y configuración de estaciones de trabajo Windows 10 Enterprise. Uno de los objetivos principales de Microsoft 365 es automatizar muchas de las tareas rutinarias que ocupan gran parte del tiempo de un administrador.

- **Piloto automático de Windows** Esta es una característica basada en la nube que está diseñada para simplificar y automatizar el proceso de implementación de estaciones de trabajo con Windows 10 en una red empresarial. En lugar de tener que crear y mantener imágenes y controladores para cada modelo de computadora, Autopilot utiliza configuraciones y políticas basadas en la nube para reconfigurar el sistema operativo instalado por el OEM en una estación de trabajo lista para el usuario, incluso instalando aplicaciones y aplicando una nueva clave de producto para transformar Windows 10 Pro a la edición Windows 10 Enterprise.
- **Virtualización de aplicaciones de Microsoft (App-V)** Esto permite que las estaciones de trabajo de Windows accedan a aplicaciones Win32 que realmente se ejecutan en servidores en lugar de discos locales. Los administradores deben instalar los componentes del servidor App-V y publicar las aplicaciones deseadas. También es necesario un componente de cliente, y Windows 10 Enterprise (versión 1607 o superior) incluye el cliente de App-V de forma predeterminada, por lo que no

Se requiere instalación adicional. Sin embargo, el cliente tiene que estar activado; los administradores pueden activar clientes utilizando la configuración de la directiva de grupo o *Enable-App* cmdlet en Windows PowerShell.

- **Virtualización de experiencia de usuario de Microsoft (UE-V)** Esta es la característica que permite a las estaciones de trabajo de Windows almacenar el sistema operativo personalizado por el usuario y la configuración de las aplicaciones en un recurso compartido de red y sincronizarlas en múltiples dispositivos. Los administradores aún deben instalar los componentes del servidor UE-V, pero a partir de la versión 1607, el cliente UE-V está incluido en la edición Windows 10 Enterprise.

## Windows 10 Business

El plan de negocios de Microsoft 365 no incluye el paquete completo de Windows 10 porque se supone que los posibles implementadores ya tienen o comprarán computadoras con un sistema operativo OEM de Windows instalado. Sin embargo, se requiere Windows 10 para que las estaciones de trabajo del usuario final funcionen con los servicios de Microsoft 365, por lo que el plan de negocios de Microsoft 365 incluye beneficios de actualización a Windows 10 Pro para computadoras que actualmente ejecutan Windows 7 o Windows 8.1 Pro.

Microsoft 365 Business también incluye una mejora llamada Windows 10 Business, que permite que Windows 10 Pro funcione con la administración basada en la nube y los controles de seguridad en Microsoft 365, incluido el piloto automático de Microsoft.

*Nota:*

## Plan Microsoft 365

### Componentes

Para obtener más información sobre los componentes incluidos en los diversos planes de Microsoft 365, vea Capítulo 4, "Comprender los precios y el soporte de Microsoft 365".

"

## Intercambio en línea

Exchange Online es una implementación basada en la nube del producto de servidor de colaboración y mensajería insignia de Microsoft. Todos los planes de Microsoft 365 Enterprise y Microsoft 365 Business incluyen acceso a Exchange Online para todos sus usuarios. Esto elimina la necesidad de que las organizaciones instalen y mantengan sus propios servidores de Exchange locales.

Al igual que con Microsoft Azure, Exchange Online usa servidores compartidos en los centros de datos de Microsoft para alojar los buzones y otros servicios para múltiples suscriptores. Los servicios de Exchange Online disponibles incluyen lo siguiente:

- **Buzones** A cada usuario se le proporciona almacenamiento de correo, cuya cantidad se basa en el plan Microsoft 365. Un archivo in situ proporciona almacenamiento adicional para el correo. Exchange también admite buzones compartidos para grupos de usuarios que comparten la responsabilidad del correo entrante.
- **Calendarios** Los usuarios pueden mantener eventos y compartir

ellos con otros usuarios para crear un entorno unificado de programación y colaboración.

- **Calendarios compartidos** Los usuarios pueden compartir sus calendarios para programar, gestionar tareas y reservar salas de conferencias. Exchange Online también proporciona una libreta de direcciones global, administración de grupos y delegación de buzones.
- **Exchange Online Protection (EOP)** EOP analiza el correo electrónico entrante en busca de spam y código malicioso y reenvía, elimina o pone en cuarentena los mensajes potencialmente peligrosos según las reglas establecidas por los administradores.
- **Mensajería unificada (UM)** La mensajería unificada permite a los administradores combinar mensajes de correo electrónico con correo de voz, de modo que ambos tipos de mensajes se almacenan en un único buzón para cada usuario. La mensajería unificada proporciona funciones estándar de correo de voz, incluida la respuesta de llamadas, y permite a los usuarios escuchar sus mensajes desde la Bandeja de entrada de Outlook o mediante Outlook Voice Access desde cualquier teléfono.
- **Prevención de pérdida de datos (DLP)** DLP permite a los administradores crear políticas DLP que protegen la información confidencial de la empresa mediante el análisis de contenido profundo para filtrar el tráfico de mensajes en función de palabras clave, expresiones regulares, términos de diccionario y otros criterios, y luego tomar acciones específicas en función del tipo de información detectada. Por ejemplo, una política de DLP puede identificar mensajes de correo electrónico que contienen números de tarjetas de crédito y notificar al remitente, cifrar los mensajes o bloquearlos directamente. Las políticas más complejas pueden identificar tipos específicos de documentos de la compañía y usar huellas digitales virtuales para identificar su fuente.

Microsoft mantiene dos planes de suscripción de Exchange Online: el Plan 1 que se incluye con Microsoft 365 Business y el Plan 2, que tiene características adicionales y se incluye con Microsoft 365 Enterprise. Las características incluidas en cada plan se enumeran en Tabla 2-1 .

## CUADRO 2-1 Planes de Exchange Online para Microsoft 365

INTERCAMBIO PLAN EN LÍNEA 1 (MICROSOFT 365 BUSINESS)	INTERCAMBIO PLAN EN LÍNEA 2 (MICROSOFT 365 ENTERPRISE)
50 GB de almacenamiento de buzones por usuario	100 GB de almacenamiento de buzones por usuario
Archivo en el lugar	Almacenamiento de usuario adicional ilimitado en el archivo local
Acceda a través de Outlook de escritorio, Outlook en la web y Outlook Mobile	Acceda a través de Outlook de escritorio, Outlook en la web y Outlook Mobile
Calendarios de usuarios individuales	Calendarios de usuarios individuales
Calendarios compartidos	Calendarios compartidos
Protección en línea de Exchange	Protección en línea de Exchange
	Mensajería unificada
	Prevención de pérdida de datos

Los usuarios pueden acceder a los servicios de Exchange Online utilizando la aplicación Microsoft Outlook incluida con Office 365, el cliente Outlook basado en la web o Outlook Mobile. Esto permite a los usuarios acceder a su correo, calendarios y otros servicios con prácticamente cualquier dispositivo, incluidos teléfonos inteligentes y tabletas con iOS, Android o

## Windows 10

Los administradores de Microsoft 365 no tienen acceso directo a los servidores de Exchange Online, pero pueden acceder al Centro de administración de Exchange desde un enlace en el Centro de administración de Microsoft 365 para administrar la configuración específica del intercambio mediante una interfaz basada en web, como se muestra en Figura 2-1 .

---



**FIGURA 2-1** La interfaz del Centro de administración de Exchange

En esta interfaz, los administradores pueden realizar tareas como las siguientes:

- Crear y administrar cuentas de usuario
- Conceder permisos de rol de administración para administradores y usuarios

- Configure las opciones de flujo de correo para integrar servidores de correo locales o servicios de correo de terceros en la solución de gestión de mensajes. Habilite el uso compartido del calendario
  - con organizaciones externas o entre usuarios locales y en la nube.
- 
- Administre libretas de direcciones jerárquicas y sin conexión, listas de direcciones y políticas de libretas de direcciones
  - Crear y administrar una jerarquía de carpetas públicas para compartir documentos y colaborar
  - Cree y administre reglas de acceso de clientes para restringir el acceso a Exchange Online según la plataforma del cliente, la dirección IP, el tipo de autenticación, la ubicación y otros criterios.

## SharePoint en Línea

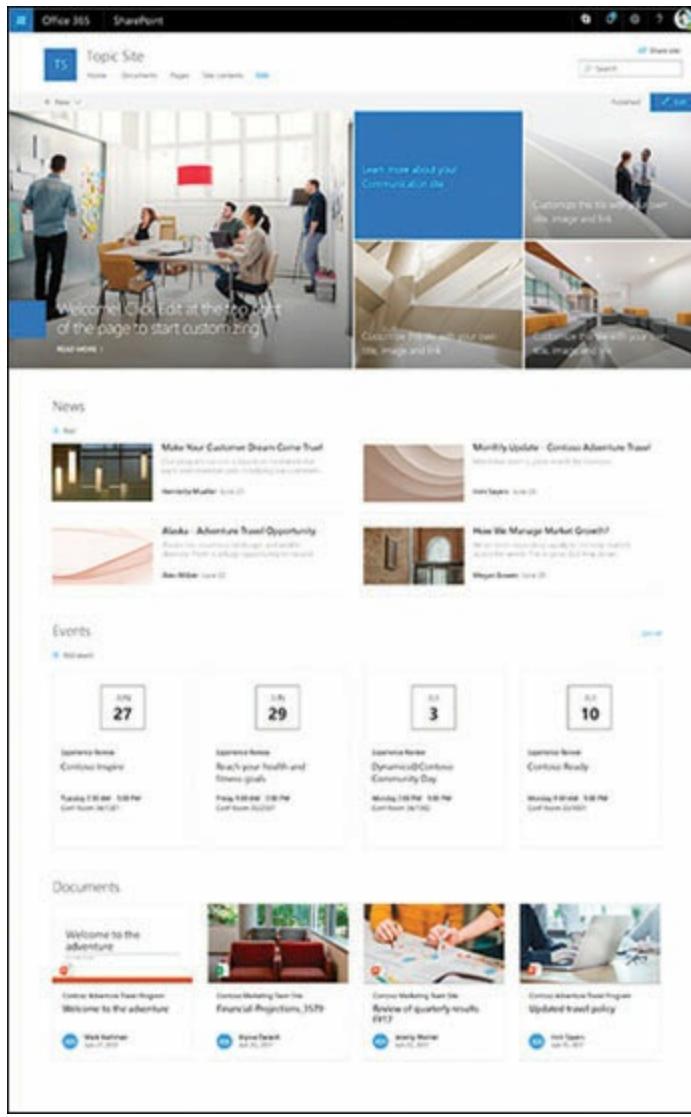
Microsoft SharePoint es una herramienta de colaboración basada en la web que se introdujo originalmente en 2001 como un producto de servidor local. SharePoint Online es el equivalente basado en la nube que se incluye con todos los planes de Microsoft 365.

SharePoint Online es un servicio que los administradores y los trabajadores pueden usar para crear sitios web para la administración, distribución y colaboración de documentos. En su forma más simple, los usuarios de SharePoint Online pueden crear una biblioteca de documentos en la web y cargar sus archivos. Los archivos son accesibles desde cualquier dispositivo que tenga acceso al sitio. Como SharePoint Online es parte de Office

365, la edición de un documento de biblioteca lo abre en la aplicación de Office adecuada, ya sea instalada en un escritorio o parte de Office Online.

Los usuarios pueden compartir sus archivos de biblioteca con otros usuarios con diferentes grados de acceso al asignarles permisos. Un escenario en el que una organización o usuario desea publicar documentos en una biblioteca para que accedan muchos usuarios se denomina *sitio de comunicación*. Por ejemplo, una empresa podría usar SharePoint Online para crear una biblioteca de documentos de recursos humanos para que todos los empleados puedan acceder. SharePoint incluye capacidades de personalización que permiten a los administradores diseñar sitios web con componentes gráficos modernos, como se muestra en Figura 2-2. .

---

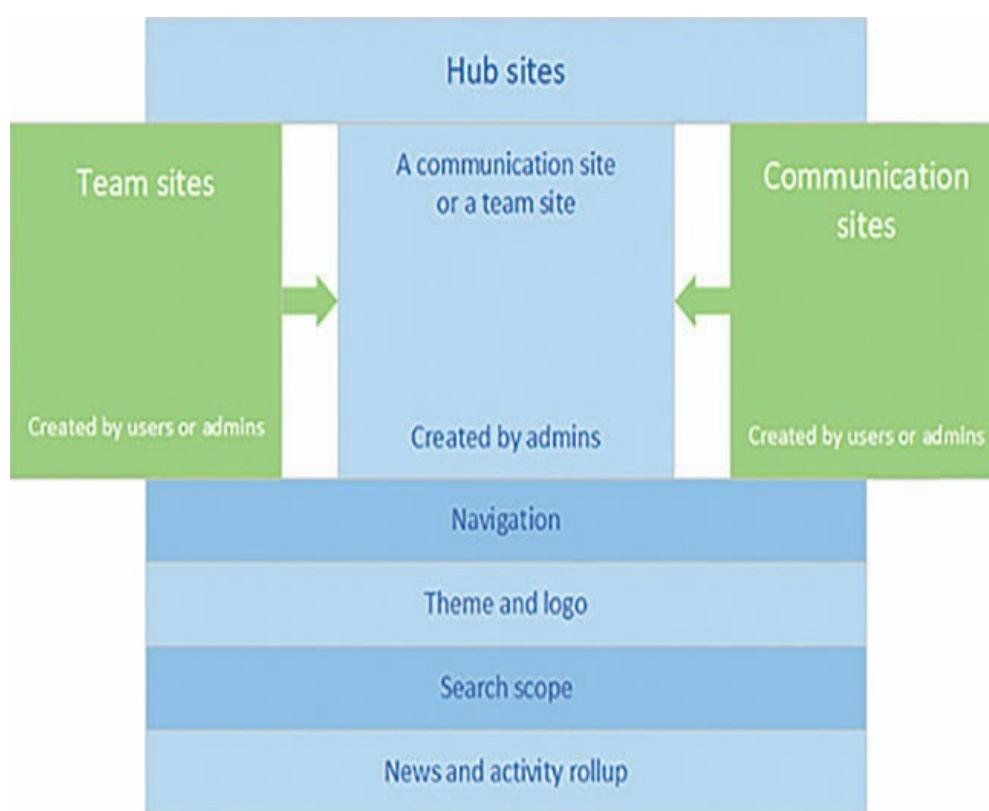


**FIGURA 2-2** Un ejemplo de sitio de SharePoint Online

Aún más útil, varias personas pueden editar un solo documento de SharePoint Online al mismo tiempo, proporcionando un entorno de colaboración que permite a los grupos trabajar juntos. Al crear un *sitio del equipo*, un grupo designado de usuarios puede trabajar simultáneamente en documentos a los que solo ellos pueden acceder. SharePoint

mantiene múltiples versiones de los archivos en una biblioteca, para que los usuarios puedan revisar las iteraciones de un documento a lo largo de su historial.

Los sitios de comunicación y los sitios de equipo están vinculados en SharePoint Online por *sitios centrales*, que proporcionan navegación centralizada a los sitios subordinados y búsqueda aguas abajo. El servicio de SharePoint Online incluido en Microsoft 365 puede alojar múltiples sitios de hub, colaboración y grupos, como se muestra en Figura 2-3 .



**FIGURA 2-3** Tipos de sitios de SharePoint Online

Debido a que SharePoint Online está integrado con los otros componentes de Microsoft 365, los usuarios pueden tomar

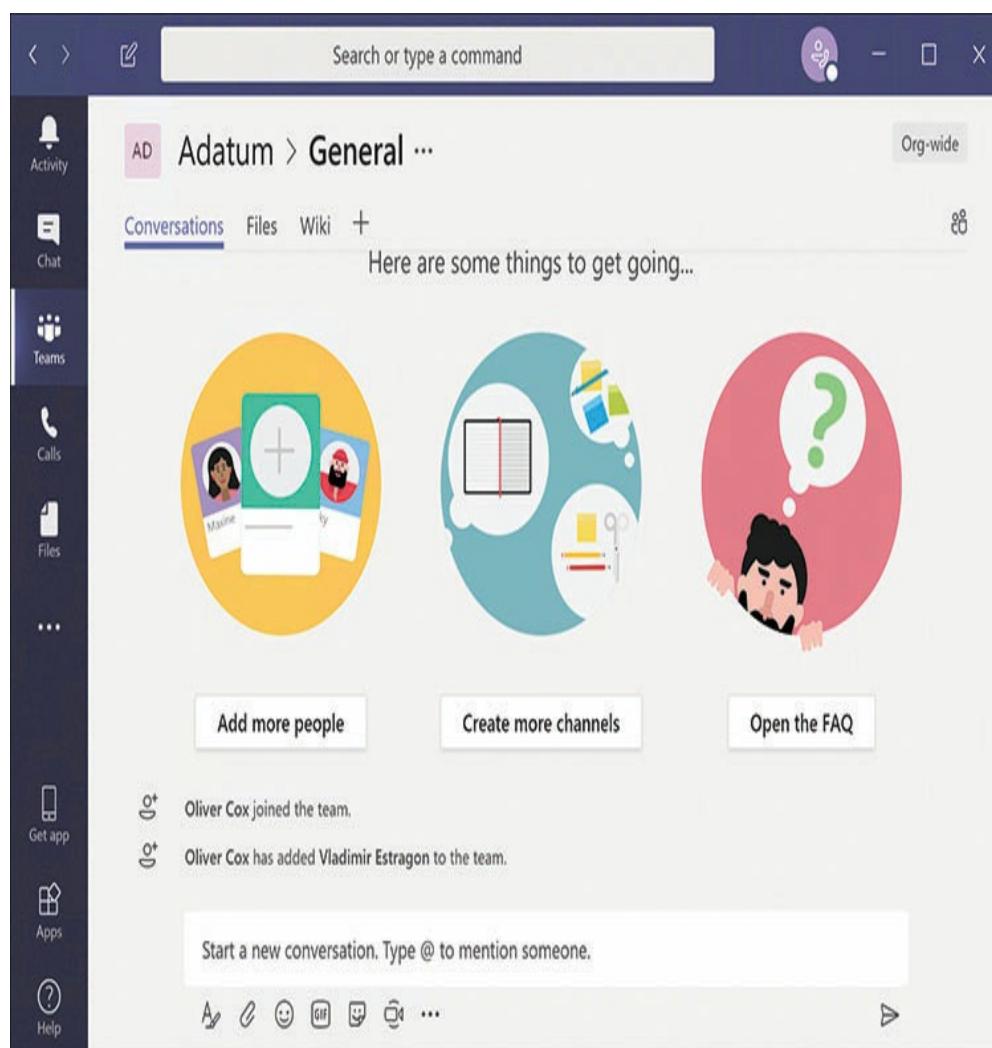
ventaja de sus características de seguridad y capacidad de administración. Los documentos cargados en los sitios de SharePoint Online están protegidos contra el código malicioso por el mismo motor antimalware utilizado por Exchange, así como por la Prevención de pérdida de datos. La integración de Outlook permite a los usuarios programar eventos de equipo y entregarlos en los calendarios de los miembros. SharePoint también puede controlar la pertenencia a grupos y los permisos de documentos con identidades de usuario tomadas de Active Directory y Azure Active Directory.

El plan de SharePoint Online incluido con Microsoft 365 Enterprise incluye 1 TB de almacenamiento para la organización más 10 GB por cada licencia comprada. Una organización también puede comprar almacenamiento adicional, hasta un máximo de 25 TB por colección de sitios. Una organización puede crear hasta un millón de colecciones de sitios.

Una biblioteca de SharePoint Online puede tener hasta 30 millones de archivos y carpetas, aunque existen limitaciones cuando el número supera los 100.000. Los archivos individuales pueden tener un tamaño de hasta 15 GB, y SharePoint puede mantener hasta 50,000 versiones de cada archivo. Los grupos de SharePoint pueden tener hasta 5,000 usuarios, y un usuario puede ser miembro de hasta 5,000 grupos. Por lo tanto, SharePoint Online puede admitir enormes instalaciones que atienden hasta 500,000 usuarios.

## Equipos de Microsoft

Microsoft Teams es otra herramienta de colaboración multiplataforma incluida con Microsoft 365 que permite a los usuarios comunicarse y trabajar juntos en tiempo real, utilizando bibliotecas de documentos, chat grupal y privado, reuniones programadas y no programadas y llamadas de audio / video. Teams es una interfaz de cliente que funciona junto con los otros servicios de Microsoft 365 para crear un entorno de colaboración unificado, como se muestra en Figura 2-4. .



## FIGURA 2-4 La interfaz de escritorio de Microsoft Teams

El cliente de Teams proporciona chat en tiempo real y la capacidad de hacer y recibir llamadas, pero las otras herramientas incorporadas en el cliente son proporcionadas por otros servicios de Microsoft 365, como se muestra en Figura 2-5 .



## FIGURA 2-5 Servicios de Microsoft 365 utilizados por los equipos de Microsoft

La funcionalidad de mensajería que proporciona Teams permite a los usuarios crear *canales*, que son sesiones de chat individuales compartidas por los miembros de un equipo. Un canal permite a sus miembros publicar texto e imágenes, así como información de servicios externos de redes sociales. La mensajería de equipos es un servicio independiente que no se basa en la comunicación por correo electrónico o SMS. Teams también admite la transmisión de mensajes privados uno a uno entre usuarios.

La capacidad de llamadas en Teams puede usar Voz sobre IP (VoIP) o conexiones estándar de red telefónica pública conmutada (PSTN). La videoconferencia también es posible dentro del software cliente de Teams. Office 365 proporciona

Equipos con acceso a funciones como el sistema telefónico, el enrutamiento directo y el plan de llamadas, que pueden realizar funciones que normalmente se dejan al hardware de telefonía estándar, como una centralita privada (PBX).

La membresía y autenticación en Microsoft Teams es proporcionada por grupos de Office 365, que almacenan su información de identidad en Azure Active Directory. Los equipos pueden almacenar sus documentos y otros archivos en la nube utilizando OneDrive para la Empresa. Los sitios web de Team, implementados usando SharePoint Online, también son accesibles a través del cliente Teams. Los buzones de grupo y la programación de eventos y reuniones son proporcionados por Exchange Online y se accede a ellos a través de Outlook. Para organizar y preservar reuniones en video, Teams puede usar el servicio Microsoft Stream.

Teams es altamente escalable y puede admitir entornos colaborativos que van desde pequeños grupos de trabajo hasta grandes departamentos, hasta presentaciones gigantescas, seminarios web y conferencias. Teams también es personalizable, lo que permite a los administradores incorporar aplicaciones y servicios de terceros en el entorno colaborativo de un equipo. Por ejemplo, varios proveedores están trabajando en soluciones de videoconferencia H.323 que permitirán a los equipos colaborar con socios externos.

*Nota:*

## **Microsoft Teams es**

### **Reemplazar Skype Empresarial en línea**

**La mensajería instantánea, las reuniones y las funciones de voz y video entre pares que antes brindaba el servicio Skype Empresarial Online ahora se están incorporando a los equipos de Microsoft. Skype for Business Online está en desuso. Los usuarios actuales deben cambiar a Microsoft Teams cuando vencen sus términos actuales de Skype Empresarial Online.**

## **Movilidad empresarial + seguridad**

Microsoft 365 es un conjunto de aplicaciones que está diseñado para proporcionar a los usuarios capacidades avanzadas de colaboración multiplataforma. Para lograr este fin, el producto incorpora dos tecnologías actuales que introducen nuevos problemas de seguridad y control de acceso: la nube y los dispositivos informáticos portátiles. Para que las características resaltadas en Microsoft 365 funcionen como se esperaba, los usuarios deben poder acceder a sus colegas y sus datos desde cualquier ubicación, utilizando cualquier dispositivo. Para los administradores de Microsoft 365, los usuarios deben poder hacer su trabajo de forma segura y confiable, incluso cuando utilizan dispositivos no suministrados por la compañía.

Debido a que Microsoft 365 lleva a la empresa más allá del perímetro físico de la organización y hacia la nube, así como hacia los bolsillos y bolsos de los usuarios, una nueva seguridad

Se necesita un paradigma, que es proporcionado por *Enterprise Mobility + Security (EMS)*. EMS es un conjunto de gestión y seguridad basado en la nube que consta de varios componentes que eran productos separados al mismo tiempo. Juntos, estos componentes proporcionan servicios a Microsoft 365 en las siguientes áreas principales:

- Gestión de identidad y acceso Gestión de dispositivos
- móviles y aplicaciones Gestión y protección de la
- información Ciberseguridad y gestión de riesgos
- 

Los componentes que componen EMS se describen en las siguientes secciones.

## Azure Active Directory Premium

Active Directory (AD) es un servicio de directorio que ha sido parte del producto Windows Server desde el lanzamiento de Windows 2000 Server. Un servicio de directorio es una base de datos de objetos, incluidos usuarios y computadoras, que proporciona servicios de autenticación y autorización para recursos de red. *Azure Active Directory (Azure AD o AAD)* es un equivalente basado en la nube que puede proporcionar a los usuarios de Microsoft 365 la capacidad de inicio de sesión único que les permite acceder a todas sus aplicaciones y servicios SaaS, incluidos Office 365 y cualquier producto de terceros que los administradores hayan integrado en su entorno Microsoft 365, desde cualquier dispositivo, en cualquier

ubicación.

Azure AD proporciona una implementación de Microsoft 365 con servicios de administración de identidad y acceso que se extienden más allá de la red local a la nube. Azure AD mejora la seguridad del entorno de Microsoft 365 al admitir la autenticación multifactor, que requiere que los usuarios verifiquen sus identidades de dos o más formas, como con una contraseña y un factor biométrico, como una huella digital.

Azure AD también puede proporcionar servicios de autenticación y autorización para recursos internos, como aplicaciones y servicios locales. Para las organizaciones con una infraestructura de AD basada en Windows Server existente, Azure AD puede conectarse a controladores de dominio internos, para crear una solución de servicio de directorio híbrido que comparta las ventajas de ambas implementaciones.

#### *¿Necesita más revisión?*

Para obtener más información sobre cómo Azure Active Directory proporciona servicios de seguridad a un entorno de Microsoft 365, vea Capítulo 3 , " Comprenda la seguridad, el cumplimiento, la privacidad y la confianza en Microsoft 365 . "

## **Microsoft Intune**

*Microsoft Intune* es una herramienta de gestión de dispositivos y aplicaciones basada en la nube que se integra con el

funciones de autenticación y autorización proporcionadas por Azure Active Directory. Si bien los administradores pueden usar Intune para administrar sus computadoras y aplicaciones internas, la principal innovación del producto es su capacidad para administrar BYOD o dispositivos de propiedad del usuario, como teléfonos inteligentes, tabletas y computadoras portátiles, y permitirles acceder a Servicios protegidos de la organización, aplicaciones y datos de forma segura.

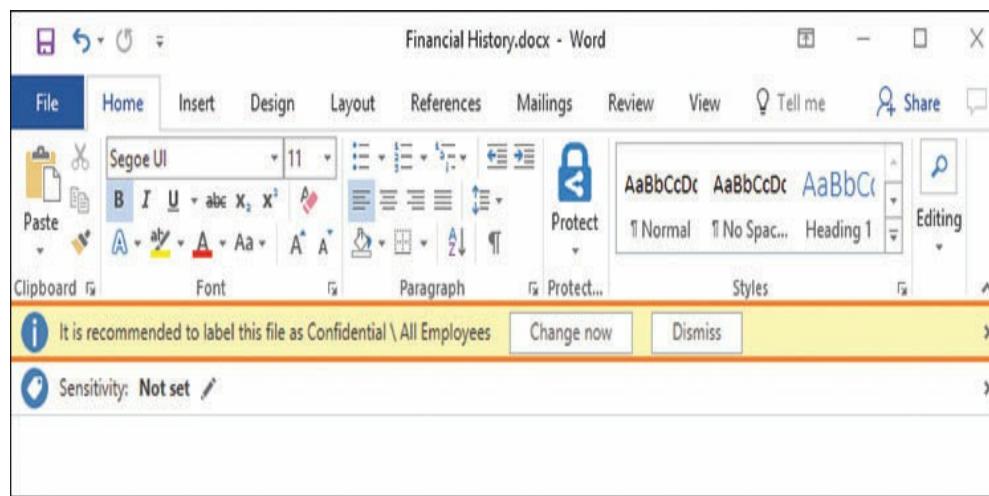
Intune puede administrar dispositivos que ejecutan cualquiera de los principales sistemas operativos móviles, incluidos Android, iOS, MacOS y, por supuesto, Windows. Con Intune, incluso los sistemas operativos que no pueden unirse a un dominio de Active Directory pueden acceder a recursos protegidos. Intune utiliza los protocolos y API del sistema operativo móvil para comunicarse, creando un inventario de dispositivos que pueden acceder a las aplicaciones y datos de la compañía.

Los administradores pueden usar Intune para crear estándares para la configuración de los ajustes de seguridad que un dispositivo debe cumplir antes de poder acceder a los recursos protegidos. Por ejemplo, un administrador puede requerir que un dispositivo use un tipo particular de autenticación o especificar que solo ciertas aplicaciones puedan acceder a los datos de la compañía. Intune incluso puede garantizar que los datos confidenciales se eliminen de un dispositivo cuando una aplicación se cierra. Este tipo de control permite a Microsoft 365 mantener la seguridad de sus recursos sin la necesidad de que los administradores tomen el control completo sobre los dispositivos propiedad de los usuarios.

## Protección de la información de Azure

*Protección de la información de Azure (AIP)* es un sistema que permite a los usuarios y administradores aplicar etiquetas a documentos y correos electrónicos que clasifican la información que contienen. Las etiquetas se pueden configurar para especificar cómo las aplicaciones tratan la información y, opcionalmente, tomar medidas para protegerla.

AIP puede aplicar etiquetas a documentos específicos, o puede seguir las reglas creadas por los administradores para identificar datos confidenciales en cualquier documento. Por ejemplo, un administrador puede crear una regla que identifique patrones de datos asociados con números de tarjeta de crédito o de seguridad social en un documento de Word a medida que un usuario lo crea. Cuando el usuario intenta guardar el documento, AIP le advierte que aplique la etiqueta, como se muestra en Dibujo 26 .



**FIGURA 2-6** Una recomendación de etiquetado AIP en un documento de Word

Los administradores también pueden configurar las etiquetas AIP para que sean visibles en los documentos a los que se aplican. Cuando un usuario acepta clasificar un documento como confidencial, la aplicación puede aplicar una marca de agua u otro indicador visual, que persistirá en el documento donde sea que esté almacenado.

AIP también puede usar *Administración de derechos de Azure (Azure RMS)* para proteger documentos o correos electrónicos que han sido etiquetados como sensibles. Según las reglas creadas por los administradores, los documentos etiquetados por AIP pueden protegerse mediante cifrado, restricciones de identidad, políticas de autorización y otros métodos. Por ejemplo, cuando un mensaje de correo electrónico contiene datos confidenciales, AIP puede ejercer control sobre la aplicación del cliente de correo electrónico, evitando que los usuarios hagan clic en **Responder a todos** o

**Adelante** botón. De la misma manera, AIP puede restringir los documentos de Office 365 a un estado no imprimible o de solo lectura.

## Análisis avanzado de amenazas de Microsoft

Advanced Threat Analytics (ATA) es una solución local que utiliza información recopilada de una amplia variedad de fuentes empresariales y la utiliza para anticipar, detectar y reaccionar ante amenazas y ataques de seguridad. ATA recibe información de registro y eventos de los sistemas Windows, y también captura el tráfico de red generado por protocolos relacionados con la seguridad, como Kerberos y NTLM.

Este tráfico proporciona a ATA información sobre los patrones de autenticación y autorización de usuarios.

Con esta información recopilada, ATA crea perfiles de aplicaciones, servicios y usuarios. Al examinar el comportamiento normal de estas entidades, ATA puede detectar un comportamiento anómalo cuando ocurre y determinar si ese comportamiento es sospechoso, en base a patrones de ataque conocidos. Cuando sospecha o detecta una violación de seguridad, ATA muestra una alerta en el panel de ATA, como la que se muestra en Figura 2-7 .

Suspicion of identity theft based on abnormal behavior

Almeta Whitfield exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 16 abnormal workstations.
- Requested access to 5 abnormal resources.

18:10 10 May 2017

```
graph LR; User[User: Almeta Whitfield<br/>Software Engineer] -- On --> Computer1[9 normal computers]; User -- On --> Computer2[16 abnormal computers]; Computer1 -- Accessed --> Resource1[13 normal resources]; Computer2 -- Accessed --> Resource2[5 abnormal resources]
```

1 of 8

**FIGURA 2-7** Una alerta de Microsoft Advanced Threat Analytics sobre comportamiento anormal

ATA es una de varias tecnologías de Microsoft 365 que utiliza inteligencia avanzada para anticipar las necesidades de los usuarios antes de que ocurran. En este caso, la necesidad es de intervención, ya sea automatizada o humana, en una situación de seguridad potencialmente peligrosa.

## **Seguridad de aplicaciones en la nube**

La investigación de Microsoft ha determinado que, de los cientos de aplicaciones en la nube que utilizan las grandes empresas en la actualidad, un gran porcentaje de ellas son desconocidas para el departamento de TI y, por lo tanto, no son administradas por ellas. Microsoft ha comenzado a llamar a estas aplicaciones clandestinas en la nube Shadow IT, y obviamente presentan un peligro para la seguridad.

Cloud App Security es un producto de agente de seguridad de acceso a la nube (CASB) que permite a los administradores de Microsoft 365 escanear sus redes en busca de las aplicaciones en la nube a las que acceden los usuarios, evaluar su vulnerabilidad de seguridad y administrarlas de manera continua.

Cloud App Security examina los registros de tráfico y la información de firewall y proxy para descubrir las aplicaciones en la nube en uso. Después de determinar si las aplicaciones presentan un peligro para los datos, las identidades u otros recursos, los administradores pueden sancionar o anular la aplicación de aplicaciones específicas para permitir o impedir el acceso de los usuarios a ellas. Para las aplicaciones que los administradores han sancionado, Cloud App Security utiliza las propias API de las aplicaciones para conectarse a ellas y monitorearlas.

actividad del usuario.

### **Protección contra amenazas avanzada de Azure**

Al igual que con la función de Protección contra amenazas avanzada de Microsoft Defender incluida en Windows 10, Microsoft Azure tiene su propio ATP, al igual que Office 365, Exchange Online, SharePoint Online, Teams y OneDrive. Cada motor ATP está diseñado para usar inteligencia artificial para prevenir, detectar y responder a las amenazas de seguridad únicas de su entorno. En Azure, la vulnerabilidad principal son las identidades almacenadas en Azure Active Directory, por lo que el motor ATP de Azure busca un comportamiento anómalo del usuario y lo compara con los patrones estandarizados utilizados por los atacantes.

## **HABILIDAD 2.2: COMPARAR LOS SERVICIOS BÁSICOS EN MICROSOFT 365 CON LOS SERVICIOS CORRESPONDIENTES EN LAS INSTALACIONES**

---

Microsoft 365 se basa principalmente en servicios en la nube, pero algunos de los servicios también están disponibles como productos locales. Por ejemplo, una organización puede usar Exchange Online para correo electrónico y programación o instalar sus propios servidores y ejecutar una versión local de Exchange. Lo mismo es cierto para SharePoint Online, Azure Active Directory y Office 365. Como con cualquier

situación de compensación, hay ventajas y desventajas para ambas partes.

## Despliegue

Un servicio basado en la nube siempre es más sencillo de implementar que un producto basado en servidor local porque el servicio se proporciona al suscriptor en un estado instalado y operativo. No es necesario diseñar una infraestructura, obtener hardware o instalar software de servidor. Un administrador puede comenzar a trabajar con el servicio inmediatamente después de suscribirse, creando objetos de usuario, buzones de Exchange o sitios de SharePoint que estén funcionando en minutos, en lugar de días o semanas.

## Actualizaciones

Una ventaja significativa de usar la versión basada en la nube de cualquiera de estas aplicaciones o servicios es que se actualizan de forma regular y automática con la última versión del software. Los administradores se sienten aliviados de la necesidad de descargar, evaluar e implementar actualizaciones a medida que se lanzan. Con una solución basada en la nube, una organización se suscribe a un servicio, no a un producto de software, por lo que el proveedor es responsable de mantener y actualizar la funcionalidad del servicio. En muchos casos, la versión de un servicio basada en la nube recibe nuevas características antes y el software local

Es posible que los productos no reciban ciertas características.

Para una instalación de servicio local, una estrategia de actualización responsable requiere la prueba y evaluación de nuevas versiones de software y puede requerir tiempo de inactividad del servicio para las implementaciones de actualización reales.

## Costo

El costo es otro factor decisivo en el despliegue de cualquiera de estos servicios. Los servicios basados en la nube requieren el pago de una tarifa de suscripción regular y, a veces, hay tarifas adicionales para las funciones adicionales. Esto permite que una organización implemente un servicio con un desembolso inicial mínimo, ya que no se requieren costos de hardware ni licencias de servidor.

Las tarifas por servicios basados en la nube son predecibles y simplifican el proceso de presupuestación. Instalar el servicio local equivalente es un asunto más complicado. Obviamente, una organización primero debe comprar la licencia de software del servidor y las computadoras en las que se ejecutará el software, así como una licencia de sistema operativo y licencias de acceso de cliente para todos los usuarios. Esto puede ser un desembolso inicial significativo.

Dependiendo de los requisitos de la organización, también puede haber costos adicionales. Una empresa grande puede requerir múltiples servidores para soportar diferentes sitios físicos, lo que multiplica la inicial

costo de desembolso. Hacer una copia de seguridad de los datos y almacenarlos también aumenta el costo.

También hay que considerar los problemas de tolerancia a fallas y recuperación ante desastres. La mayoría de los servicios basados en la nube de Microsoft se suministran con un acuerdo de nivel de servicio (SLA) del 99.9% de forma predeterminada. Esto significa que el servicio no experimentará más del 0.1% del tiempo de inactividad en un período determinado. La infraestructura que utiliza Microsoft para mantener ese rendimiento constante no preocupa al suscriptor. Duplicar ese nivel de rendimiento con servidores locales requerirá hardware redundante y posiblemente incluso centros de datos redundantes. No todas las organizaciones requieren este mismo nivel de rendimiento constante, pero incluso una garantía de tiempo de actividad más modesta aumentará el gasto para una solución local.

Finalmente, está el problema de las personas necesarias para diseñar, instalar y mantener servicios locales. Por ejemplo, implementar servidores de Exchange no es una simple cuestión de instalar el software y crear cuentas de usuario. Dependiendo del tamaño de la organización, es posible que se necesiten varios servidores en cada ubicación, y el proceso de diseño y configuración puede requerir habilidades avanzadas. Estas personas serán un gasto continuo durante toda la vida del servicio.

Si bien los servicios basados en la nube pueden proporcionar una gran cantidad de rendimiento por el precio, esto no quiere decir que sean

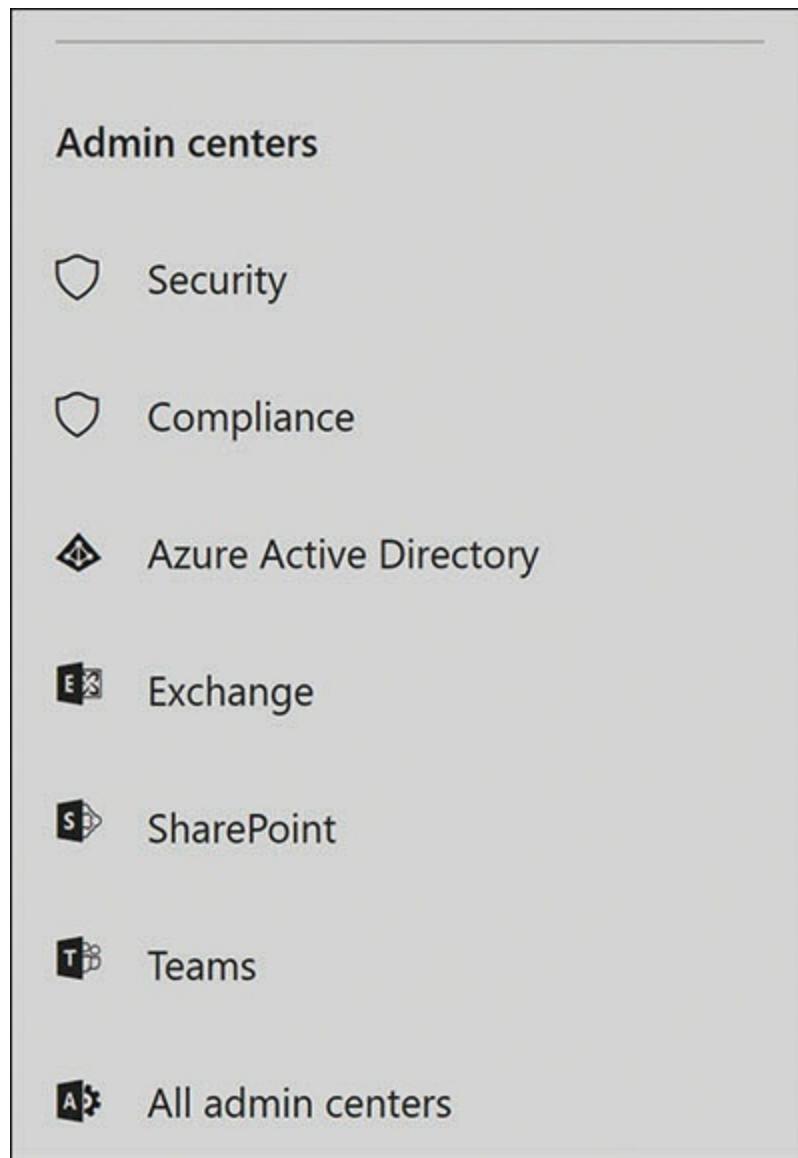
siempre más barato que los servidores locales. A largo plazo, los servicios basados en la nube pueden llegar a un punto en el que son más caros. Las tarifas de servicio en la nube son continuas y perpetuas, y aunque los gastos para servidores locales pueden comenzar con un gran desembolso inicial, pueden reducirse a un nivel mucho más bajo una vez que los servidores y el software se hayan comprado e implementado.

Una comparación de los costos relativos también depende de los requisitos de la organización y su infraestructura existente. Para una gran empresa que ya mantiene centros de datos en múltiples ubicaciones con personal experimentado, la implementación de un nuevo servicio interno puede ser relativamente asequible. Para una compañía recién formada sin infraestructura de TI existente, el desembolso inicial para un servicio local podría no ser factible.

## Administración

En comparación con los administradores de servidores locales, que pueden trabajar directamente con los controles del software del servidor, los administradores de Microsoft 365 trabajan con servicios en la nube utilizando interfaces remotas basadas en la web. El Centro de administración de Microsoft 365 proporciona acceso a las diversas herramientas para todos los servicios incluidos en el producto, como el Centro de administración en línea de Exchange y el Centro de administración en línea de SharePoint, como se muestra en Figura 2-8. . Estas herramientas lo hacen

es posible administrar configuraciones de configuración y crear recursos virtuales, como buzones y objetos de servicio de directorio.



**FIGURA 2-8** Acceso al centro de administración a través de Microsoft 365

Sin embargo, los administradores de servicios en la nube no

tener acceso a los recursos subyacentes en los que se ejecutan los servicios. No pueden acceder al sistema operativo de las computadoras en las que se ejecutan sus servicios, ni tienen acceso directo a los archivos y bases de datos que forman sus entornos de servicio. Por ejemplo, aunque los administradores pueden crear buzones para usuarios en el Centro de administración en línea de Exchange, no tienen acceso a las bases de datos de buzones que contienen los mensajes de los usuarios. La experiencia puede ser similar a la de un piloto acostumbrado a sentir la retroalimentación táctil de los controles mecánicos de un avión que de repente tiene que pasar a los controles indirectos de un sistema de "vuelo por cable".

Las interfaces basadas en web no son necesariamente un inconveniente para todos los administradores. Es completamente posible administrar un servicio basado en la nube sin necesidad de acceder a las estructuras de datos subyacentes del servicio. Además, Microsoft mantiene la responsabilidad de esas estructuras de datos, garantizando su disponibilidad y seguridad. En una implementación de servicio local, corresponde a los administradores locales replicar las estructuras de datos para disponibilidad e implementar una solución de equilibrio de carga para mantener un nivel similar de rendimiento.

Aquí nuevamente, las diferencias entre los dos entornos de servicio dependen de la experiencia y las preferencias de las personas responsables de ellos. Los administradores con experiencia de Exchange Server, por ejemplo, podrían ser

Tenga cuidado con el uso de una implementación de Exchange basada en la nube que los aislaría de los servidores, el sistema operativo y los controles tradicionales de Exchange. Sin embargo, un administrador relativamente nuevo en Exchange podría recibir con agrado el acceso simplificado que proporciona el Centro de administración en línea de Exchange.

## Seguridad

Uno de los factores más críticos en la decisión de utilizar servicios locales o basados en la nube es la ubicación de datos confidenciales. Para muchas organizaciones, la seguridad de sus datos no es solo una cuestión de su propio beneficio. En algunos casos, las restricciones contractuales y legales pueden hacer que el almacenamiento de datos basado en la nube sea imposible. Una empresa con un contrato con el gobierno, por ejemplo, podría estar obligada a mantener la responsabilidad personal de sus datos almacenados; no pueden pasar esa responsabilidad a un proveedor de la nube de terceros.

Sin embargo, en los casos en los que no existen restricciones legales, el almacenamiento de datos en la nube puede proporcionar una protección equivalente a varios productos de seguridad locales diferentes. La protección antivirus, el cifrado de mensajes, la gestión de los derechos de información y la prevención de pérdida de datos son solo algunos de los mecanismos de seguridad que pueden proporcionar los servicios en la nube de Microsoft 365, todos los cuales requerirían más

mantenimiento y gastos a implementar para servidores locales.

## Servicio de comparaciones

No todos los servicios en la nube incluidos en Microsoft 365 están disponibles en versiones locales. Microsoft Teams y Microsoft Streams, por ejemplo, solo existen como servicios en la nube. Sin embargo, algunos de los servicios centrales de Microsoft 365 han existido como productos de software de servidor independiente durante años, y las organizaciones que planean una implementación de Microsoft 365 pueden querer comparar los servicios en la nube con sus correspondientes versiones locales, como en las secciones siguientes, antes de comprometerse con o el otro

## Oficina 365

El conjunto de aplicaciones de Microsoft Office es una colección de aplicaciones de productividad que ha estado disponible como producto independiente durante muchos años. Office 365 se introdujo luego como un producto basado en suscripción que permite a los usuarios acceder a las mismas aplicaciones de varias maneras diferentes. En la mayoría de los planes de Office 365, todavía es posible instalar las aplicaciones en una computadora para uso en línea o sin conexión, pero también están disponibles en la nube para usar en cualquier dispositivo, utilizando un navegador web. Además, también hay versiones que no son de Windows de las aplicaciones disponibles para su uso en dispositivos Android e iOS.

Con el producto independiente de Office, actualmente llamado Office 2019, solo paga una vez y recibe las aplicaciones de productividad, como Word, Excel, PowerPoint y Outlook, pero eso es todo. La licencia de Office 2019 se limita a la instalación de un solo dispositivo, mientras que Office 365 le permite instalar las aplicaciones en hasta cinco dispositivos.

Las actualizaciones de seguridad gratuitas para las versiones actuales de las aplicaciones se lanzan regularmente, pero no con tanta frecuencia como las actualizaciones para Office 365, que también pueden incluir nuevas funciones. En el caso de una versión de actualización importante, como de Office 2016 a Office 2019, hay un cargo adicional por el producto independiente. Una suscripción a Office 365 garantiza que siempre tenga la última versión del software.

Office 2019 está disponible en varias versiones dirigidas a diferentes audiencias, con diferentes precios. Las versiones básicas, como Office Home & Student 2019, incluyen algunas de las aplicaciones, mientras que Office Professional 2019 incluye el conjunto completo. En este punto de la vida del producto Office, Microsoft apunta a Office 2019 en empresas que "no están listas para la nube" y que compran licencias por volumen para toda la organización. Debido a que Office 2019 está bloqueado por funciones, las aplicaciones no cambian, algo que los licenciatarios corporativos podrían preferir, para evitar interrumpir la productividad de sus usuarios con nuevas versiones de funciones.

Office 365 está disponible en varios planes diferentes que brindan otros servicios además de las aplicaciones, como correo electrónico en línea basado en Exchange y almacenamiento adicional de OneDrive. La versión incluida en Microsoft 365, llamado Office 365 ProPlus, está integrado con todos los servicios en la nube descritos anteriormente en este capítulo, incluidos Exchange Online, SharePoint Online, OneDrive para empresas y Teams. La integración de las aplicaciones de Office con estos servicios proporciona a los usuarios funciones avanzadas de inteligencia y colaboración que no están disponibles con Office 2019.

## Intercambiar

Todos los problemas descritos anteriormente en esta sección se aplican a una comparación de Exchange Online con la versión local de Exchange. Una implementación de Exchange Server puede ser un asunto complejo y costoso que requiere múltiples servidores y una configuración extensa, mientras que los administradores pueden tener Exchange Online en funcionamiento en menos de un día.

Exchange Online proporciona a cada usuario 50 o 100 GB de almacenamiento. En una instalación de intercambio local, el tamaño de los buzones de los usuarios está regulado por los administradores, que a menudo no quieren gastar tanto espacio de almacenamiento, que muchos usuarios podrían nunca necesitar.

Además, a diferencia de Exchange Server, Exchange Online puede

crear grupos de Office 365, que permiten a los usuarios trabajar juntos con recursos compartidos. Este puede ser un recurso valioso para los administradores. Por ejemplo, un equipo de soporte técnico puede agregar sus miembros a un grupo de Office 365. Luego, los administradores otorgan al grupo los permisos necesarios para acceder a un buzón de Exchange compartido, un sitio de grupo de SharePoint y otros recursos. Cuando los miembros entran o salen del grupo, los permisos para acceder a esos recursos se otorgan o revocan automáticamente.

En Exchange Server, de manera predeterminada, los buzones de correo de los usuarios existen en un servidor y, por lo tanto, son vulnerables a fallas de hardware, fallas del sistema y otros desastres que pueden hacer que no estén disponibles temporalmente o incluso provocar la pérdida de datos. Por esta razón, una implementación de intercambio empresarial a menudo requiere servidores adicionales para mantener buzones duplicados, una estrategia de respaldo confiable y, en algunos casos, centros de datos duplicados, todo lo cual se suma al costo de la instalación. Exchange Online, de forma predeterminada, replica las bases de datos de buzones en servidores y centros de datos, asegurando la disponibilidad continua del servicio. Este también es un problema que algunos administradores de Exchange preferirían abordar por sí mismos, en lugar de dejarlo en manos de un proveedor de servicios,

*Nota:*

## Servicio híbrido

### Implementaciones

Otra posible solución a los problemas de disponibilidad inherentes a las implementaciones locales de Exchange, SharePoint y Active Directory es que una organización cree una implementación de servicios híbridos, utilizando servidores locales y servicios en la nube juntos. Por lo tanto, el servicio en la nube puede funcionar como un mecanismo de disponibilidad que podría ser más económico que la creación de servidores locales redundantes o centros de datos. Cuando replica buzones o sitios o cuentas de AD en la nube, pueden aprovechar los mecanismos de seguridad que ofrece Microsoft. Una implementación híbrida también puede funcionar como un mecanismo de migración para organizaciones que desean pasar gradualmente de servicios locales a servicios basados en la nube.

## SharePoint

Al igual que con Exchange, SharePoint está disponible como un producto de servidor local y como el servicio de SharePoint Online basado en la nube. Las principales ventajas de la versión en la nube son las mismas que las de los otros servicios: implementación simplificada, actualización automática, redundancia de datos, administración basada en web, etc.

Microsoft presenta sus productos basados en la nube como la próxima ola en informática empresarial, y SharePoint Online es ahora el buque insignia del venerable SharePoint

producto. Nuevas características, como la experiencia moderna en diseño de sitios, aparecen primero en SharePoint Online. Sin embargo, en el caso de SharePoint, esto no significa que SharePoint Server se quede atrás.

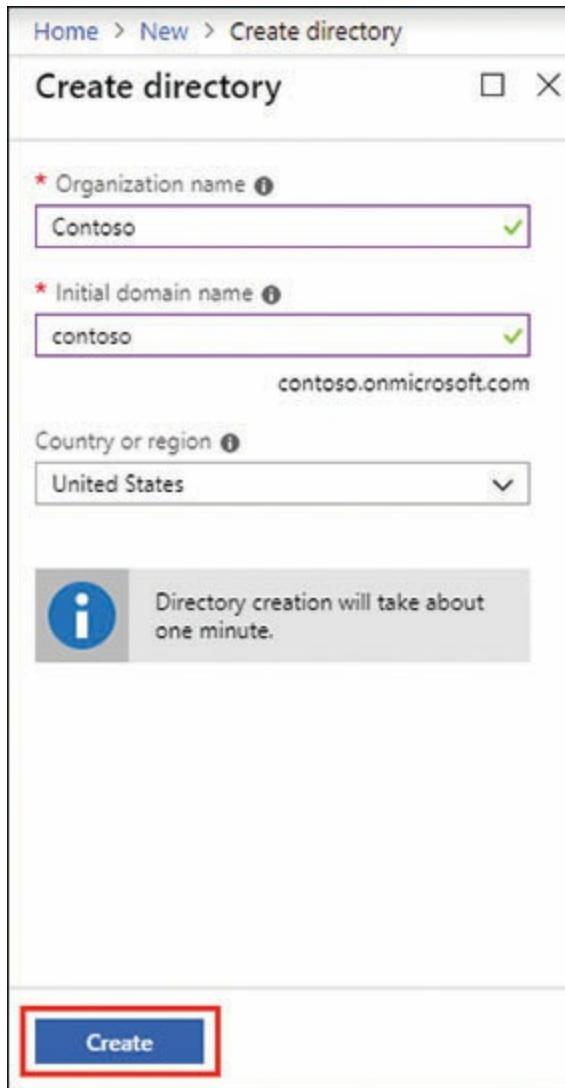
SharePoint Server 2019 incluye características que le permiten trabajar junto con los servicios en la nube de Microsoft 365. Por ejemplo, los administradores pueden redirigir el enlace de MySites en SharePoint Server a OneDrive para la Empresa, de modo que los usuarios serán dirigidos al almacenamiento en la nube, en lugar de al servidor local. También hay una capacidad de búsqueda en la nube híbrida que hace que una búsqueda de Office 365 incorpore el índice de un servidor local en la búsqueda en la nube estándar.

## Directorio Activo

A partir de la versión de Windows 2000 Server, los Servicios de dominio de Active Directory (AD DS) funcionaron como una solución de administración de identidad para recursos empresariales. Después de crear un controlador de dominio AD DS desde un servidor de Windows, los administradores crean una jerarquía de bosques y dominios y los completan con objetos lógicos que representan a los usuarios, computadoras, aplicaciones y otros recursos. Con esos objetos, AD DS funciona como intermediario entre los usuarios y los recursos de la red, proporcionando servicios de autenticación y autorización cuando los usuarios intentan acceder a ellos. Azure Active Directory (Azure AD o AAD) es un

El mecanismo de identidad como servicio (IDaaS) que realiza las mismas funciones básicas de autenticación y autorización para los servicios en la nube de Microsoft 365, pero lo hace de una manera diferente.

No hay bosques ni dominios en Azure AD. Después de que una organización se suscribe a Microsoft 365 (o cualquiera de los servicios en la nube individuales de Microsoft), un administrador crea un inquilino, utilizando la página **Crear directorio, como se muestra en Figura 2-9**. En Azure AD, un *inquilino* **Es una construcción lógica que representa a toda la organización**. Los administradores del inquilino pueden usar Azure Portal para crear cuentas de usuario y administrar sus propiedades, como permisos y contraseñas. Las cuentas proporcionan a los usuarios la capacidad de inicio de sesión único para todos los servicios de Microsoft.



**FIGURA 2-9** Crear un inquilino

AD DS utiliza protocolos como Kerberos y NT LAN Manager (NTLM) para la comunicación entre los controladores de dominio y las otras computadoras involucradas en una autenticación o autorización. Esto es apropiado para sus funciones porque AD DS funciona solo dentro de las instalaciones de la organización; no está diseñado para trabajar con

usuarios fuera de la empresa o administran servicios basados en la nube como los de Microsoft 365.

Azure AD, obviamente, está diseñado para administrar servicios en la nube y puede trabajar con usuarios ubicados en cualquier lugar, empleando diferentes protocolos de seguridad, como el Lenguaje de marcado de aserción de seguridad (SAML) y la Autorización abierta (OAuth). Debido a que son tan diferentes, Azure AD y AD DS no son funcionalmente

intercambiables, al igual que las versiones locales y basadas en la nube de servicios como Exchange y SharePoint.

Por lo tanto, para cualquier organización que tenga una implementación AD DS existente en las instalaciones y esté considerando implementar Microsoft 365, los administradores deberán trabajar con AD DS y Azure AD. Afortunadamente, esto no significa que será necesario crear cuentas de usuario duplicadas en cada uno de los servicios de directorio. Microsoft proporciona una herramienta llamada *Azure AD Connect* que crea un enlace entre los dos y proporciona a cada usuario un solo *identidad híbrida* que abarca tanto los servicios locales como los basados en la nube. Esto proporciona al usuario la capacidad de inicio de sesión único para todas las aplicaciones y servicios.

## HABILIDAD 2.3: ENTENDER EL CONCEPTO DE GESTIÓN MODERNA

---

*Gestión moderna* es un término acuñado por Microsoft, pero que se está aceptando rápidamente en toda la industria de TI. Descrito por Microsoft usando el lema "móvil primero; primero en la nube ", pretende ser un reemplazo o, al menos, una evolución de las prácticas de administración tradicionales que los administradores de TI empresariales han estado utilizando durante años.

El enfoque tradicional para la administración de dispositivos de TI consiste en un paradigma en el que todos los dispositivos son propiedad, implementados y administrados por el departamento de TI de la empresa. Esta gestión generalmente incluye los siguientes elementos:

- **Despliegue** Los administradores de TI crean y mantienen archivos de imagen del sistema y los implementan en computadoras nuevas utilizando una herramienta de administración, como System Center Configuration Manager (SCCM). Los administradores deben crear y almacenar imágenes y controladores separados para cada modelo de computadora comprado y actualizarlos cada vez que cambie la configuración del software.
- **Actualizaciones** Los administradores administran las actualizaciones del sistema operativo y de las aplicaciones, generalmente mediante un proceso elaborado de descarga, evaluación e implementación, utilizando una herramienta como Windows Server Update Services (WSUS).
- **Identidad** Active Directory es una base de datos de identidades y otros recursos de red que proporcionan servicios de autenticación y autorización para usuarios internos, servicios y aplicaciones.
- **Configuración** Los administradores usan la directiva de grupo para implementar la configuración mientras se conectan e inician sesión en la red interna.

Este paradigma de gestión tradicional ha funcionado

durante mucho tiempo, y muchos profesionales de TI son extremadamente reacios a abandonarlo, especialmente cuando la adopción de un nuevo concepto de gestión moderno requiere que aprendan a usar nuevas herramientas y tecnologías.

Sin embargo, el problema es que la administración moderna no es solo una solución para algo que no está roto. La idea de que todos los usuarios trabajen en dispositivos administrados y de propiedad de la empresa ubicados en el sitio de una empresa se está convirtiendo rápidamente en una reliquia del pasado. Un gran número de usuarios trabajan fuera de la oficina utilizando sus propios dispositivos, como computadoras portátiles, tabletas y teléfonos inteligentes, que no se pueden implementar, actualizar y configurar fácilmente según las especificaciones de un departamento de TI utilizando herramientas tradicionales.

La otra motivación para modernizar la administración de TI es la mayor ubicuidad de las aplicaciones basadas en la nube en la empresa. A medida que los fabricantes de software cambian su énfasis de marketing a la nube, cada vez es más difícil para los administradores de TI proporcionar los servicios que sus usuarios necesitan con aplicaciones y servicios tradicionales locales.

La administración moderna está diseñada para reemplazar las herramientas tradicionales por otras nuevas que pueden funcionar con recursos basados en la nube, administrando los propios dispositivos de los usuarios y simplificando los procesos de implementación, actualización y administración. El objetivo es reemplazar los procesos tradicionales de gestión reactiva con modernos

procesos proactivos Microsoft 365 incluye herramientas que hacen todas estas cosas, como las siguientes:

- **Despliegue** Windows AutoPilot es un servicio basado en la nube que elimina la necesidad de imágenes de sistema separadas y SCCM y simplifica el proceso de implementación de nuevas computadoras al automatizar el proceso de instalación, activación y configuración de Windows 10.
- **Actualizaciones** El programa de actualización de Windows como servicio proporciona a las estaciones de trabajo de Windows 10 actualizaciones de características y calidad programadas regularmente que se aplican automáticamente. Microsoft también ha implementado tecnologías para reducir el tamaño de las descargas de actualizaciones, mitigando la carga sobre las redes y las conexiones a Internet.
- **Identidad** Azure Active Directory mueve las identidades de los usuarios de la red local a la nube, lo que permite a los administradores administrarlas desde cualquier lugar y brinda a los usuarios la capacidad de inicio de sesión único para todos los servicios y aplicaciones basados en la nube.
- **Configuración** Microsoft Intune expande el perímetro de administración de una empresa para incluir dispositivos que no son de Windows y dispositivos accesibles a través de la nube. Sin embargo, Intune también puede reemplazar la Política de grupo para configurar computadoras con Windows 10 porque también se ha mejorado con cientos de API de administración de dispositivos móviles (MDM) que permiten a Intune y herramientas similares controlarlas a través de la nube.

## Transición a la gestión moderna

Las nuevas organizaciones o divisiones que eligen Microsoft 365 como su solución de TI inicial pueden, obviamente, adoptar las herramientas y técnicas de administración modernas de Microsoft desde cero. Microsoft llama a esto la opción "nube primero". Administradores, incluso si tienen un previo

historia con herramientas de gestión tradicionales, puede adaptarse a las nuevas sin ningún conflicto entre los dos modelos. Sin embargo, cuando una organización tiene una infraestructura existente basada en el modelo tradicional, debe decidir si cambia a una administración moderna y cómo debe hacerlo.

La transición al modelo de gestión moderno requiere nuevas herramientas y también nuevas habilidades para los administradores. Microsoft ha diseñado tres enfoques para una transición de la administración tradicional a la moderna, de la siguiente manera:

- **Gran interruptor** En la transición del gran cambio, una organización abandona todas las herramientas y modalidades de gestión tradicionales y comienza a utilizar exclusivamente herramientas de gestión modernas. Si bien esta podría ser una opción factible para una organización relativamente pequeña, las grandes empresas probablemente encontrarán una transición repentina poco práctica.
- **Grupo por grupo** En una transición de grupo por grupo, una organización clasifica a sus usuarios por departamento, ubicación o carga de trabajo y convierte un grupo de usuarios a la vez en el entorno de administración moderno. En muchos casos, el proceso de transición estará determinado por las aplicaciones que los usuarios requieran y si se pueden administrar fácilmente desde la nube.
- **Cogestión** El modelo de gestión conjunta exige que los administradores mantengan los paradigmas de gestión tradicionales y modernos durante un período prolongado. Esto hace posible que la organización haga una transición gradual de las aplicaciones y procedimientos tradicionales a aquellos que respaldan la administración moderna.

La gestión conjunta se ha convertido en una solución ampliamente aceptada para las empresas que son reacias a renunciar

su modelo de gestión tradicional o que tienen aplicaciones y servicios que no son manejables utilizando las herramientas modernas. Desde el punto de vista de Microsoft, el objetivo de la gestión conjunta es formar un puente entre el modelo de gestión tradicional y el moderno. Los administradores pueden continuar utilizando elementos de su infraestructura local tradicional, como los Servicios de dominio de Active Directory y System Center Configuration Manager, y migrar gradualmente a herramientas modernas, como Azure Active Directory y Microsoft Intune.

Los pasos involucrados en una transición de cogestión (no necesariamente en orden) son los siguientes:

- Comience a usar el modelo de Windows como servicio en Windows 10 y Office 365 ProPlus.
- Pase de una solución de actualización de Windows local, como los Servicios de actualización de Windows Server, a la Actualización de Windows basada en la nube para empresas.
- Transición de la creación, mantenimiento e implementación de imágenes del sistema para estaciones de trabajo de Windows al uso de Windows AutoPilot para implementaciones basadas en la nube y sin tocar.
- Deje de usar la directiva de grupo para configurar los ajustes de la estación de trabajo a favor de la herramienta Microsoft Intune incluida con Enterprise Mobility + Security.

Aunque es posible realizarlos por separado, todas estas tareas se incorporan a una implementación de Microsoft 365.

## Windows como servicio

Con el lanzamiento de Windows 10, Microsoft cambió la forma en que generan y lanzan las actualizaciones del sistema operativo. Copiando el nuevo sistema Windows as a Service (WaaS), está diseñado para reducir la carga de los usuarios y administradores.

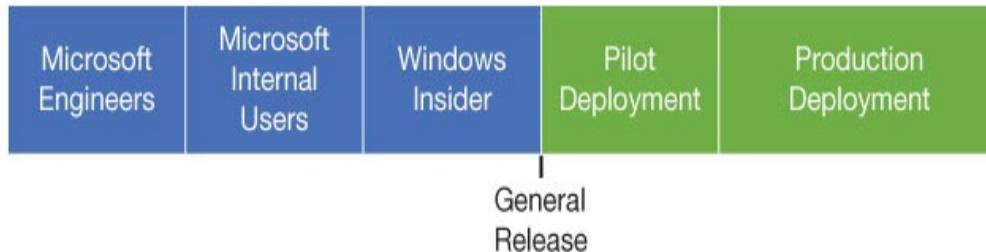
En el pasado, Microsoft lanzó actualizaciones de versiones principales de Windows cada tres o cinco años, paquetes de servicio grandes entre esas actualizaciones y pequeñas actualizaciones cada mes. Las actualizaciones de la versión fueron una tarea importante tanto para los administradores como para los usuarios. Los administradores tuvieron que reinstalar el sistema operativo en todas sus estaciones de trabajo, y los usuarios se enfrentaron a una interfaz diferente y nuevas características.

El modelo de Windows como servicio elimina las actualizaciones de versión. En cambio, hay actualizaciones de funciones dos veces al año y actualizaciones de calidad al menos cada mes. Las actualizaciones de calidad abordan problemas de seguridad y confiabilidad, mientras que las actualizaciones de características agregan nuevas funcionalidades. Debido a que las actualizaciones de características son más frecuentes que las actualizaciones de versiones principales anteriores, distribuyen el proceso de implementación de actualizaciones para los administradores y no representan un cambio tan profundo de interfaz y características para los usuarios.

Microsoft ofrece tres canales de servicio para Windows 10:

- **Canal semianual** De manera predeterminada, las instalaciones de Windows 10 usan el canal semianual.
- **Canal Windows Insider** Para los usuarios u organizaciones que desean un acceso temprano a las actualizaciones para las pruebas y la capacidad de proporcionar comentarios, existe el canal Windows Insider.
- **Canal de servicio a largo plazo** Para los dispositivos con funciones especializadas en las que la continuidad es esencial, como equipos médicos, sistemas de punto de venta y quioscos, existe el Canal de servicio a largo plazo, que recibe actualizaciones de funciones solo cada dos o tres años, que luego son respaldadas por Microsoft por diez años.

El ciclo de actualización de características semestral comienza con una fase de desarrollo en la que la actualización la ejecutan primero los ingenieros de Microsoft y luego un grupo más grande de usuarios internos de Microsoft durante seis meses, un proceso que Microsoft llama "alimentación de perros". Luego, Microsoft lanza la actualización de características a los miembros del programa Windows Insider, para pruebas y comentarios. Finalmente, la actualización pasa a la versión general, que en una gran empresa generalmente consiste en una implementación piloto o de prueba, seguida de una implementación de producción general en todas las estaciones de trabajo, como se muestra en Figura 2-10. . Para la mayoría de las ediciones de Windows 10, los servicios de Microsoft actualizan cada característica durante dieciocho meses después de su lanzamiento general. Para las ediciones Windows 10 Enterprise y Education, el período de servicio es de 30 meses.



**FIGURA 2-10** Fases de una versión de actualización de características de Windows 10

Las actualizaciones de calidad mensuales en el modelo anterior tomaban la forma de muchos parches individuales, que los administradores empresariales tenían que evaluar e implementar individualmente. Muchos administradores optaron por implementar solo soluciones de seguridad esenciales, dejando sus estaciones de trabajo en un estado fragmentado. Solo los paquetes de servicio infrecuentes incorporaron todos los parches anteriores y actualizaron completamente las estaciones de trabajo. Las estaciones de trabajo fragmentadas hicieron difícil o imposible para Microsoft predecir con precisión el resultado de futuras actualizaciones.

Las actualizaciones de calidad de WaaS toman la forma de lanzamientos mensuales acumulativos que incluyen todas las últimas correcciones de seguridad y confiabilidad. Esto deja las estaciones de trabajo en un estado completamente parcheado cada mes. Por lo tanto, Microsoft puede probar actualizaciones posteriores en una plataforma consistente, en lugar de tener que preocuparse si se han aplicado todos los parches anteriores.

Una de las quejas hechas por muchos administradores

El responsable de la implementación de la actualización es el tamaño de las actualizaciones de características semestrales. Una descarga de 3–4 GB para cada estación de trabajo en una gran flota empresarial de cientos o miles de computadoras puede abrumar fácilmente incluso una conexión a Internet sólida. Además, debido a que las actualizaciones de calidad son acumulativas, crecen cada mes después de la actualización de funciones más reciente, llegando a 1 GB o un poco más.

Microsoft ha abordado este problema con una función llamada Actualizaciones rápidas, que genera descargas diferenciales para estaciones de trabajo basadas en las actualizaciones que ya han instalado. Una descarga diferencial contiene solo los archivos que necesita la estación de trabajo. Express Update puede reducir una actualización de calidad a 150–200 MB en una computadora que ya está actualizada. También es posible reducir la carga de las conexiones a Internet mediante el uso de funciones punto a punto, como BranchCache y Delivery Optimization.

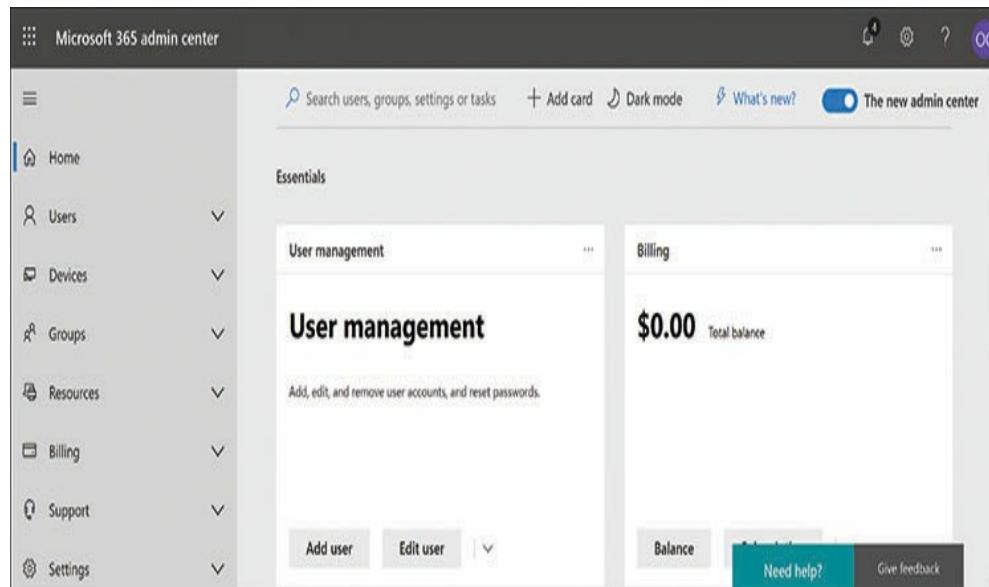
## Usando los portales de Microsoft 365

Debido a que Microsoft 365 consiste principalmente en servicios basados en la nube, los administradores usan controles basados en la web para administrarlos y los usuarios pueden usar portales basados en la web para acceder a ellos. Los servicios individuales que se incluyen con Microsoft 365, como Exchange Online y SharePoint Online, también están disponibles por separado.

productos, por lo que tienen sus propios portales administrativos, llamados Centros de administración. Sin embargo, el Centro de administración de Microsoft 365 es el portal administrativo principal del producto y también proporciona acceso a todos los portales individuales.

## Usar el Centro de administración de Microsoft 365

Cuando inicia sesión en el Centro de administración de Microsoft 365 en [admin.microsoft.com](https://admin.microsoft.com), ves la pantalla de inicio que se muestra en Figura 2-11, con un menú de navegación en el panel izquierdo y una serie de tarjetas que contienen controles esenciales a la derecha. Los administradores pueden colocar sus controles más utilizados en la página de inicio arrastrando elementos del menú de navegación al panel derecho para agregar más tarjetas.



**FIGURA 2-11** El Centro de administración de Microsoft 365 Inicio

pantalla

El panel de navegación contiene menús para categorías de control, con menús desplegables para tipos de control específicos. Las categorías son las siguientes:

- **Los usuarios** Permite a los administradores crear, administrar y eliminar cuentas de usuario. Al asignar licencias a las cuentas, los usuarios tendrán acceso a Office 365 u otras aplicaciones y servicios. La asignación de roles administrativos a los usuarios les otorga privilegios para acceder a ciertos controles adicionales.
- **Dispositivos** Permite a los administradores agregar nuevos dispositivos, individualmente o en masa, como teléfonos inteligentes y tabletas, crear políticas para proteger los dispositivos y administrar dispositivos individuales al restablecerlos, eliminar datos corporativos o eliminarlos por completo.
- **Grupos** Permite a los administradores crear varios tipos de grupos, incluidos Office 365, seguridad, seguridad habilitada para correo y grupos de listas de distribución, asignarles propietarios y configurar configuraciones de privacidad. También pueden crear buzones compartidos para el acceso de todos los miembros de un grupo específico.
- **Recursos** Permite a los administradores crear y configurar salas y equipos para asignarlos a reuniones y crear sitios y colecciones de SharePoint. El Centro de administración en línea de SharePoint proporciona control total sobre SharePoint, pero esta interfaz puede controlar el uso compartido del sitio y eliminar usuarios externos.
- **Facturación** Permite a los administradores comprar aplicaciones y servicios adicionales de Microsoft, administrar suscripciones de productos, monitorear licencias de productos disponibles y administrar facturas y pagos.
- **Apoyo** Permite a los administradores encontrar soluciones a problemas comunes de Microsoft 365 y crear y ver solicitudes de servicio de técnicos de Microsoft.
- **Configuraciones** Permite a los administradores configurar ajustes de servicio y complementos para toda la empresa, configurar ajustes de seguridad y monitorear

relaciones de pareja

- **Preparar** Permite a los administradores monitorear sus productos de Microsoft y administrar las licencias para esos productos, comprar o agregar dominios de Internet y migrar datos de proveedores de correo electrónico externos a cuentas de Microsoft 365.
- **Informes** Permite a los administradores generar varios informes, como actividad de correo electrónico, usuarios activos y uso del sitio de SharePoint, en intervalos de 7 a 180 días. Informes como estos pueden indicar quién está utilizando los servicios de Microsoft 365 en gran medida, quién está cerca de alcanzar las cuotas de almacenamiento y quién podría no necesitar una licencia.
- **Salud** Permite a los administradores monitorear el estado operativo de los diversos servicios de Microsoft 365, leer cualquier incidente y los informes de aviso que se hayan generado, y recibir mensajes sobre la disponibilidad de actualizaciones del producto y otros temas.
- **Centros Administrativos** Permite a los administradores abrir nuevas ventanas que contienen los centros de administración para los otros servicios proporcionados en Microsoft 365, incluidos Seguridad, Cumplimiento, Azure Active Directory, Exchange, SharePoint y Teams.

#### *Nota:*

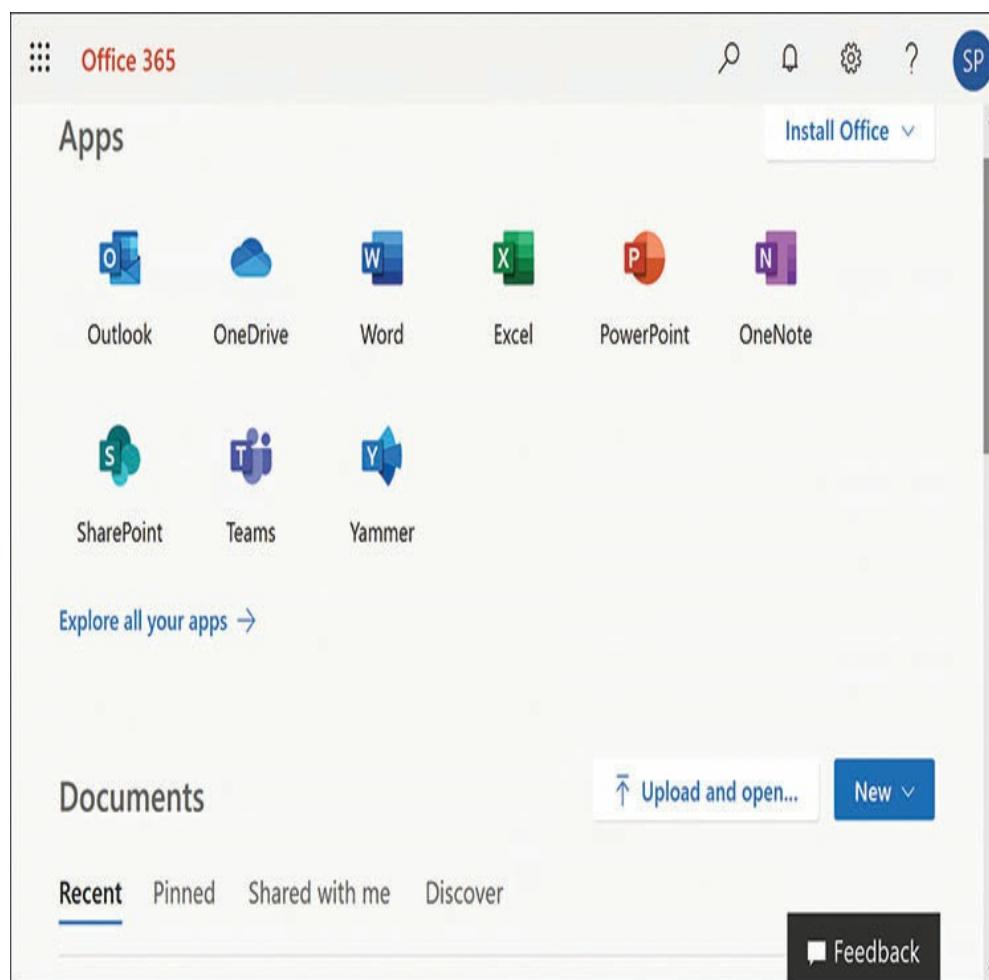
## Microsoft 365

### Centro de administración

Debido a que los centros de administración para los servicios de Microsoft 365 están basados en la web, los desarrolladores de productos pueden modificarlos fácilmente y agregar características a medida que estén disponibles sin interrumpir a sus usuarios. A principios de 2019, Microsoft creó un nuevo diseño para el Centro de administración de Microsoft 365 con la configuración predeterminada y agregó un control en la esquina superior derecha que permite a los usuarios cambiar entre el diseño anterior y el nuevo a voluntad. Las cifras de los controles del centro de administración en este libro están tomadas del nuevo diseño tal como existe al momento de la escritura. Los cambios de diseño y características podrían haberse introducido desde el momento de la publicación.

## Usar el portal de Office 365

Una vez que un usuario ha recibido una cuenta de Microsoft 365, él o ella tiene acceso a Office 365 ProPlus y puede iniciar sesión en el portal del usuario en <http://office.com>. Despues de iniciar sesión con la dirección de correo electrónico creada por el administrador como parte de la cuenta de usuario, aparece el portal de Office 365, como se muestra en Figura 2-12.



**FIGURA 2-12** El portal de usuarios de Office 365

Los iconos de la aplicación en la página principal del portal proporcionan al usuario acceso a las versiones web de las aplicaciones de productividad de Office: Outlook, OneDrive, Word, Excel y PowerPoint. Debajo de los íconos hay un área de Documentos que proporciona al usuario acceso a los archivos de documentos recientemente utilizados, anclados y compartidos almacenados en la nube OneDrive del usuario.

Junto con las aplicaciones, los íconos adicionales brindan acceso a los servicios basados en la nube incluidos con una licencia de Microsoft 365, incluidos OneDrive, OneNote, SharePoint, Teams y Yammer.

El ícono de SharePoint, de manera predeterminada, abre una nueva ventana que contiene el sitio principal del centro del dominio. Agregar usuarios a grupos puede hacer que el ícono proporcione acceso a un sitio de grupo. Al hacer clic en el **Equipos** El ícono abre por primera vez una página que invita al usuario a descargar la aplicación Teams o usar el cliente Teams basado en la web. Después de eso, el cliente web aparece de forma predeterminada. los

**Una nota** el ícono abre el cliente de toma de notas basado en la web del usuario, y el **Quejarse** El ícono abre el sitio web de redes sociales empresariales.

Si al usuario se le han otorgado privilegios de administrador global, un adicional **Administración** El ícono aparece en el portal, que proporciona al usuario acceso al Centro de administración de Microsoft 365.

De forma predeterminada, Microsoft 365 permite al usuario instalar

las aplicaciones de productividad de Office 365 en hasta cinco sistemas. Haciendo clic **Instalar Office** y seleccionando **Aplicaciones de Office 365** abre el **Mis instalaciones** página, que muestra la interfaz que se muestra en Figura 2-13 .



**FIGURA 2-13** La interfaz Mis instalaciones en el portal de usuario de Office 365

La instalación incluye todas las aplicaciones de Office locales, incluidas Word, Excel, PowerPoint, Access, Publisher, Outlook, Skype for Business y OneDrive for Business. Esta es la única forma para que un usuario de Office 365 ejecute las aplicaciones Access y Publisher porque no hay versiones basadas en la web de estas.

## Comprender el modelo de implementación y lanzamiento de Microsoft

Como se señaló anteriormente, Microsoft 365 consta de tres productos:

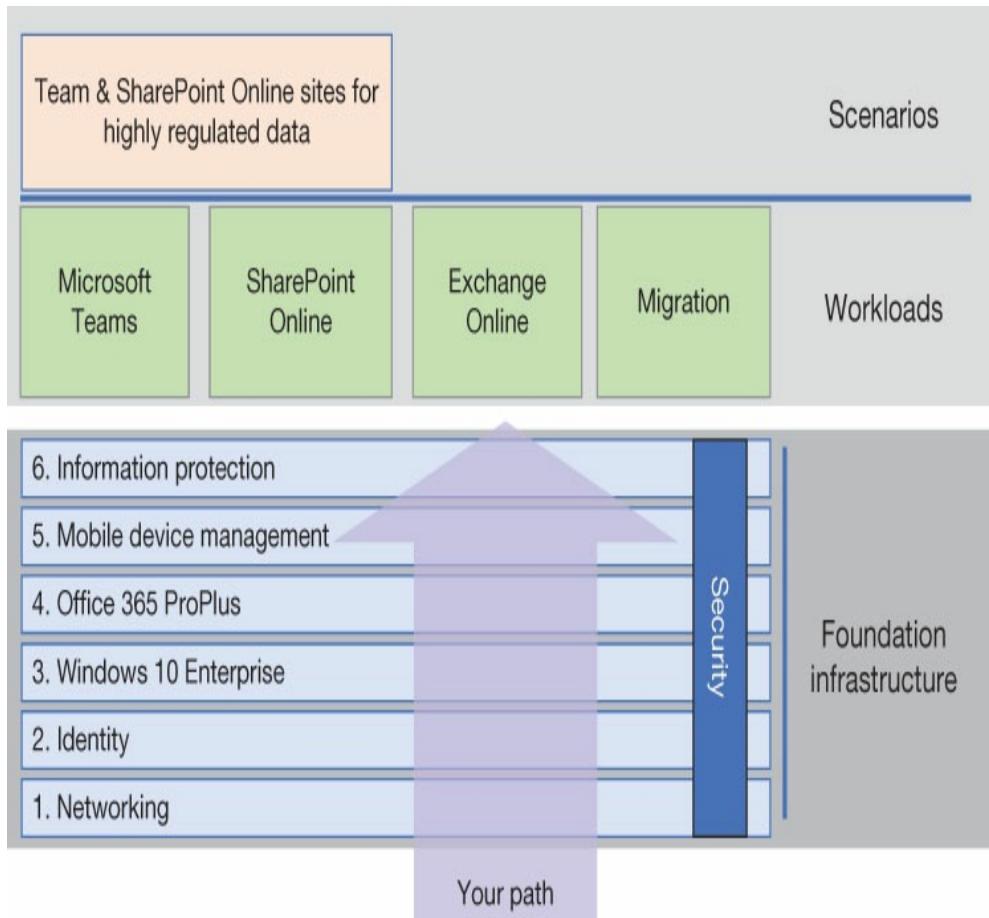
Windows 10 Enterprise, Office 365 ProPlus y Enterprise Mobility + Security.

Sin embargo, el proceso de implementación de Microsoft 365 no es solo una cuestión de obtener licencias para estos tres productos e instalarlos. Las formas en que los componentes de Microsoft 365 trabajan juntos para proporcionar administración inteligente, seguridad y colaboración requieren que la implementación se realice como un proceso integrado.

La complejidad de una implementación empresarial de Microsoft 365 depende del tamaño de la empresa existente y de las aplicaciones que se ejecutan en ella. Microsoft ha definido tres estrategias de implementación de Microsoft 365:

- **FastTrack para Microsoft 365** FastTrack es un beneficio incluido como parte de una suscripción de Microsoft 365 Enterprise que proporciona soporte continuo del personal de Microsoft, incluido un administrador de FastTrack, un ingeniero y un ingeniero de migración. Estos especialistas dividen la implementación de Microsoft 365 del suscriptor en tres etapas, llamadas Envision, Onboard y Drive Value, lo que les permite planificar e implementar Microsoft 365 en la infraestructura empresarial existente, y luego ayudar a las personas de la organización a adaptar sus roles al entorno de Microsoft 365.
  
- **Servicios de terceros** Los socios de Microsoft y los servicios de consultoría pueden proporcionar ayuda con una implementación de Microsoft 365 en muchos niveles, desde el control completo de la operación hasta el soporte ocasional.
  
- **Autodespliegue** La guía de implementación de Microsoft 365 Enterprise define un *infraestructura de cimientos* para la creación de una instalación viable de Microsoft 365, que incluye Windows 10 Enterprise y Office 365 ProPlus, después de lo cual los administradores pueden crear cargas de trabajo y escenarios, que incluyen Exchange Online, SharePoint

En línea y equipos de Microsoft, como se muestra en Figura 2-14. .



**FIGURA 2-14** El modelo de implementación de Microsoft 365

Enterprise

La guía de implementación de Microsoft 365 Enterprise rompe la infraestructura básica, a veces denominada *despliegue central*—En seis fases, como se describe en las siguientes secciones. Cada fase se divide en pasos y concluye con los criterios de salida que deben cumplirse antes de que la implementación de la infraestructura básica se pueda considerar completa.

Para una implementación en una organización relativamente pequeña o nueva que recién comienza a utilizar los productos basados en la nube de Microsoft, seguir las fases de implementación de la infraestructura básica para crear una estructura confiable para las cargas de trabajo y los escenarios que se implementarán más adelante. Para una empresa existente que ya está utilizando algunos de los componentes de Microsoft 365, es posible que algunos de los criterios de salida ya se hayan cumplido, y las seis fases no tienen que seguirse en una secuencia ininterrumpida. Los administradores pueden abordar las fases en cualquier orden que consideren práctico, si finalmente cumplen con los criterios de salida para cada fase.

#### ***Necesita más revisión***

Para obtener una cobertura más detallada de los pasos en cada una de las fases de implementación de la infraestructura básica, así como los procedimientos para implementar las cargas de trabajo y los escenarios de Microsoft 365, consulte la documentación de Implementación de Microsoft 365 Enterprise en <https://docs.microsoft.com/en-us/microsoft-365/enterprise/deploy-microsoft-365-enterprise?view=o365-worldwide>.

## **Fase 1: Redes**

La fase de red tiene como objetivo garantizar que todos los clientes de Microsoft 365 tengan suficiente conectividad a Internet para acceder a los recursos en la nube que requieren de forma regular. Esto no es solo una cuestión de

ancho de banda, sin embargo. Microsoft Global Network proporciona puntos finales a sus servicios en la nube en todo el mundo, y para que los clientes de Microsoft 365 funcionen de manera eficiente, deben tener acceso al punto final más cercano posible.

Muchas redes empresariales se diseñaron y construyeron en un momento en que la proximidad de la conexión a Internet no era una prioridad. Era común que el tráfico de Internet en sitios remotos se enrutara a través de una red troncal a una ubicación central que proporcionaba el acceso real a Internet. Esto puede resultar en una cantidad significativa de latencia de red que puede tener un efecto negativo en el rendimiento de Microsoft 365.

Los servidores DNS de Microsoft dirigen el tráfico del cliente al punto final más cercano en función de su solicitud de conexión inicial. Por lo tanto, los clientes también deben utilizar un servidor DNS geográficamente local para su tráfico saliente de Internet.

Para una empresa que tiene una infraestructura de acceso a Internet centralizada, la organización debe tomar los pasos necesarios para redirigir el tráfico de Internet para que cada cliente sea dirigido al punto final de Microsoft que está geográficamente más cercano a su ubicación. En una empresa grande con muchos sitios remotos, esto puede ser una tarea sustancial, que podría desempeñar un papel en la decisión de adoptar Microsoft 365 en primer lugar.

Microsoft también recomienda que las redes empresariales eviten el uso de mecanismos de protección, como servidores proxy e inspección de paquetes, para el tráfico de Microsoft 365. Los nombres DNS y las direcciones IP utilizadas por los servicios en la nube de Microsoft 365 son bien conocidos, y los servicios ya están protegidos por los propios mecanismos de Microsoft. Duplicar esta protección en el extremo empresarial también puede tener un efecto negativo en el rendimiento de Microsoft 365. Para evitar estos mecanismos de protección local, es necesario que los navegadores, los firewalls y otros componentes identifiquen el tráfico de Microsoft 365 y lo procesen de manera diferente a otros tipos de tráfico de Internet.

## Fase 2: identidad

En la fase de identidad, los administradores crean las cuentas de Azure AD que serán necesarias para que los usuarios accedan a los servicios y aplicaciones en la nube de Microsoft. Estas cuentas pueden ser para los usuarios internos de la organización o para socios, proveedores y consultores externos a la organización. Para organizaciones sin una infraestructura local o para usuarios que solo requieren servicios en la nube, los administradores pueden crear cuentas directamente en Azure AD. Si la organización tiene una infraestructura interna basada en los Servicios de dominio de Active Directory, los administradores pueden sincronizar las cuentas existentes de AD DS con Azure AD.

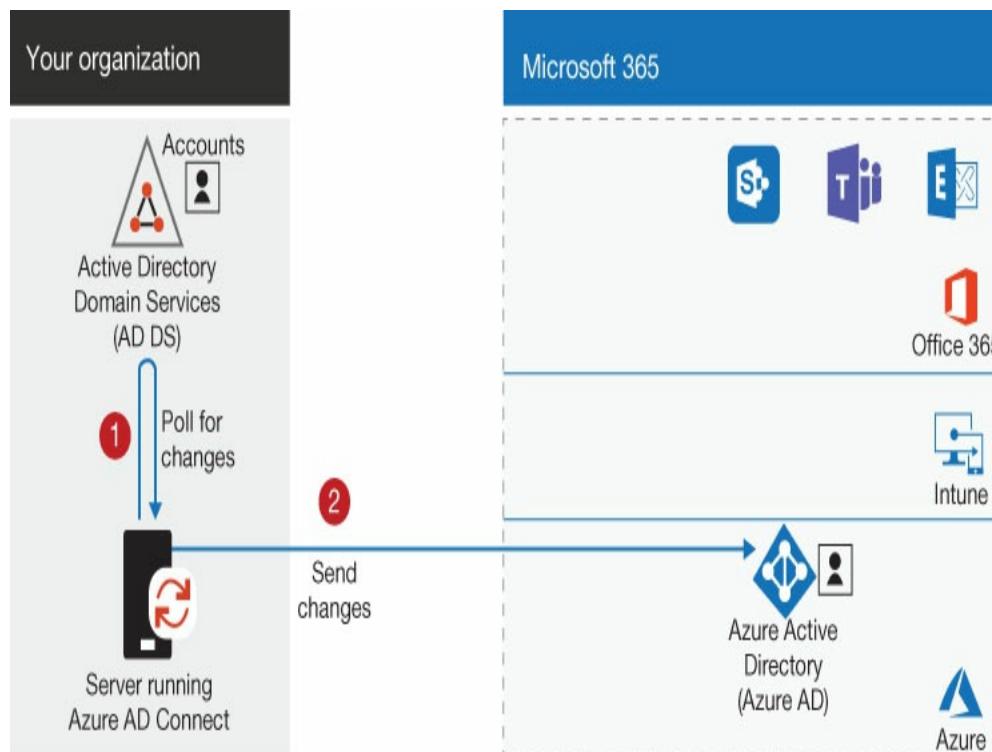
Los administradores también deben planificar cómo van

para agrupar a los usuarios en la organización y cómo van a usar los grupos de Office 365 para la administración de la red. Por ejemplo, Microsoft 365 admite licencias basadas en grupos, en las cuales los miembros de un grupo obtienen automáticamente una licencia para Office 365 y / o Enterprise Mobility + Security. Al igual que con AD DS, también es posible asignar permisos a grupos, lo que permite a los miembros acceder a sitios de grupo de SharePoint y otros recursos. Azure AD también admite la pertenencia a un grupo dinámico, en el que las cuentas de usuario con propiedades específicas, como el nombre de un departamento o país, se agregan automáticamente a un grupo.

En esta fase, los administradores también configuran protección para cuentas administrativas. Cuentas de administrador global, las más privilegiadas en Microsoft 365, debe configurarse con las contraseñas más seguras que sean prácticas y que también utilicen multifactor autenticación (MFA). Además de la contraseña, MFA puede solicitar un atributo biométrico, como una huella digital o un código de verificación enviado a un teléfono inteligente. Otras cuentas de administrador, como las de servicios específicos, e incluso cuentas de usuario estándar, pueden requerir un nivel similar de protección MFA.

Cuando una organización tiene una infraestructura AD DS existente, los administradores pueden crear cuentas duplicadas en Azure AD, pero tendrían que realizar manualmente cualquier cambio futuro en ambos directorios. UNA

Una solución más simplificada está disponible en la creación de cuentas híbridas. *Cuentas híbridas* son cuentas de AD DS que están sincronizadas con cuentas de Azure AD, usando una herramienta llamada Azure AD Connect. Al ejecutarse en un servidor interno, Azure AD Connect sondea AD DS para detectar cambios en cuentas y grupos y los replica en Azure AD, como se muestra en Figura 2-15 .



**FIGURA 2-15** Mantenimiento de cuenta híbrida de Azure AD Connect

Cuando los administradores crean cuentas híbridas con Azure AD Connect, deben seleccionar el método de autenticación que usarán las identidades híbridas. La autenticación en la nube usa el hash de contraseña de Azure AD

sincronización o autenticación de paso de Azure AD. La otra alternativa, utilizada cuando se necesitan requisitos de inicio de sesión que Azure AD no admite, es la autenticación federada, que usa un servicio de autenticación separado, como los Servicios de federación de Active Directory (AD FS).

Los administradores también pueden configurar Azure AD para admitir *reescritura de contraseña*, una característica que permite a los usuarios híbridos en ubicaciones remotas y sin acceso a la red interna cambiar sus contraseñas en Azure AD, después de lo cual las contraseñas se replican automáticamente en AD DS. La reescritura de contraseñas es necesaria para admitir la función Azure AD Identity Protection que requiere que los usuarios cambien sus contraseñas cuando se detecta actividad sospechosa en la cuenta. Con la reescritura de contraseña habilitada, los administradores también pueden habilitar el restablecimiento de contraseña de autoservicio (SSPR), que permite a los usuarios restablecer sus contraseñas y desbloquear sus cuentas.

## Fase 3: Windows 10 Enterprise

El proceso de implementación de Windows 10 Enterprise puede variar según la condición actual de la red y las herramientas que los administradores están usando para administrar las estaciones de trabajo. Para una empresa que tiene estaciones de trabajo que ya ejecutan Windows 7 o Windows 8.1, es posible realizar una actualización in situ a Windows 10 Enterprise y automatizar el proceso usando el Sistema

Administrador de configuración del centro.

El procedimiento para una actualización in situ de SCCM a Windows

10 Enterprise es el siguiente:

**1. Verifique la preparación de la estación de trabajo para ejecutar Windows 10**

La herramienta de preparación en Windows Analytics, disponible a través del portal de Azure, recopila información sobre computadoras, aplicaciones y controladores y la analiza en busca de problemas de compatibilidad que podrían evitar una actualización exitosa del sistema operativo. Los administradores también deben verificar que las estaciones de trabajo estén ejecutando versiones de Windows 7 u 8.1 elegibles para la actualización a Windows 10 Enterprise y preparar el entorno SCCM creando un contenedor de administración del sistema.

**2. Agregue una imagen de Windows 10 a SCCM**

Biblioteca, cree un paquete de actualización del sistema operativo cargando una imagen de Windows 10 Enterprise.

**3. Cree una secuencia de tareas**

Cree una secuencia de tareas que funcionará como el script de actualización seleccionando **Actualice un sistema operativo desde el paquete de actualización** y agregando el archivo de imagen que cargó anteriormente. Luego, cree una colección de dispositivos para la secuencia de tareas, especificando las estaciones de trabajo que recibirán la actualización. Luego, cree una implementación que asocie la secuencia de tareas con la colección de dispositivos.

**4. Inicie la secuencia de tareas en las estaciones de trabajo.**

Ejecutar software Centrarse en cada estación de trabajo, seleccionar la secuencia de tareas creada anteriormente y seleccionar **Instalar en pc** para ejecutar la secuencia de tareas y realizar la actualización. Opcionalmente, la implementación puede incluir configuraciones que automatizan el proceso de actualización y programan que ocurra a una hora específica.

Para las nuevas estaciones de trabajo con Windows 10, los administradores pueden usar Windows AutoPilot para personalizar la configuración de la estación de trabajo, incluido el cambio de la edición de Windows 10 de Pro a Enterprise. Para hacer esto,

las estaciones de trabajo deben ejecutar Windows 10, versión 1703 o posterior.

Para comenzar el proceso, los administradores primero deben configurar AutoPilot creando un perfil de implementación y registrando las estaciones de trabajo que se implementarán. Esto puede incluir la modificación de la Experiencia lista para usar (OOBE) con la marca de la empresa y otras configuraciones de instalación específicas, así como la configuración de la inscripción de las estaciones de trabajo en Windows Intune. Cuando se configura AutoPilot, los usuarios de la estación de trabajo pueden seleccionar la configuración para una opción de organización en Windows 10 e iniciar sesión con sus credenciales de cuenta de Microsoft 365. AutoPilot luego completa el resto del proceso.

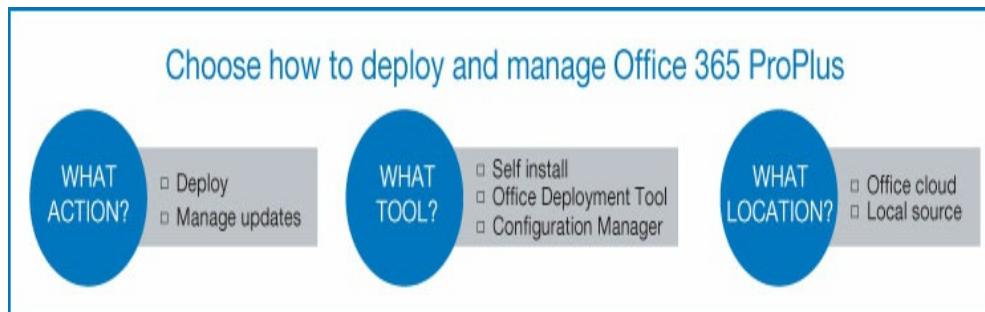
Después de implementar Windows 10 Enterprise, los administradores deben asegurarse de que las soluciones de seguridad estén activadas, como Antivirus de Windows Defender, Exploit Guard y Advanced Threat Protection.

## Fase 4: Office 365 ProPlus

En una implementación de Microsoft 365, hay varias formas de instalar Office 365 ProPlus, pero todas deben ir precedidas de un proceso de evaluación y planificación preliminar. La evaluación consiste en una revisión de las estaciones de trabajo de destino con respecto a los requisitos del sistema para Office 365, idiomas, licencias y compatibilidad con otras aplicaciones.

En la etapa de planificación del despliegue,

los administradores deben decidir qué herramienta de implementación usar, qué paquetes de instalación se necesitarán, dónde se ubicarán los archivos de origen (nube o fuente local) y qué canal de actualización de Office deben usar las estaciones de trabajo, como se muestra en Figura 2-16. En algunos casos, estas decisiones variarán para diferentes partes de la empresa, dependiendo del equipo de la estación de trabajo utilizado, la disponibilidad de conectividad a Internet y el personal administrativo disponible.



**FIGURA 2-16** Implementación de Office 365 ProPlus

**Nota:**

**Creando un piloto**

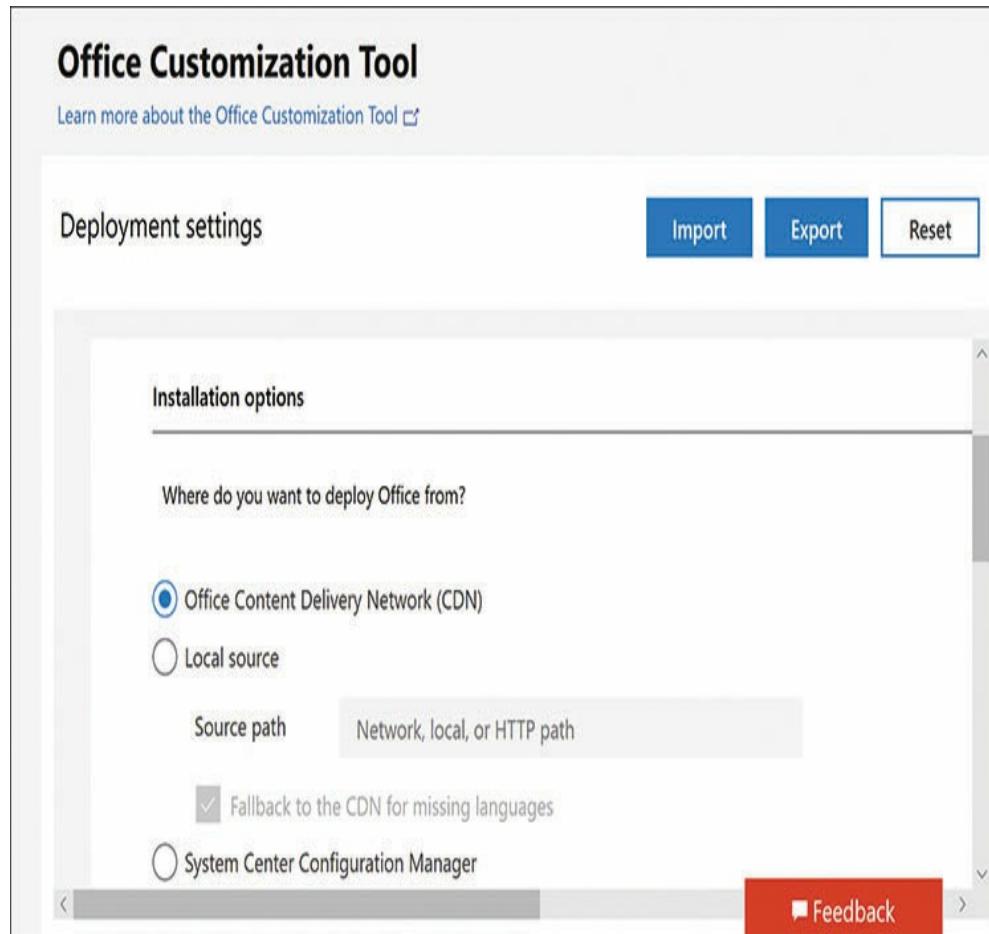
**Despliegue**

Las recomendaciones de mejores prácticas de Microsoft requieren la creación de dos grupos de implementación de Office 365 separados, un grupo piloto y un grupo amplio, cualquiera sea el método de implementación que use una organización. Esto requerirá la creación de dos colecciones o dos scripts ODT, según el método utilizado. Los administradores deben implementar primero el grupo piloto y probar la compatibilidad antes de implementar el grupo amplio.

Con el plan de implementación implementado, los administradores pueden usar cualquiera de los siguientes métodos de implementación de Office 365:

- **Administrador de configuración de System Center** Para las organizaciones que ya usan SCCM, los administradores pueden implementar Office 365 ProPlus como lo harían con otras aplicaciones, sin modificaciones especiales al procedimiento. Los administradores crean colecciones que representan grupos de estaciones de trabajo con diferentes requisitos de instalación, luego configuran el instalador de Office 365 con configuraciones como el canal de actualización a usar y si se deben agregar paquetes de idiomas. Una vez que la aplicación está configurada, los administradores pueden programar la implementación para que se realice en un momento específico.
- **Herramienta de implementación de Office (ODT) con fuente en la nube** El ODT es una herramienta de línea de comandos que utiliza un archivo de script XML para especificar la configuración de instalación de Office. Los administradores pueden modificar el script manualmente, pero Microsoft también proporciona un sitio web de la Herramienta de personalización de Office, que utiliza una interfaz gráfica para generar el código XML. La configuración predeterminada de las opciones de instalación (Office Content Delivery Network (CDN)) hace que la ODT use archivos de origen en la nube para instalar Office

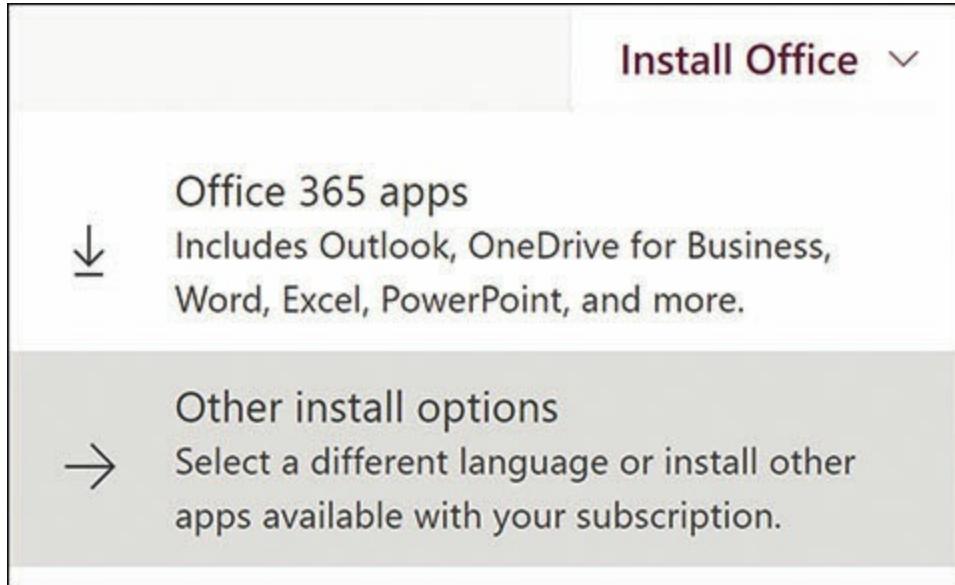
365, como se muestra en [Figura 2-17](#). Para realizar la instalación, ejecute el ejecutable ODT, nombrando el archivo de script en la línea de comando, de la siguiente manera: **setup.exe /configure scriptfile.xml**.



**FIGURA 2-17** Herramienta de personalización de Office

- **Herramienta de implementación de Office con fuente local** El proceso para instalar Office 365 usando el ODT con una fuente local requiere que los administradores creen una secuencia de comandos XML con el valor de Fuente local en la configuración de Opciones de instalación y un nombre de ruta a un recurso compartido de red. Ejecutar el ODT con el / descargar interruptor, como en `setup.exe /descargar scriptfile.xml`: Hace que el programa descargue los archivos de instalación de Office 365 a la ruta especificada en el script. Una vez que se completa la descarga, los administradores pueden implementar Office 365 ejecutando ODT con el / configurar cambiar, usando el mismo script.
- **Autoinstalación usando el portal de Office** El método de autoinstalación generalmente se usa para estaciones de trabajo que no están conectadas a la red interna.

red y que no tienen acceso a herramientas de instalación, como SCCM y ODT. Los usuarios instalan Office 365 ellos mismos iniciando sesión en [Office.com sitio web](#) utilizando sus cuentas de Microsoft 365 y haciendo clic **Instalar Office**, como se muestra en Figura 2-18 .



**FIGURA 2-18** Controles de instalación del portal de Office

Un elemento importante del proceso de implementación de Office 365 es la selección del canal de actualización que usarán las estaciones de trabajo instaladas. El canal de actualización especifica con qué frecuencia las estaciones de trabajo recibirán actualizaciones de funciones. Office 365 ProPlus admite cuatro canales de actualización, de la siguiente manera:

- **Canal semestral** Proporciona estaciones de trabajo de Office con nuevas funciones cada seis meses, en enero y julio. Este es el canal de actualización predeterminado para Office365 ProPlus, incluido en Microsoft 365.
- **Canal semestral (dirigido)** Proporciona a las estaciones de trabajo de Office nuevas funciones cada seis meses, en marzo y septiembre, cuatro meses antes de que se publiquen las mismas funciones en la publicación semestral.

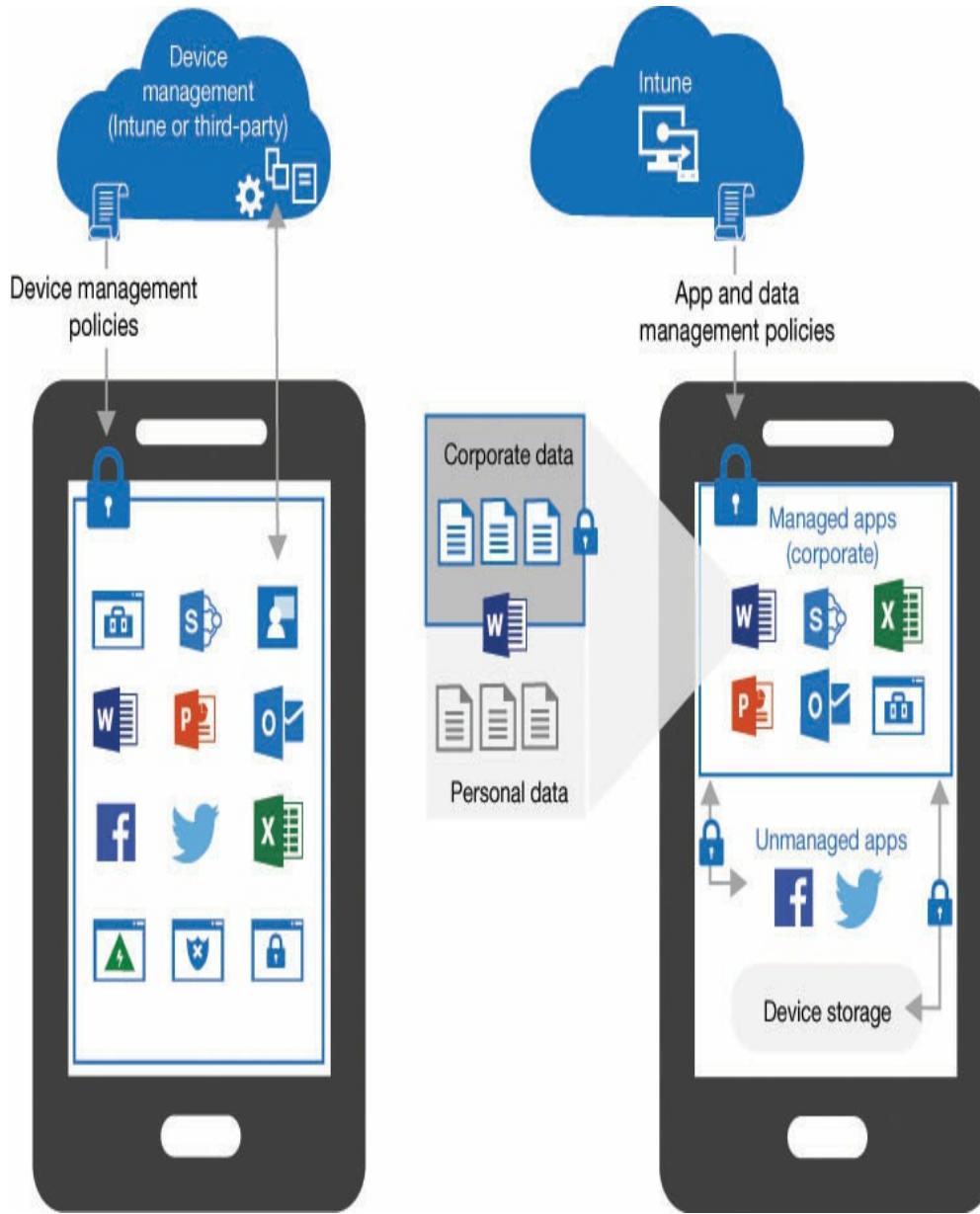
Canal. Esta opción está diseñada para implementaciones piloto o plataformas de prueba, de modo que los administradores puedan evaluar las nuevas funciones antes de que sean lanzadas a las estaciones de trabajo de producción.

- **Canal mensual** Proporciona estaciones de trabajo de Office con nuevas funciones cada mes a medida que están disponibles.
- **Canal mensual (dirigido)** Proporciona estaciones de trabajo de Office con nuevas funciones cada mes, aproximadamente una semana antes del lanzamiento del Canal mensual.

## Fase 5: Administración de dispositivos móviles

Una de las características más importantes de Microsoft 365 es la capacidad de admitir dispositivos móviles, como computadoras portátiles, teléfonos inteligentes y tabletas, incluso aquellos que ejecutan sistemas operativos que no son de Microsoft, como Android, iOS y MacOS. La herramienta que usan los administradores para administrar dispositivos móviles es Microsoft Intune, que se incluye como parte del producto Enterprise Mobility + Security.

Microsoft Intune proporciona dos formas de administrar dispositivos móviles, como se muestra en Figura 2-19 :



**FIGURA 2-19** Microsoft Intune MDM o MAM

- **Administración de dispositivos móviles (MDM)** En MDM, los dispositivos se inscriben en Intune y se convierten en dispositivos administrados. Los administradores pueden instalar aplicaciones, asignar políticas de contraseña y cifrar o eliminar cualquier información en los dispositivos administrados, así como aplicar políticas, reglas y configuraciones. MDM esencialmente le otorga a la organización un control completo

a través del dispositivo, lo que permite a los administradores asegurarse de que el dispositivo cumple con las normativas requeridas u otras políticas de la compañía.

- **Gestión de aplicaciones móviles (MAM)** En MAM, Intune administra aplicaciones específicas, pero no todo el dispositivo. Los administradores pueden imponer políticas en las aplicaciones administradas, como solicitar una contraseña para acceder a Exchange, y pueden eliminar los datos corporativos de las aplicaciones, pero no los datos del sistema. MAM se usa más comúnmente para organizaciones que admiten Bring Your Own Device (BYOD), en las que los usuarios pueden no querer otorgarle a la organización un control total sobre su propiedad, y cuando la compañía no tiene políticas rigurosas de cumplimiento de seguridad para mantener.

Como parte del proceso de planificación de Intune, los administradores deben decidir si usar MDM o MAM o ambos, y si es esto último, qué dispositivos deben usar qué modelo de administración. También es posible usar Intune en un entorno de administración híbrido junto con otro producto, como SCCM.

El proceso mediante el cual se agrega un dispositivo a Microsoft Intune para la administración se denomina inscripción. Antes de que los dispositivos puedan inscribirse en Intune, los administradores deben crear usuarios y grupos y asignarles licencias de Intune. Los administradores pueden crear usuarios y grupos manualmente o sincronizar los usuarios existentes desde Azure AD o una instalación local de AD DS. También podría ser necesario crear grupos adicionales específicamente para Intune. Por ejemplo, los administradores pueden querer crear grupos individuales para tipos de dispositivos específicos.

El proceso de inscripción puede tomar muchas formas,

dependiendo de la plataforma del dispositivo y si un administrador o usuario está inscribiendo el dispositivo. Para dispositivos BYOD, por ejemplo, los usuarios pueden descargar una aplicación de portal y realizar la inscripción ellos mismos. Para los dispositivos propiedad de la organización, los administradores pueden configurar protocolos de inscripción automática y utilizar el administrador de inscripción de dispositivos (DEM), una cuenta de usuario especial que permite la inscripción de hasta 1,000 dispositivos.

Una vez que los dispositivos están inscritos, los administradores pueden agregarles aplicaciones a través de la página de aplicaciones del Cliente en el portal Microsoft Intune. Los procedimientos para agregar aplicaciones y las tareas de administración que son posibles después de agregar las aplicaciones varían según la plataforma del dispositivo y el tipo de aplicación.

El aspecto más crítico de administrar dispositivos móviles con Microsoft Intune es proteger los recursos de la organización. Una de las formas más poderosas de hacer esto es creando *políticas de cumplimiento*, que especifican las condiciones de seguridad que debe cumplir un dispositivo. Por ejemplo, los administradores pueden crear y asignar políticas que requieren una versión mínima del sistema operativo, o especificar una longitud de contraseña requerida, o que impiden el uso de dispositivos que han sido rooteados o liberados. Según el cumplimiento del dispositivo con las políticas asignadas, los administradores pueden restringir el acceso a aplicaciones específicas o a todo el dispositivo. Se llama

*acceso condicional*

Una de las herramientas de administración más poderosas para usar con dispositivos móviles son los perfiles de dispositivos que puede crear en Microsoft Intune, que permiten a los administradores aplicar una amplia variedad de características y configuraciones que pueden mejorar o restringir las capacidades de un dispositivo.

## Fase 6: protección de la información

La fase final de la implementación de una infraestructura básica es aplicar las diversas herramientas de protección de la información incluidas con Microsoft 365, para proteger los datos confidenciales del compromiso. Como con la mayoría de las implementaciones cubiertas en esta sección, el primer paso es la planificación. Este es el proceso de evaluar los datos de la organización y crear clasificaciones, que los administradores pueden usar para determinar cuánta seguridad necesitan los diversos tipos de datos y qué herramientas deben usar para proporcionarlos.

Microsoft recomienda que las organizaciones creen al menos tres niveles de protección de seguridad, como línea de base, confidencial y clasificada, y los usen para clasificar sus datos. Los administradores pueden ensamblar los tipos de protección necesarios para cada uno de los niveles. Cada nivel sucesivo necesitará más protección que el siguiente.

Algunas de las herramientas de protección de información de Microsoft 365 que los administradores pueden aplicar a los niveles, utilizando diferentes configuraciones para cada una, si es necesario, son

sigue:

- **Etiquetas de retención** Estos especifican cuánto tiempo la organización debe retener un documento o tipo de documento en particular y qué debe suceder cuando expire el período de retención. Es posible que algunos documentos deban conservarse durante un número determinado de años y luego eliminarse, por ejemplo, mientras que otros deben conservarse indefinidamente. Los administradores pueden crear etiquetas de retención con valores específicos en el Centro de seguridad de Microsoft 365 y aplicarlas manual o automáticamente a documentos, carpetas, bibliotecas o conjuntos.
- **Etiquetas de sensibilidad** Estos identifican documentos que requieren tipos específicos de seguridad. Al igual que las etiquetas de Azure Information Protection, los administradores pueden crear etiquetas de sensibilidad de Microsoft 365 que hacen que los documentos a los que se aplican tengan marcas de agua, se cifren, se restrinjan a aplicaciones o dispositivos específicos y se protejan de otras maneras.
- **Políticas de gestión de amenazas** Los administradores pueden usar políticas de administración de amenazas en el Centro de seguridad de Microsoft 365 para protegerse contra el phishing, los archivos adjuntos de malware, los enlaces maliciosos, el spam y otros peligros.
- **Protección de información de Windows (WIP)** WIP proporciona a los administradores la capacidad de separar los datos de la compañía de los datos personales en los dispositivos de los usuarios, encriptar selectivamente los datos de la compañía, borrar los datos corporativos de un dispositivo MDM mientras deja los datos personales intactos y auditar el acceso del usuario a los datos confidenciales.
- **Prevención de pérdida de datos de Office 365** Al igual que con Exchange Online DLP, los administradores pueden crear políticas que identifiquen datos confidenciales analizando el contenido de los documentos y tomando medidas para protegerlos limitando el acceso de los usuarios y evitando el intercambio.
- **Gestión de acceso privilegiado** Permite a los administradores crear políticas que ayuden a evitar el compromiso de cuentas de administrador privilegiadas al requerir aprobación explícita para el desempeño de tareas específicas.

## Cargas de trabajo y escenarios

Independientemente del orden en que los administradores completen las fases de la implementación de la infraestructura básica, los criterios de salida para todas las fases deben cumplirse antes de que la implementación de Microsoft 365 pueda continuar. Una vez que la infraestructura de la fundación está en su lugar, los administradores pueden implementar las cargas de trabajo y los escenarios que utilizan los servicios proporcionados por la fundación.

Las cargas de trabajo de Microsoft 365 son Microsoft Teams, Exchange Online y SharePoint Online. El proceso de implementación para cada carga de trabajo consta de tres fases, como sigue:

- **Visualizar** Reúna un equipo que represente los intereses comerciales, de TI y de usuario de la empresa. Luego, haga una lluvia de ideas y priorice los escenarios en los que la organización hará uso de las capacidades que proporciona el servicio.
- **A bordo** Prepare un plan detallado para la implementación del servicio, incluida la planificación de la creación de cuentas y la migración de datos necesaria, así como si será necesaria la ayuda del programa FastTrack de Microsoft. Luego, cree una implementación piloto, preferiblemente incluyendo algunos o todos los representantes involucrados en la fase de Envision.
- **Valor de accionamiento** Implemente el servicio en el resto de la empresa, fomente su adopción según sea necesario y monitoree cuidadosamente los informes de actividad y los comentarios de los usuarios para determinar el éxito de la implementación.

Una vez que los servicios de carga de trabajo de Microsoft 365 están en su lugar, los administradores pueden comenzar a desarrollar escenarios que los utilicen, como implementar tecnologías de protección de datos, crear sitios web de equipos.

## HABILIDAD 2.4: ENTENDER LA OFICINA 365 PROPLUS

---

Office 365 ProPlus es uno de los tres componentes principales de Microsoft 365; es el que es más visible para los usuarios porque proporciona las aplicaciones que probablemente usan todos los días. Para los administradores, Office 365 ProPlus es una parte crucial del proceso de implementación de Microsoft 365 porque sus aplicaciones pueden hacer uso de todos los servicios basados en la nube que también se incluyen en el producto Microsoft 365.

Office 365 ProPlus es una de las muchas versiones de Office 365 que Microsoft ofrece para varios tipos de usuarios. Para la mayoría de los paquetes de Office 365, las aplicaciones principales son las mismas; Las diferencias son las aplicaciones y servicios adicionales que se incluyen en el paquete.

Como producto independiente, Office 365 ProPlus incluye los siguientes elementos:

- Word: procesamiento de textos Excel: hojas de cálculo y gráficos PowerPoint: gráficos de presentación Outlook: correo electrónico y programación Acceso: administración de bases de datos Editor: publicación de escritorio
-

- OneDrive: almacenamiento en la nube
- OneNote: toma de notas basada en la nube

Otros paquetes orientados a los negocios incluyen varias combinaciones de los servicios en la nube de Microsoft discutidos anteriormente en este capítulo.

El paquete de Office 365 E5, por ejemplo, agrega lo siguiente:

- **Intercambio en línea** Este es un servicio de calendario y correo electrónico basado en la nube que proporciona a los usuarios empresariales buzones y calendarios a los que pueden acceder y compartir utilizando prácticamente cualquier dispositivo.
- **SharePoint en línea** Esta es una herramienta de colaboración basada en la nube que permite a los administradores y usuarios crear sitios web y mantener bibliotecas de documentos.
- **Equipos** Este es un paquete de colaboración basado en la nube que permite a grupos de usuarios chatear, realizar llamadas telefónicas y acceder a documentos, calendarios, videos y otros recursos de aplicaciones compartidos.
- **Quejarse** Este es un servicio de red social empresarial basado en la nube.
- **Power BI** Este es un paquete de análisis de negocios y minería de datos que permite a los usuarios crear paneles, informes y otras visualizaciones de sus datos.
- **Corriente** Este es un servicio de transmisión de video que permite a los usuarios empresariales cargar, ver y compartir contenido de video.

El paquete Microsoft 365 Enterprise E5 incluye todos estos elementos, además de licencias para Windows 10 Enterprise y Enterprise Mobility + Security. El producto está diseñado para permitir que todos estos componentes trabajen juntos de manera inteligente y para proporcionar a los usuarios capacidades avanzadas de comunicación y colaboración.

El paquete Office 365 ProPlus incluido en la licencia de Microsoft 365 incluye acceso a las versiones instaladas y basadas en la web de las aplicaciones de productividad, incluidas Word, Excel, PowerPoint y Outlook. También hay versiones móviles de estas aplicaciones para dispositivos Android, iOS y Windows. También se incluyen versiones instaladas de Access y Publisher, pero no hay versiones web o móviles de estas aplicaciones.

Las aplicaciones de Office para la web y el uso móvil están limitadas en sus funciones avanzadas en comparación con las versiones instaladas, pero permiten a los usuarios con una licencia de Microsoft 365 (u Office 365) acceso completo a sus documentos utilizando cualquier computadora o dispositivo móvil conectado a Internet con Un navegador web. Los usuarios también pueden guardar documentos en su almacenamiento en la nube OneDrive para acceder más tarde.



---

#### ***Consejo de examen***

Las versiones web de las aplicaciones de Office ahora están oficialmente designadas por Microsoft como Office para la web. Anteriormente se conocían como Office Web Apps, y algunas fuentes más antiguas aún podrían referirse a ellas por ese nombre.

---

## **Comparación de Office 365 ProPlus con Office local**

Office 365 es la versión basada en suscripción de la suite de aplicaciones de Microsoft Office local que ha estado disponible durante décadas. Office se diseñó originalmente como un producto de productividad empresarial local que consistía en aplicaciones como Word, Excel y PowerPoint. Todas estas aplicaciones alguna vez fueron productos independientes, pero al agruparlas en el paquete de Office, una sola licencia le da al usuario acceso ilimitado a todas las aplicaciones. Esto simplifica el proceso de implementación y licencia para compradores y administradores de TI.

La versión más reciente del paquete local es Microsoft Office 2019, pero muchos departamentos de TI corporativos todavía usan la versión anterior, Microsoft Office 2016. El paquete incluye versiones de escritorio de Outlook, Word, Excel, PowerPoint y OneNote para Windows o Macintosh Los productos de Office 2016 y 2019 se compran directamente, por lo que no hay una tarifa de suscripción continua. Office 2016 y 2019 están disponibles en varias ediciones, con diferentes contenidos. Los administradores empresariales suelen seleccionar Office Professional Plus 2016 u Office Professional Plus

2019, ambos con licencia por volumen. Microsoft claramente está tratando de instar al mercado de Office hacia sus productos basados en suscripción.

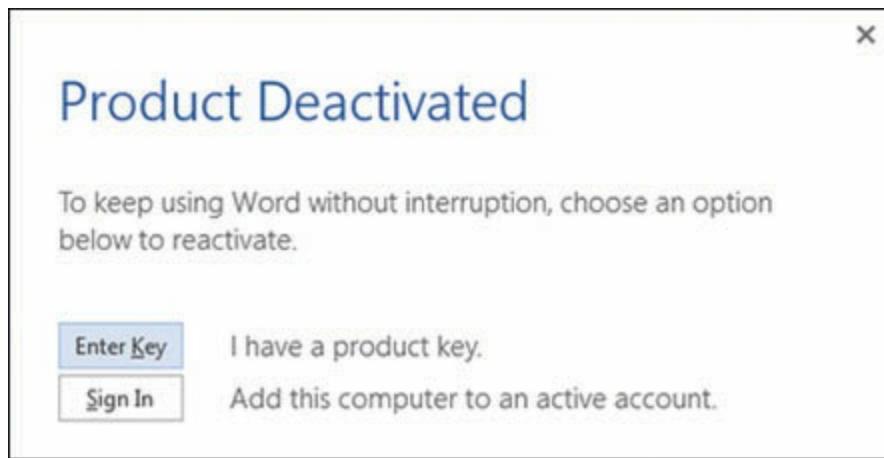
La lista de características y beneficios que no están incluidos en los paquetes de Office 2016 y 2019, pero que están disponibles

en Office 365, es largo e incluye lo siguiente:

- **Actualizaciones automáticas de funciones** Los paquetes de Microsoft 365 y Office 365 reciben actualizaciones periódicas de características, calidad y seguridad a intervalos mensuales o semestrales determinados por el administrador de la empresa. Office 2016 y 2019, de manera predeterminada, descargan automáticamente actualizaciones de calidad y seguridad todos los meses desde la Red de entrega de contenido de Microsoft (CDN), pero no reciben actualizaciones de funciones en absoluto. Las actualizaciones importantes, como Office 2016 a Office 2019, requieren la compra de una nueva licencia.
- **Dispositivos con licencia** Las licencias de Microsoft 365 y Office 365 permiten a cada usuario instalar las aplicaciones de Office en hasta cinco dispositivos. Esto significa que se puede usar una sola licencia para la oficina de un usuario, computadora portátil y computadoras domésticas, e incluso dos teléfonos inteligentes o tabletas. La licencia de Office 2016/2019 solo permite la instalación de las aplicaciones en una computadora de escritorio Windows o Macintosh.
- **Soporte del sistema operativo** Si bien Microsoft 365 incluye Windows 10 Enterprise y requiere ese sistema operativo para muchas de sus funciones de colaboración, el componente Office 365 ProPlus se puede instalar en cualquier sistema que ejecute Windows 7 con Service Pack 1 o posterior. Office 2016 también se puede instalar en cualquier sistema que ejecute Windows 7 con Service Pack 1 o posterior. Office 2019, sin embargo, requiere Windows 10.
- **Almacenamiento en la nube OneDrive** Cualquier usuario registrado puede obtener almacenamiento en la nube OneDrive, pero los suscriptores de Microsoft 365 reciben 1 TB de almacenamiento. Los usuarios sin licencia y los licenciatarios de Office 2016/2019 solo tienen permitido 5 GB.
- **Soporte técnico** Los paquetes comerciales de Microsoft 365 y Office 365 incluyen soporte telefónico y en línea las 24 horas, los 7 días de la semana, así como el servicio de implementación FastTrack. Las licencias de Office 2016/2019 tienen opciones de soporte más limitadas.
- **Alojamiento de correo electrónico y calendario** El paquete de Microsoft 365 y muchos de los paquetes de Office 365 incluyen el servicio en la nube Exchange Online, que proporciona correo electrónico y calendario. Para oficina 2016/2019

usuarios, este servicio solo está disponible como una suscripción separada, por una tarifa adicional. También hay un producto de Exchange Server local que se vende por separado.

- **Herramientas de colaboración** El paquete de Microsoft 365 y muchos de los paquetes de Office 365 incluyen servicios de colaboración basados en la nube, como SharePoint Online y Teams. Para los usuarios de Office 2016/2019, estos servicios solo están disponibles como suscripciones separadas, por tarifas adicionales. SharePoint también está disponible como servidor local, se vende por separado.
- **Modo de funcionalidad reducida** Con Microsoft 365 y Office 365, si caduca la suscripción de un usuario, si un administrador elimina la licencia del usuario o si la computadora en la que están instaladas las aplicaciones de Office no se conecta a Internet al menos una vez cada 30 días, Office entra en una funcionalidad reducida modo y muestra un mensaje como el que se muestra en Figura 2-20 . En el modo de funcionalidad reducida, el usuario puede abrir, ver e imprimir documentos existentes, pero todas las funciones de edición están deshabilitadas y el usuario no puede crear documentos nuevos. Office 2016 y 2019 nunca vuelven a un modo de funcionalidad reducida y no se requiere que los usuarios se conecten a Internet.



**FIGURA 2-20** Advertencia del modo de funcionalidad reducida de Office 365

Mientras que los usuarios individuales pueden ver estas omisiones como

inconvenientes considerables para los productos de Office 2016 y 2019, para los administradores empresariales, esto no es necesariamente así. En algunos casos, los administradores pueden preferir que las aplicaciones de Office no reciban actualizaciones de funciones, debido a los problemas adicionales de soporte y capacitación que pueden causar. En la empresa, cada nuevo problema de soporte se multiplica por cientos o miles de usuarios, por lo que la aparición repentina de cambios sustanciales o nuevas características en las aplicaciones de Office puede ser más problemático de lo que vale.

En cuanto a los servicios adicionales en la nube proporcionados en muchos de los paquetes de Microsoft 365 y Office 365, como los que proporcionan correo electrónico y colaboración, muchas organizaciones ya tienen soluciones para estos servicios y no quieren pagar por funciones que no necesitan o no desean. . El soporte técnico de Microsoft para usuarios individuales también podría no ser necesario, ya que los administradores de empresas suelen proporcionar ese soporte ellos mismos. Muchas organizaciones grandes también obtienen Office 2016 o 2019 comprando una licencia por volumen, que podría incluir soporte de incidentes, en caso de ser necesario.

## **Despliegue de oficina**

El proceso de implementación de Office 365 ProPlus en un entorno empresarial se describe anteriormente en este capítulo en " Comprender la implementación de Microsoft

---

y modelo de lanzamiento . " Dado que Office 365 se distribuye utilizando el modelo

Hacer clic y ejecutar, los administradores pueden elegir si usar la Herramienta de implementación de Microsoft Office (ODT) o el Administrador de configuración de System Center (SCCM) para implementar Office 365, o pueden permitir que los usuarios lo instalen para ellos mismos desde el portal de autoservicio.

Al implementar Office 365 usando la ODT, los administradores pueden modificar el archivo de configuración XML que contiene la configuración de las opciones de instalación manualmente, o pueden usar el sitio web de la Herramienta de personalización de Office (OCT) para crear el archivo XML usando una interfaz gráfica.

De forma predeterminada, Office 365 instala todas las aplicaciones en el paquete, pero la OCT permite a los administradores omitir selectivamente aplicaciones específicas de la instalación, como se muestra en Figura 2-21. .

---

**Apps**

Turn apps on or off to include or exclude them from being deployed

Access	<input checked="" type="checkbox"/> On	Excel	<input checked="" type="checkbox"/> On
OneDrive (Groove)	<input type="checkbox"/> Off	Skype for Business	<input checked="" type="checkbox"/> On
OneDrive Desktop	<input checked="" type="checkbox"/> On	OneNote 2016	<input type="checkbox"/> Off
Outlook	<input checked="" type="checkbox"/> On	PowerPoint	<input checked="" type="checkbox"/> On
Publisher	<input checked="" type="checkbox"/> On	Teams	<input checked="" type="checkbox"/> On
Word	<input checked="" type="checkbox"/> On		

**Next**

**FIGURA 2-21** Selectores de aplicaciones en la herramienta de personalización de Office

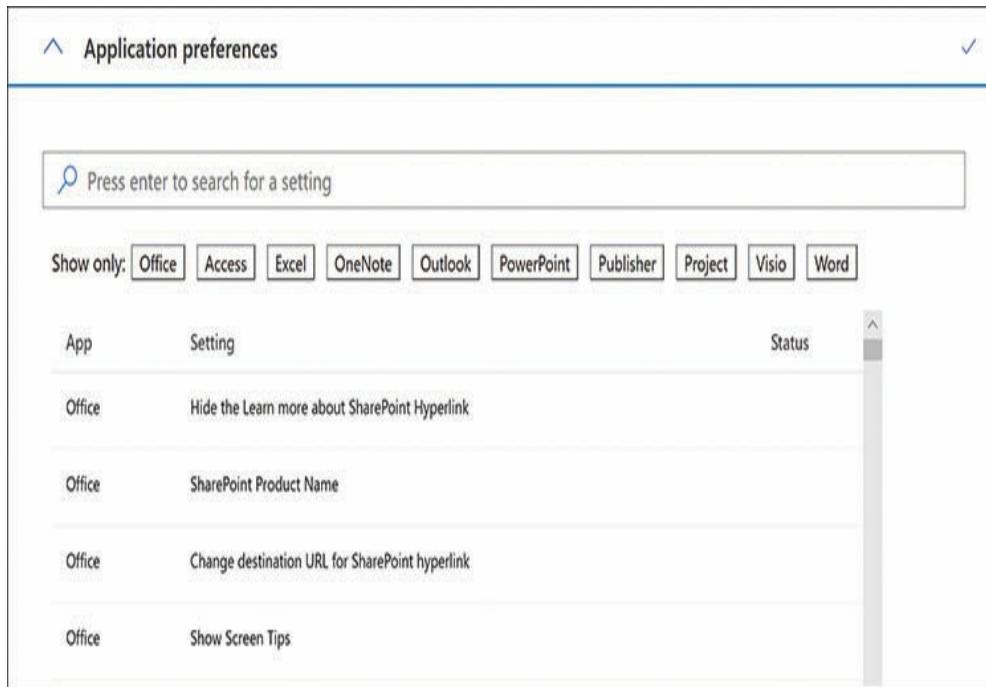
Cuando excluye aplicaciones que usan OCT, el sitio crea un archivo XML que se modifica para incluir un *ExcludeApp* código, como en el siguiente ejemplo que excluye la aplicación Publisher.

Haga clic aquí para ver la imagen del código

```
<Agregar SourcePath = "\\\ Server \ share" Version = "15.1.2.3" OfficeClientEdition =
"32">
<Product ID = "O365ProPlusRetail">
    <Language ID = "en-us" /> <ExcludeApp ID =
"Publisher" /> </Product> </Add>
```

Además de seleccionar las aplicaciones para instalar, OCT también proporciona controles para las siguientes opciones:

- **Arquitectura** 32 bits o 64 bits
- **Productos** La edición específica de Office 365 que se instalará
- **Productos adicionales** Permite la adición de otros productos de Microsoft a la instalación, como Project y Visio
- **Actualizar canal** Especifica cuál de los cuatro canales de actualización disponibles debe usar la instalación
- **Versión** Permite la selección de una versión de compilación de producto específica o solo la última versión
- **Idioma** Especifica el idioma principal para la instalación, además de idiomas adicionales y herramientas de corrección
- **Instalación** Especifica el origen de los archivos de Office 365 (CDN, disco local o SCCM) y configura las opciones de instalación, como si la instalación debe estar registrada y ser visible para el usuario
- **Actualizar y actualizar** Especifica el origen de los archivos de actualización futuros y si se deben desinstalar instalaciones anteriores de MSI
- **Licencias y activación** Para instalaciones con licencia por volumen, especifica el origen de la clave del producto (KMS o MAK)
- **General** Permite al administrador agregar el nombre de la organización y una descripción a la instalación
- **Preferencias de aplicación** Permite al administrador configurar cientos de configuraciones de directiva, para Office en su conjunto y para las aplicaciones individuales, como se muestra en Figura 2-22. .



**FIGURA 2-22** Preferencias de aplicación en la herramienta de personalización

de Office

#### Hacer clic para ejecutar

*Hacer clic para ejecutar* es un sistema de entrega de software que se basa en las tecnologías de virtualización y transmisión desarrolladas para Microsoft Application Virtualization (App-V). Durante el proceso de instalación, se crea un espacio de aplicación virtualizado en la computadora y el paquete de Office se descarga en él. Debido a que los datos se transmiten desde el CDN de Microsoft en la nube, las aplicaciones de Office pueden comenzar a ejecutarse a medida que avanza la instalación. Por lo tanto, las funciones básicas son operativas mientras que las funciones más avanzadas aún se están descargando en segundo plano, como se muestra en Figura 2-23. .



**FIGURA 2-23** Procesamiento en segundo plano en una instalación de Office 365 de Hacer clic y ejecutar

Debido a que el software se ejecuta dentro de un entorno virtualizado, no entra en conflicto con otro software en el sistema. En su mayor parte, los únicos datos que pasan del sobre virtualizado al sistema local son los datos del usuario. Los usuarios pueden incluso instalar múltiples versiones de Office en un sistema sin conflictos, siempre que sean todas instalaciones de Hacer clic y ejecutar.

Hacer clic y ejecutar también es la base de las actualizaciones de Office. En lugar de publicar archivos de parches individuales que contengan actualizaciones, Microsoft lanza una compilación completa y nueva de Office a la CDN. A intervalos regulares, una computadora en la que está instalado Office ejecuta una tarea programada y compara su versión instalada de Office con la última publicada en el CDN. El sistema puede descargar solo los bits nuevos que necesita para actualizar la instalación. Esto reduce la cantidad de datos que deben descargarse y, al igual que con la instalación inicial, las actualizaciones se transmiten, por lo que el trabajo puede continuar mientras se descargan e instalan.

El ODT se está posicionando como la principal herramienta de implementación empresarial para Office 365. Si bien todavía es posible usar SCCM para organizar las implementaciones de Office 365, todavía usan la versión Hacer clic y ejecutar del paquete de instalación. Además, debido a la virtualización inherente al modelo de entrega Click-to-Run, es posible que los administradores que inviertan en tecnología AppV creen sus propios paquetes de Office 365 y los implementen a los usuarios desde una fuente local, como lo harían con cualquier otro paquete de aplicaciones .

## Implementaciones de Office 2016 y 2019

Office 2019 no tiene un portal de autoservicio, por lo que es poco probable que los administradores en un entorno empresarial tengan usuarios que instalen el producto ellos mismos.

Sin embargo, Office 2019 usa Hacer clic y ejecutar y, por lo tanto, admite tanto ODT como SCCM para la implementación empresarial.

Cuando se anunció que Office 2019 solo se podía instalar usando Hacer clic y ejecutar, muchos administradores de TI se indignaron. La versión previa local, Office 2016, se lanzó en un momento en que el modelo de instalación de Hacer clic y ejecutar se usaba para las versiones domésticas de Office, pero los licenciatarios por volumen aún usaban el método de implementación tradicional de Windows Installer (MSI). Algun tiempo después, Click-to-Run estuvo disponible para todos los productos de Office 2016, pero el modelo de instalación MSI se mantuvo para aquellos administradores que lo prefirieron.

El método de implementación de Windows Installer requiere el uso de un paquete que contenga software de Office en el formato MSI. El producto de Office solo estaba disponible en formato MSI desde el Centro de licencias por volumen de Microsoft para organizaciones que compran un Acuerdo de empresa con Software Assurance. Para administrar las licencias, las organizaciones deben obtener Claves de activación múltiple (MAK) o mantener un servidor local del Servicio de administración de claves (KMS). Para implementar el MSI, los administradores pueden usar SCCM u otros productos de entrega de software.

La principal objeción a la sustitución del modelo de implementación de MSI con Hacer clic y ejecutar es una resistencia a

cambio. El modelo Click-to-Run ofrece muchas ventajas: es más rápido de instalar, los paquetes son más pequeños y el software siempre está actualizado. Click-toRun es esencialmente el método moderno de implementación de administración, pero todavía hay administradores que detestan cambiar a una nueva tecnología cuando la anterior ha estado funcionando bien durante años.

## **HABILIDAD 2.5: ENTENDER COLABORACIÓN Y MOVILIDAD CON MICROSOFT 365**

---

Hubo un tiempo en que era común que los lugares de trabajo se dividieran en oficinas y cubículos. Las personas trabajaban solas, solo se unían para reuniones celebradas en una sala de conferencias separada, lejos de sus espacios de trabajo. Entonces, el diseño de oficina abierta se hizo popular; las paredes del cubículo se cayeron y los trabajadores se vieron obligados a funcionar como un equipo durante todo el día. Ambos extremos tienden a causar problemas. O fue difícil reunir al equipo para un tiempo de colaboración de calidad, porque sus materiales se dejaron en su mayoría en sus espacios de trabajo, o se sintieron apretados y sofocados al estar unidos todo el tiempo. Lograr un equilibrio entre estos dos extremos puede mejorar tanto la armonía como la productividad. Los trabajadores que pueden colaborar cuando sea necesario y aún así dedicar un tiempo a la concentración por su cuenta, a menudo pueden impulsar

proyecto hacia la finalización de manera más eficiente.

Microsoft 365 es un producto diseñado para proporcionar a los trabajadores exactamente este tipo de flexibilidad. Al principio puede parecer un simple paquete de un sistema operativo, un conjunto de aplicaciones de productividad y un paquete de seguridad. Sin embargo, la combinación de Windows 10, Office 365 y Enterprise Mobility + Security está diseñada para ser más que la suma de sus partes.

Microsoft 365 incluye aplicaciones de usuario final y servicios en la nube, todos los cuales trabajan juntos para crear un entorno que permita a las personas comunicarse y colaborar cuando lo necesiten, desde cualquier lugar donde se encuentren. Se pueden realizar reuniones en las que todos los miembros del equipo se encuentran en sus propios espacios de trabajo: en la oficina, en el hogar o en la carretera. Los mensajes pueden intercambiarse por el medio que mejor se adapte a los propósitos del equipo: chat, correo electrónico, voz o videoconferencia. Los documentos se pueden almacenar en la nube para que los usuarios puedan leerlos, editarlos o publicarlos desde cualquier lugar, utilizando cualquier dispositivo. Los usuarios pueden trabajar individualmente, en pares o en grupos de cualquier tamaño, en cualquier combinación, en cualquier lugar.

## Herramientas de colaboración de Microsoft 365

Esta sección examina las capacidades de colaboración integradas en los componentes de Microsoft 365, y luego

analiza cómo las personas pueden usarlos para mejorar sus flujos de trabajo.

## Intercambio en línea

Como plataforma de servidor de mensajería de correo electrónico de Microsoft, Exchange es la herramienta de colaboración más familiar para la mayoría de los usuarios. El correo electrónico proporciona una comunicación rápida multiplataforma, pero a menudo no es inmediato, y aunque los correos electrónicos pueden transportar información entre los miembros del equipo, su naturaleza asincrónica les impide ser el equivalente colaborativo de una conversación cara a cara.

Además de los intercambios de correo electrónico uno a uno, Exchange Online también admite varios otros medios para que los usuarios colaboren utilizando mensajes de correo electrónico, como los siguientes:

- **Listas de distribución** También conocidas como grupos de distribución, las listas de distribución permiten a los usuarios enviar mensajes de correo electrónico a múltiples destinatarios simultáneamente. Esta herramienta de colaboración ha estado disponible en Exchange durante muchos años, pero los grupos de Office 365 ahora ofrecen una alternativa más poderosa.
- **Lista de distribución dinámica** Esta es una variación de una lista de distribución estándar en la que la membresía se calcula cada vez que se envía un mensaje a la lista, según las reglas establecidas por el administrador de la lista. Por ejemplo, las reglas pueden especificar que todos los usuarios en un departamento específico o en una ubicación específica se incluyan como miembros de la lista. Cada vez que se envía un mensaje a la lista, solo los usuarios identificados por las reglas en ese momento se incluyen en el grupo.
- **Grupos de seguridad habilitados para correo** Por lo general, se usan grupos de seguridad

para asignar permisos a los recursos, mientras que los grupos de distribución se utilizan para enviar correos electrónicos. Sin embargo, es posible habilitar el correo para un grupo de seguridad, de modo que los usuarios que posean permisos para un recurso protegido puedan ser notificados por correo si hay problemas relacionados con ese recurso. Por ejemplo, si una impresora está fuera de línea por mantenimiento o reparaciones, sus usuarios pueden ser notificados por correo electrónico de su falta de disponibilidad.

- **Buzones compartidos** Por lo general, los buzones compartidos son buzones de Exchange con calendarios adjuntos que representan un rol en lugar de un individuo, al que pueden acceder varios usuarios. Por ejemplo, un departamento de soporte técnico puede crear un buzón compartido llamado

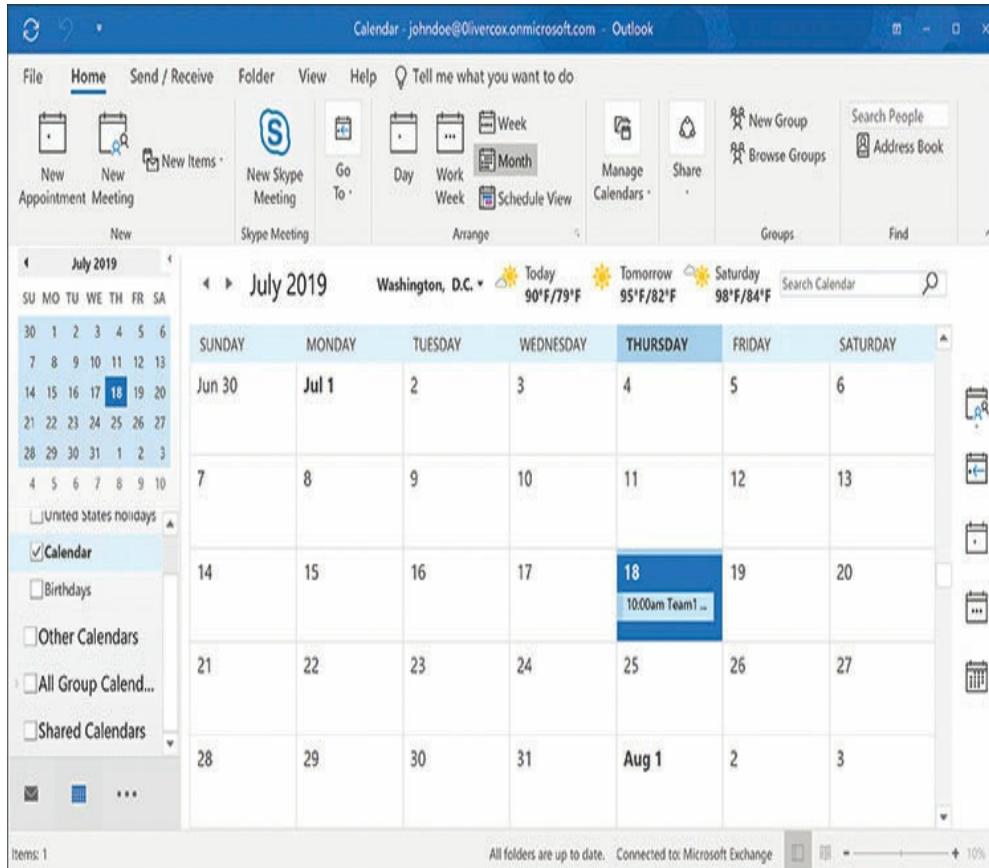
[helpdesk@domain.com](mailto:helpdesk@domain.com), que es monitoreado por los miembros del equipo que están de servicio en un momento dado.

- **Carpetas públicas** Exchange puede mantener una jerarquía de carpetas que contienen documentos que están disponibles para cualquier usuario. Los administradores pueden vincular una carpeta pública a un grupo de distribución para que el correo enviado al grupo se agregue automáticamente a la carpeta.

Si bien estos mecanismos tienen sus usos, y muchos administradores se han acostumbrado a usarlos durante años, los grupos de Office 365 ofrecen una solución más integral para la colaboración que funciona en todas las aplicaciones y servicios de Office 365.

Además de los buzones, Exchange Online proporciona a cada usuario un calendario que proporciona capacidades de programación, recordatorio y uso compartido, como se muestra en Figura 2-24. Los usuarios pueden compartir sus calendarios con sus compañeros de trabajo, lo que les permite ver su disponibilidad y planificar reuniones y citas. Los grupos de Office 365 también tienen sus propios calendarios, por lo que los miembros del grupo pueden compartir su información de programación con el equipo y crear reuniones que no entren en conflicto con las de los demás.

## obligaciones



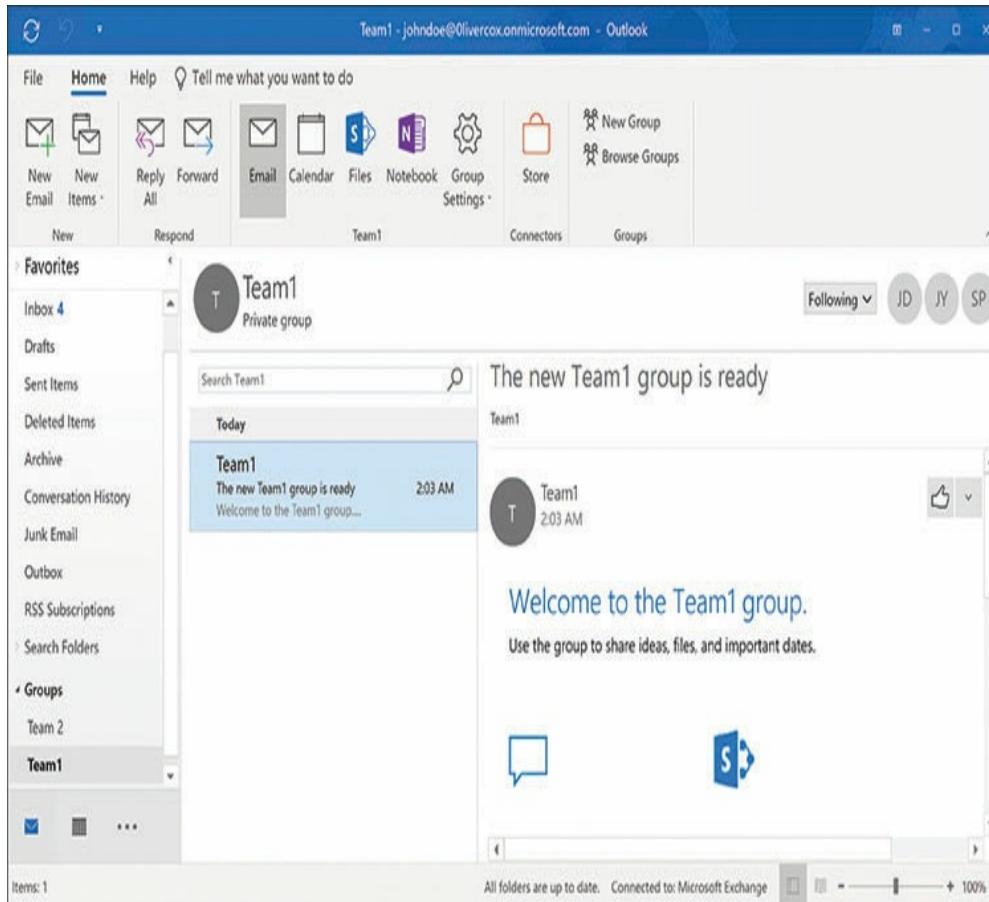
**FIGURA 2-24** Un calendario de Exchange Online como se muestra en Outlook

## Grupos de Office 365

Los grupos de Office 365 permiten a los administradores proporcionar a los miembros del grupo acceso a recursos que abarcan los servicios que ofrece Microsoft. La creación de un grupo de Office 365 crea automáticamente los siguientes recursos, a los que pueden acceder todos los miembros del grupo:

- **Buzón compartido de Exchange en línea** Esta es una bandeja de entrada que muestra todo

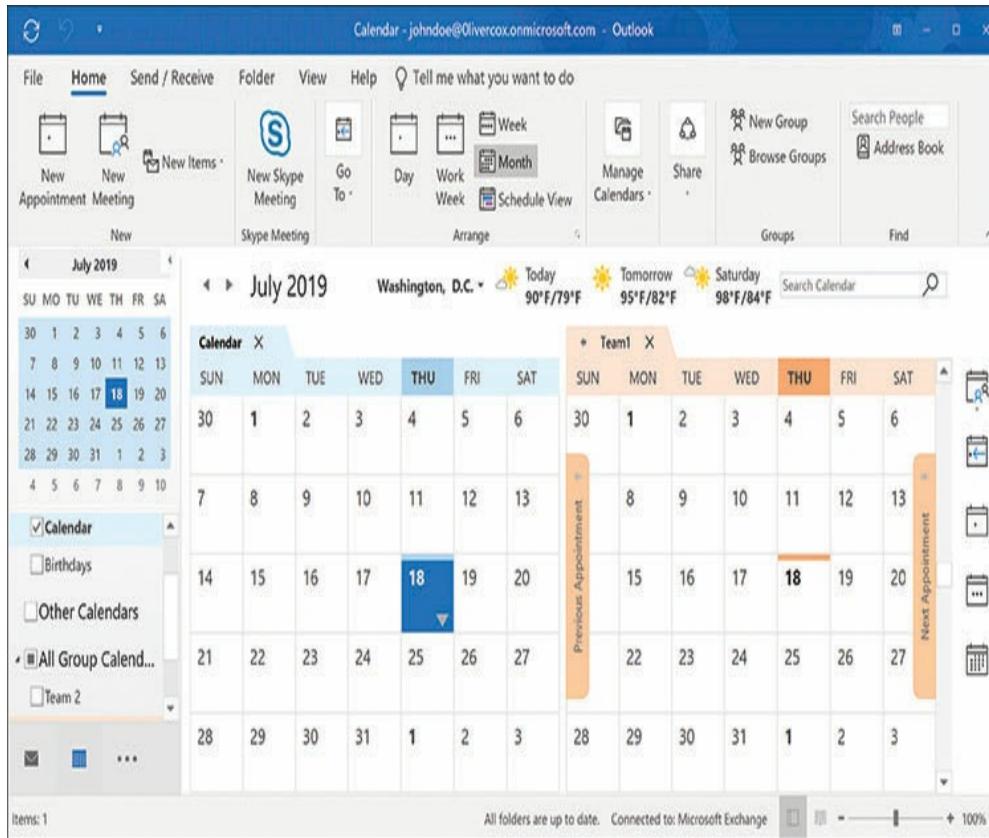
Los mensajes de correo electrónico enviados al grupo. A diferencia de una lista de distribución, la bandeja de entrada se puede buscar y mantiene un registro permanente de las comunicaciones por correo electrónico del grupo. Los usuarios pueden mostrar el contenido de la bandeja de entrada del grupo por separado en Outlook, como se muestra en Figura 2-25 , o suscríbase al grupo, para que los mensajes aparezcan en sus carpetas personales de la bandeja de entrada.



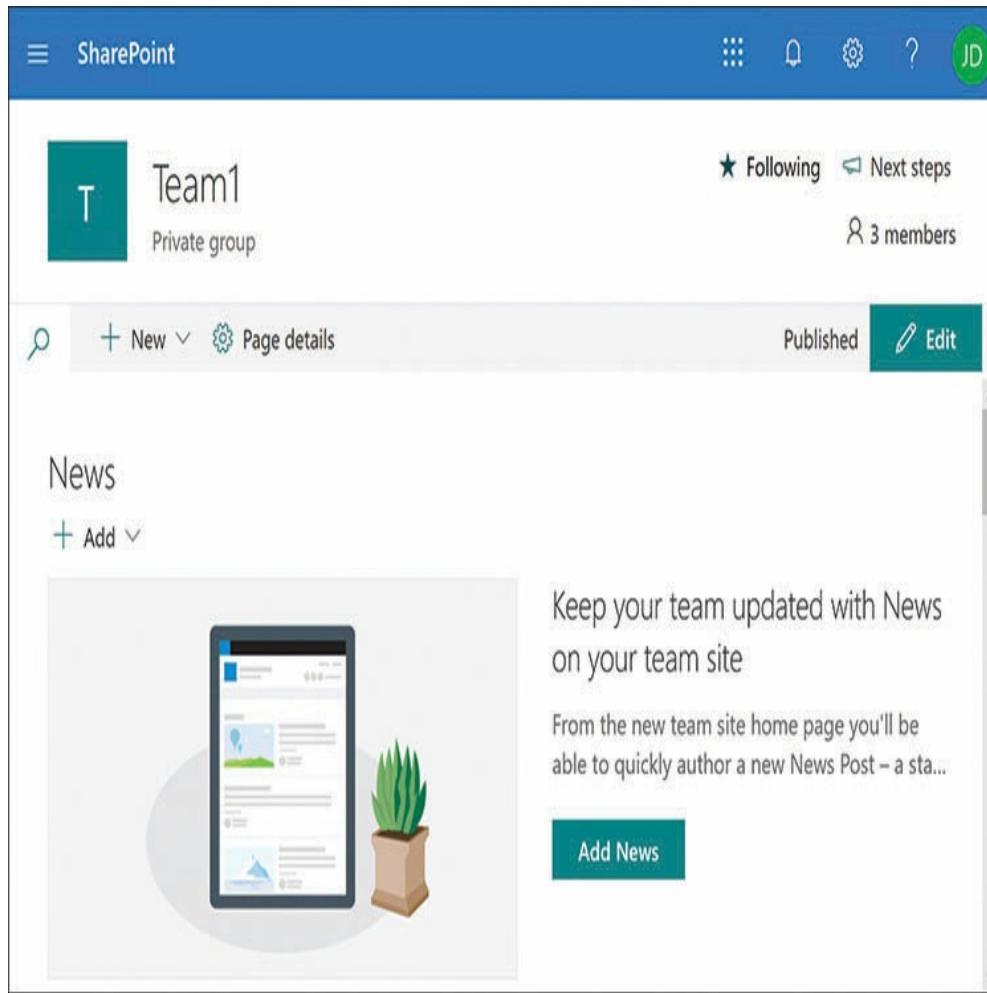
**FIGURA 2-25** Outlook muestra una bandeja de entrada de grupo de Office 365

- **Calendario compartido de Exchange Online** El grupo tiene un calendario separado que se comparte, por lo que los miembros están invitados a todos los eventos publicados en ese calendario. Al igual que con la bandeja de entrada, los usuarios pueden configurar Outlook para agregar los eventos del calendario grupal a sus calendarios personales, o verlos por separado, como se muestra en Figura 2-26. .

- **Sitio de grupo compartido de SharePoint Online** La creación de un grupo de Office 365 también crea un sitio de grupo dedicado para el grupo en SharePoint Online, como se muestra en Figura 2-27. , que incluye una biblioteca donde los miembros del grupo pueden almacenar, compartir y colaborar en documentos.

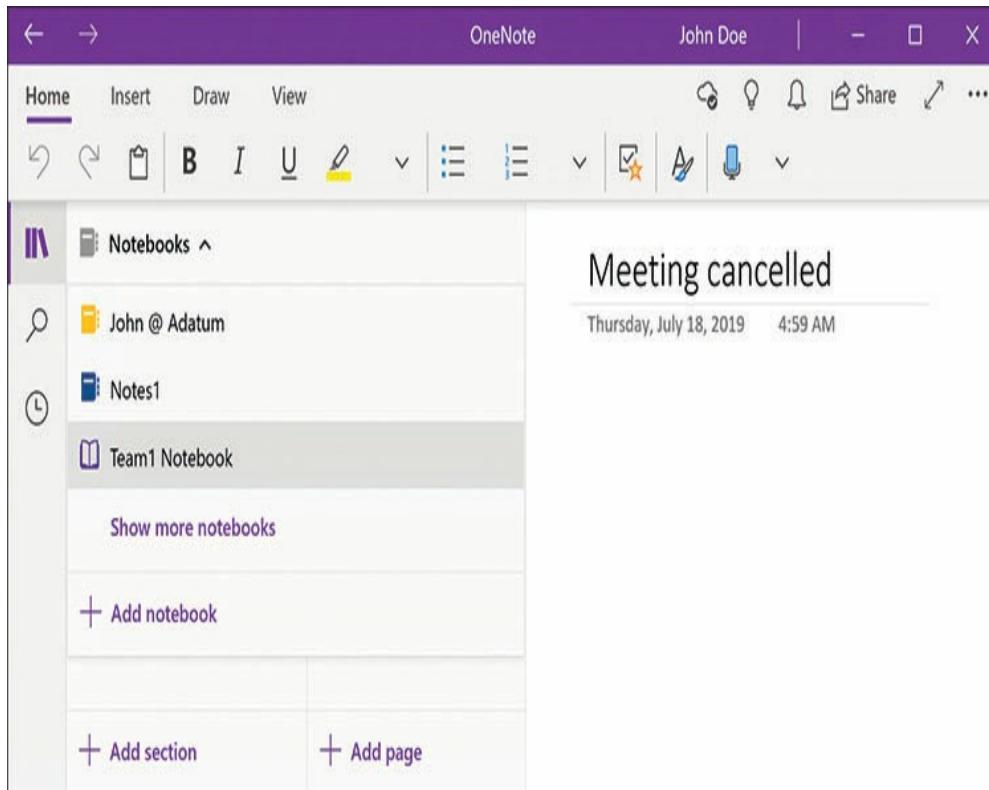


**FIGURA 2-26** Una página de calendario de Outlook con calendarios de usuarios y grupos



**FIGURA 2-27** Sitio de grupo de SharePoint Online predeterminado para un grupo de Office 365

- **Cuaderno compartido de OneNote** Como parte de la creación del sitio de grupo del grupo en SharePoint Online, se crea un cuaderno dedicado, al que los miembros pueden acceder a través del cliente web OneNote o la aplicación de escritorio, como se muestra en Figura 2-28. .

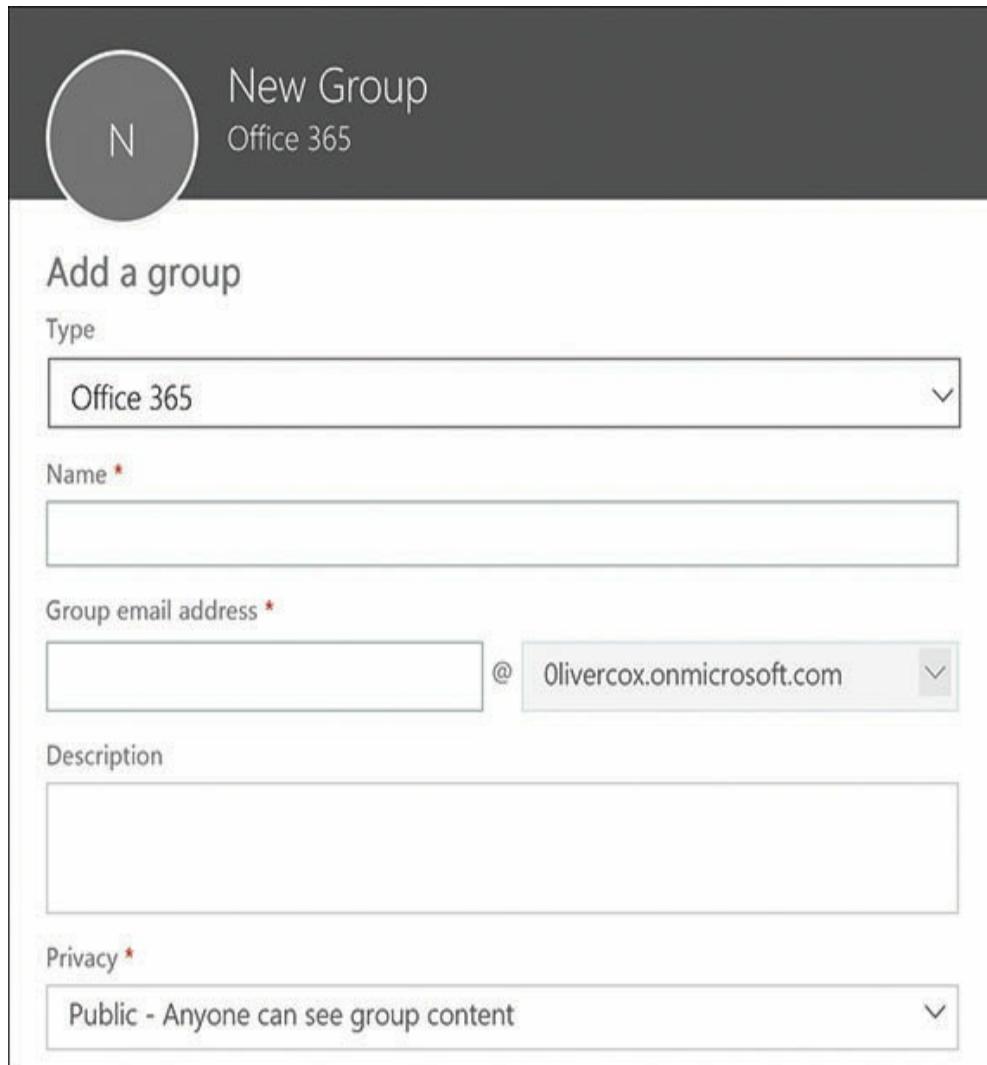


**FIGURA 2-28** Cliente OneNote que muestra un cuaderno de grupo de Office

365

Debido a su utilidad en muchas de las aplicaciones y servicios, existen métodos para crear grupos de Office 365 en muchas herramientas diferentes de Microsoft 365, algunas de las cuales crean el grupo directamente y otras indirectamente, incluidas las siguientes:

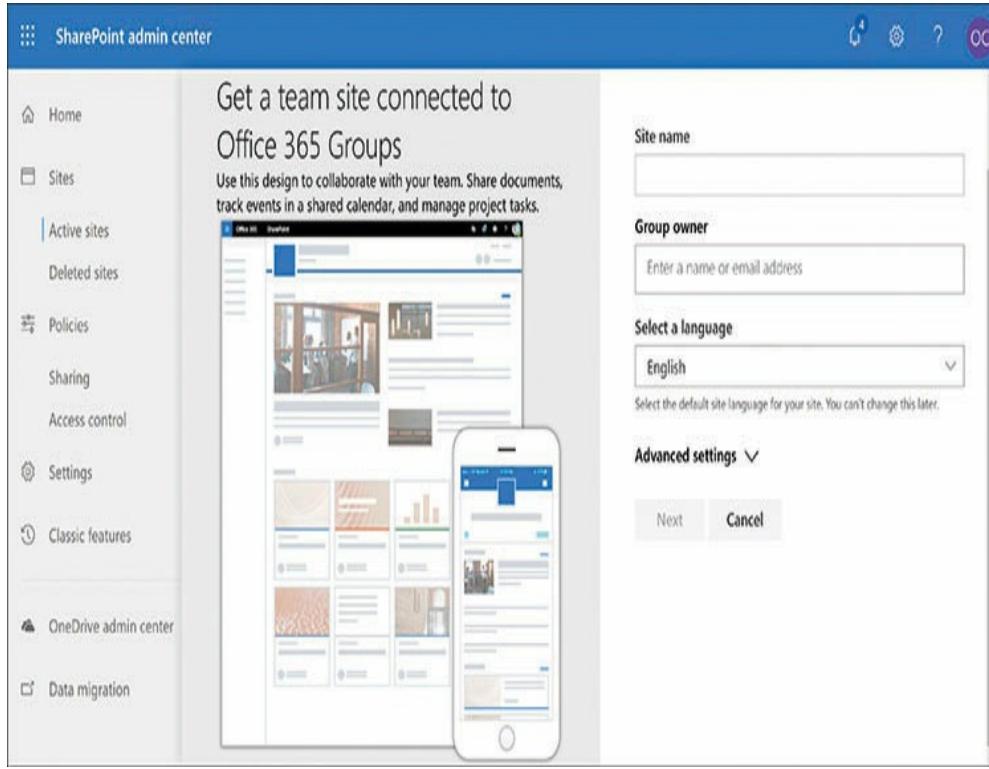
- **Centro de administración de Microsoft 365** En la página Grupos, haciendo clic en **Agregar un grupo** muestra la interfaz que se muestra en Figura 2-29., con el que puede crear un grupo de Office 365, así como una lista de distribución, seguridad o grupo de seguridad habilitado para correo.



**FIGURA 2-29** La nueva interfaz de grupo en el Centro de administración de Microsoft 365

- **Centro de administración de Azure Active Directory** Sobre el **Todos los grupos** página, haciendo clic **Nuevo grupo** abre una interfaz en la que puede crear un grupo de Office 365 o un grupo de seguridad.
- **Centro de administración de Exchange Online** Sobre el **Destinatarios** página, seleccionando el **Grupos** pestaña y haciendo clic **Nuevo grupo de Office 365** abre una nueva ventana que contiene una interfaz para la creación de un nuevo grupo.

- **Centro de administración de SharePoint Online** Cuando crea un nuevo sitio de grupo en el Centro de administración de SharePoint Online, usando la interfaz que se muestra en Figura 2-30 , se crea automáticamente un grupo de Office 365, que está asociado con el sitio y usa el mismo nombre.

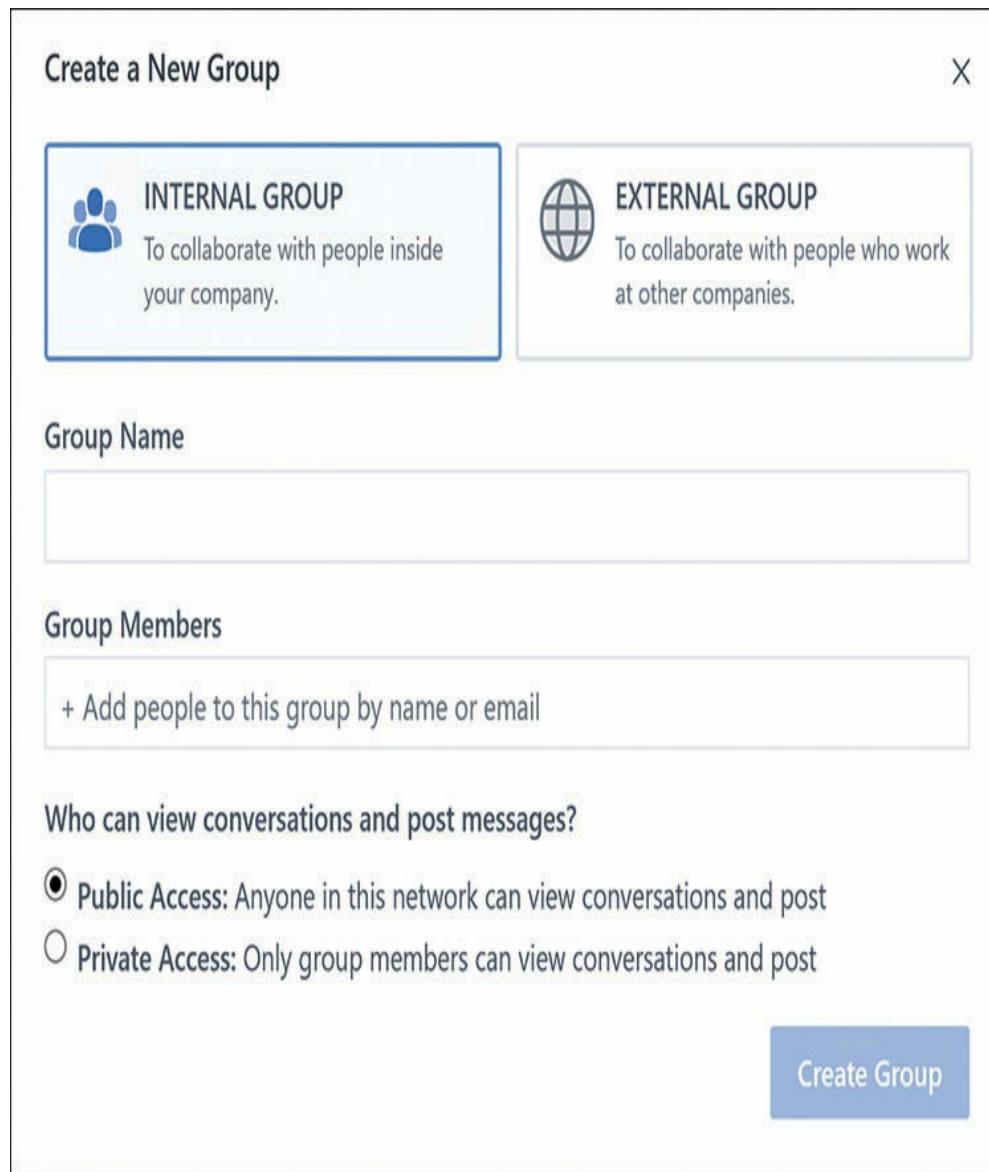


**FIGURA 2-30** La interfaz de creación del sitio de grupo en el Centro de administración de SharePoint Online

- **panorama** Los grupos de Office 365 pueden ser creados por usuarios y administradores. los **Nuevo grupo** El botón en la pestaña de inicio permite al usuario de Outlook crear un grupo público o privado y agregarle miembros.
- **Quejarse** Crear un grupo de Office 365 en Yammer seleccionando **Crear un grupo** en el panel de navegación le permite especificar si desea crear un grupo interno o externo, como se muestra en [Figura 2-31](#) . Los grupos internos permiten a los miembros colaborar solo con personas dentro de la organización, mientras que los miembros de grupos externos pueden

colaborar con personas ajenas a la organización.

- **Planificador** Cuando un usuario crea un nuevo plan en Planner, la herramienta crea un grupo de Office 365 para él de manera predeterminada. Los usuarios también pueden optar por crear un plan y asociarlo con un grupo de Office 365 que ya existe.



**FIGURA 2-31** La interfaz Crear un nuevo grupo en Yammer

Estas interfaces tienen diferentes apariencias, pero la mayoría de ellas requieren la misma información, incluida la siguiente:

- **Nombre del grupo** Especifica el nombre por el cual el grupo aparecerá en todas las herramientas de Microsoft 365.
- **Dirección de correo electrónico grupal** Especifica una dirección de correo electrónico en el dominio empresarial para el buzón de Exchange que se crea junto con el grupo.
- **Público o privado** Esta configuración especifica si cualquiera puede ver el contenido del grupo o solo los miembros del grupo pueden ver el contenido del grupo.
- **Nombre del dueño** Especifica el usuario que funcionará como el propietario del grupo y recibirá acceso administrativo completo a sus propiedades.

## SharePoint en línea

Como se señaló anteriormente en este capítulo, SharePoint Online es un servicio que aloja sitios web de centro de intranet, comunicación y equipo que permiten a los usuarios almacenar bibliotecas de documentos y también colaborar en los documentos editándolos simultáneamente. En la colección de servicios en la nube de Microsoft 365, SharePoint Online ocupa una posición interesante, ya que puede funcionar como un destino final para los usuarios y proporcionar almacenamiento de archivos a otros servicios, como Microsoft Teams.

Los administradores pueden crear fácilmente sitios de grupo de SharePoint Online separados para cada proyecto en el que trabaja un grupo de usuarios y llenar los sitios no solo con bibliotecas que contienen los documentos y archivos que los usuarios necesitarán, sino también con listas, elementos de noticias, aplicaciones y enlaces a otro

páginas web, entre otras cosas.

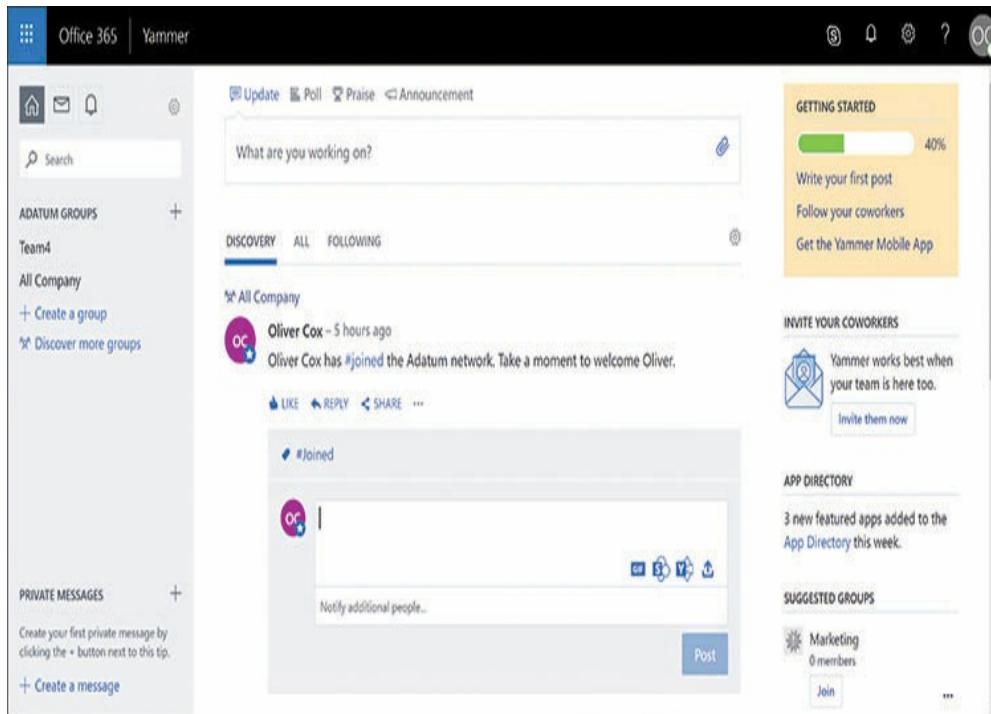
El acceso al sitio del grupo está controlado por el grupo de Office 365 que se crea automáticamente con el sitio del grupo. Agregar usuarios al grupo les otorga los permisos que necesitan. Los usuarios pueden acceder a un sitio de grupo desde la página de inicio de SharePoint usando cualquier navegador, o pueden usar las aplicaciones móviles de SharePoint. Los usuarios también pueden acceder a los archivos en un sitio de grupo utilizando OneDrive para la Empresa.

Los sitios de equipo de SharePoint Online también se pueden integrar en una interfaz de Microsoft Teams, junto con elementos proporcionados por otros servicios de Microsoft 365, como buzones de Exchange Online, archivos de OneDrive, videos Stream y grupos de Yammer.

## **Microsoft Yammer**

Yammer está diseñado para ser un servicio de red social basado en la nube para una empresa, permitiendo a los usuarios de toda la organización comunicarse y colaborar utilizando los otros servicios de Microsoft 365. Los usuarios de Yammer pueden comunicarse mucho como lo hacen en Facebook y otras aplicaciones de redes sociales, como se muestra en

Figura 2-32 , excepto que el servicio es local para la empresa. Los administradores pueden admitir usuarios externos, pero solo por invitación.



**FIGURA 2-32** La interfaz web de Yammer

Al igual que Teams, Yammer permite a los usuarios acceder a otros servicios de Microsoft 365 disponibles en la interfaz de Yammer. Por ejemplo, los usuarios pueden abrir una videollamada, programar una reunión en Outlook, acceder a archivos almacenados en OneDrive o colaborar en un documento de una biblioteca de SharePoint, todo desde una conversación de Yammer.

En el modelo de colaboración de Microsoft 365, Yammer se ubica en lo que se conoce como el bucle externo, la audiencia más amplia dentro de la empresa. Estas son personas con las que un usuario podría no trabajar todos los días. Si bien Yammer puede proporcionar colaboración grupal, muchos

Las organizaciones lo utilizan para proporcionar un canal de comunicación alternativo en toda la empresa, que permite a los usuarios que rara vez se ven porque trabajan en diferentes departamentos o ciudades diferentes para construir una identidad corporativa.

Si bien Yammer a menudo se conoce como una herramienta de red social, el hecho de que su alcance esté restringido a la empresa significa que su comunicación no necesita ser estrictamente social. Es posible que no todos los usuarios de Yammer estén en el mismo equipo del proyecto, trabajando hacia un objetivo definido, pero aún pueden intercambiar información valiosa entre ellos sobre las mejores prácticas o la cultura corporativa.

- información que puede generar un sentido de comunidad que no puede existir en un servicio de Internet con miles de desconocidos.

### **OneDrive para hacer negocios**

Cada usuario que registra una cuenta personal de Microsoft para usar con Windows 10 u otras aplicaciones recibe una cuenta gratuita de OneDrive para almacenar archivos personales en la nube. OneDrive para la Empresa es un servicio equivalente que se proporciona con Microsoft 365. OneDrive y OneDrive para la Empresa son casi idénticos en su funcionalidad. Los usuarios pueden acceder a sus archivos OneDrive desde cualquier dispositivo con acceso a la nube y sincronizar sus archivos en un disco local.

La diferencia principal entre OneDrive y

OneDrive para la Empresa es que este último se administra como parte de Microsoft 365. Los usuarios de Office 365 reciben 1 TB de espacio de almacenamiento en la nube en una cuenta personal de OneDrive. Sin embargo, en OneDrive para la Empresa, los administradores de Microsoft 365 controlan la cantidad de espacio asignado a cada usuario y los permisos de acceso otorgados a ese espacio.

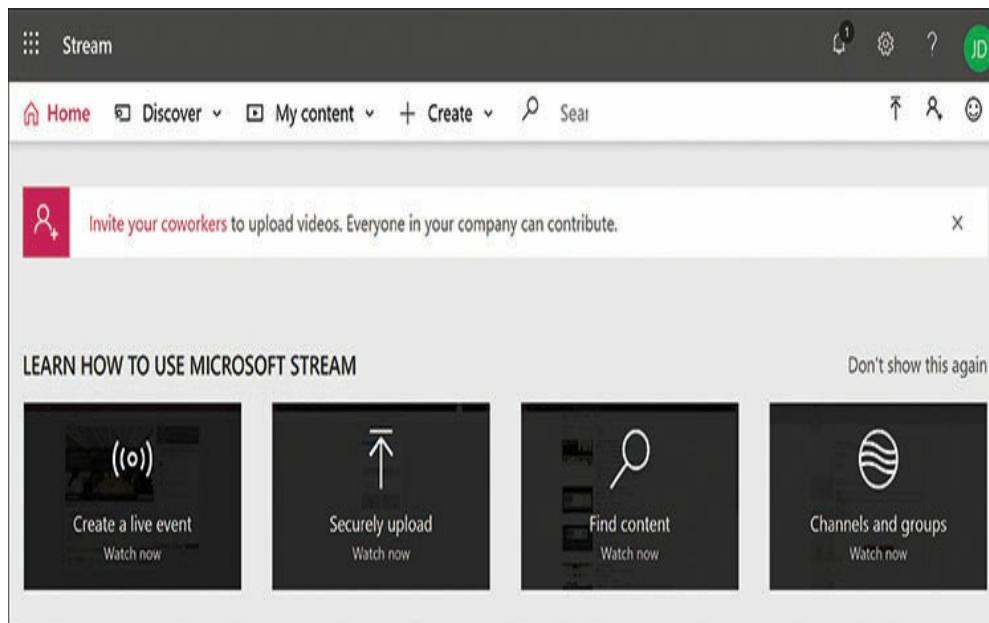
OneDrive para la Empresa sirve como medio de almacenamiento para otros servicios de Microsoft 365. Office 365 lo usa para almacenamiento en la nube general, y Microsoft Teams lo usa para almacenar archivos de usuario, así como archivos compartidos en chats privados. Sin embargo, los archivos compartidos en un canal de Teams se almacenan en una biblioteca de SharePoint Online asociada a un sitio de grupo. Los usuarios también pueden acceder a los documentos almacenados en las bibliotecas de SharePoint Online utilizando el cliente OneDrive.

## **Microsoft Stream**

Microsoft Stream es un servicio de almacenamiento y distribución de video que permite a los clientes del navegador transmitir video y también proporciona contenido de video a otros servicios de Microsoft 365, incluidos Office 365, Exchange Online, SharePoint Online, Teams y Yammer. El servicio Stream incluye su propio almacenamiento basado en Azure y, por lo tanto, tiene sus propias cuotas de almacenamiento.

Además de aceptar contenido de video preexistente cargado por los usuarios, como se muestra en Figura 2-33. , Microsoft Stream puede procesar eventos en vivo creados en Teams,

Yammer, o Stream en sí y proporcionarlos como video transmitido a usuarios en tiempo real o más tarde como contenido de video a pedido.

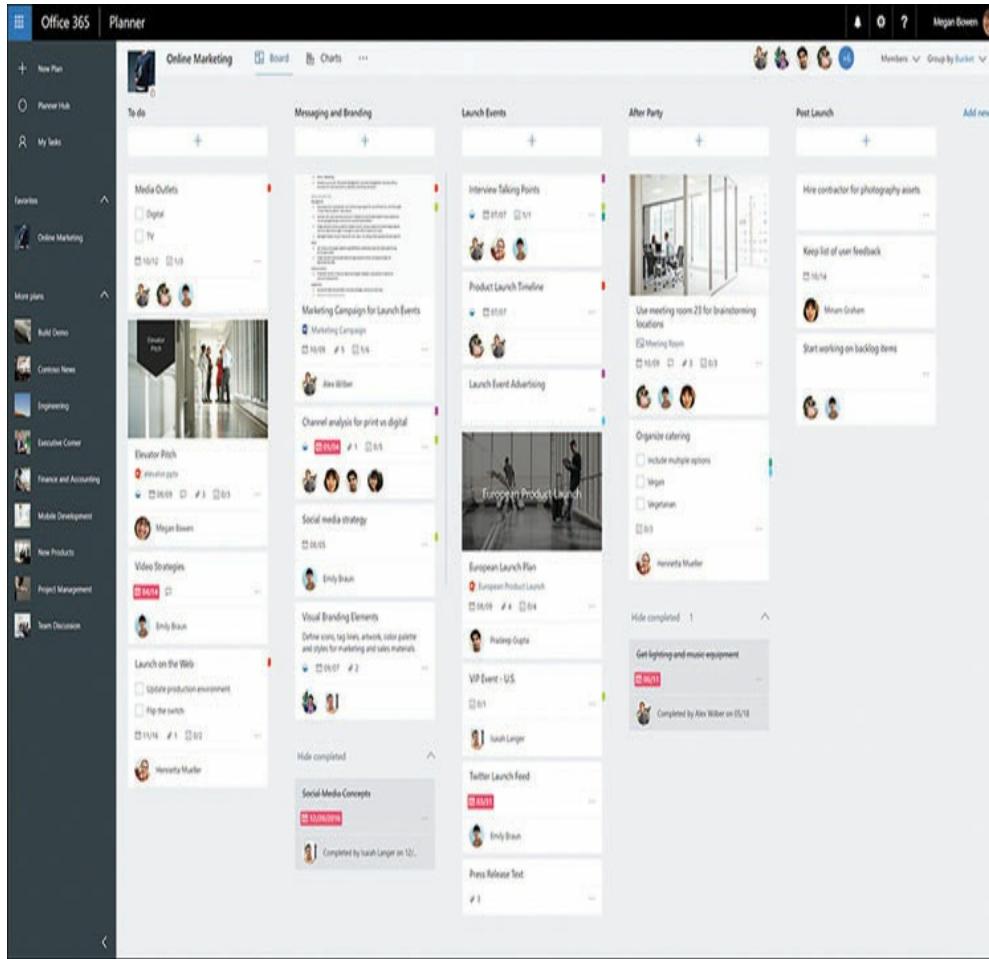


**FIGURA 2-33** La interfaz de la página de inicio de Microsoft Stream

Stream también puede mejorar el contenido de video al generar transcripciones de voz a texto y subtítulos, así como al identificar e indexar las caras de las personas que hablan en el video. Esto permite a los usuarios localizar material de archivo específico en un video buscando términos hablados o localizando un orador en particular. Stream también ha introducido una función de "desenfoque" que permite desenfocar el fondo en un video, eliminar distracciones y artefactos no deseados y concentrar la atención del espectador en el orador.

## Microsoft Planner

Microsoft Planner es una herramienta de administración de proyectos simple que permite a los usuarios crear planes y completarlos con tareas, eventos y otros elementos de varios servicios de Microsoft 365. La vista predeterminada de un plan consta de columnas verticales llamadas cubos, cada una de las cuales consiste en tareas, como se muestra en Figura 2-34. Las tareas pueden contener gráficos, enlaces y archivos alojados por SharePoint Online.



**FIGURA 2-34** Un plan creado en Microsoft Planner

Cuando un usuario crea un plan, se crea automáticamente un grupo de Office 365, cuyos miembros son aquellos a quienes se aplica el plan. Lo contrario también es cierto; cuando un usuario o administrador crea un grupo de Office 365, se crea un plan para él. Al igual que con todos los grupos de Office 365, también hay un buzón de grupo y un calendario asociados, que los usuarios del plan pueden emplear para programar citas y eventos y recibir notificaciones por correo electrónico.

Un plan Planner también se puede integrar en Microsoft Teams agregando una nueva pestaña a la página General de un equipo. Por lo tanto, los usuarios pueden trabajar con tareas planificadas mientras están en contacto con otros miembros del equipo a través de chat o llamada.

## **Equipos de Microsoft**

Si Yammer es parte del ciclo externo en el modelo de colaboración de Microsoft 365, Microsoft Teams está en el ciclo interno, las personas que se ven y trabajan juntas todos los días. Teams es otra herramienta de colaboración que puede alojar elementos proporcionados por otros servicios de Microsoft 365. La función principal que realmente está integrada en Teams es su capacidad de chat y llamadas de voz / video.

Por lo tanto, la herramienta está diseñada en torno a grupos que trabajan activamente en tiempo real y deben comunicarse de forma continua e inmediata, sin los retrasos de latencia inherentes a otros medios como el correo electrónico. Como se señaló anteriormente, este es exactamente el tipo de herramienta de colaboración que

puede permitir que los miembros del equipo funcionen en sus espacios de trabajo nativos y aún así mantenerse en comunicación constante con sus colegas, incluso cuando están a kilómetros de distancia y utilizan diferentes dispositivos.



---

### ***Consejo de examen***

Office 365 anteriormente confiaba en Skype Empresarial para llamadas de voz y videoconferencias. Estas capacidades ahora se han incorporado a los equipos de Microsoft. Microsoft está despreciando el producto Skype for Business e insta a las organizaciones que actualmente usan Skype for Business a planear migrar a Teams. Los candidatos para el examen MS-900 deben tener en cuenta que muchas fuentes antiguas de Microsoft 365 y Office 365 todavía hacen referencia a Skype for Business.

---

Además del chat y las llamadas que proporcionan comunicación básica, los otros componentes que los miembros del grupo pueden necesitar son proporcionados por otros servicios de Microsoft 365, como los siguientes:

- Grupos de Office 365
- Intercambie buzones y calendarios de usuarios y grupos Sitios de grupo de
- SharePoint Online OneDrive para el almacenamiento empresarial
- 
- Transmite grabaciones de reuniones y listas de tareas del Planificador de
- contenido de video
- OneNote notebook para compartir

Uno de los principales beneficios de Teams es que todos estos elementos se pueden combinar en una única interfaz unificada, evitando que los usuarios tengan que cambiar constantemente de una aplicación a otra. Los administradores pueden agregar pestañas a una página de canal en la interfaz de Teams que usan conectores para vincular a otras aplicaciones de Microsoft 365, como una hoja de cálculo de Excel o un plan Planner. Esto es especialmente ventajoso para los usuarios que trabajan en dispositivos móviles con pantallas más pequeñas, como teléfonos inteligentes y tabletas. El entorno de Teams, por supuesto, se almacena en la nube, y los usuarios pueden acceder a él a través de una interfaz basada en la web, utilizando una aplicación de escritorio o con aplicaciones para todas las principales plataformas móviles.

Cuando crea un equipo en Equipo, consta de un solo canal, llamado General. Para grupos que trabajan en proyectos múltiples, también es posible crear canales adicionales, que tienen sus propias conversaciones de chat, direcciones de correo electrónico y carpetas de SharePoint. Para grupos cuyos miembros abarcan países o culturas, la capacidad de chat en Teams también incluye la capacidad de traducir mensajes en más de cuarenta idiomas.

## Colaborando en Microsoft 365

Como debería quedar claro en las secciones anteriores, Microsoft 365 proporciona una amplia gama de herramientas y capacidades de colaboración. Para algunos administradores, podría

incluso sea demasiado amplio, requiriendo una gran cantidad de pruebas y evaluaciones, incluso para determinar cuáles de las muchas formas de colaboración disponibles son las más adecuadas para sus usuarios.

Para una red empresarial mundial con decenas o cientos de miles de usuarios, puede haber una causa suficiente para implementar todos los componentes de Microsoft 365 y utilizarlos de diferentes maneras, pero para organizaciones más pequeñas, una implementación selectiva podría ser La mejor opción. ¿Cómo pueden los administradores determinar qué servicios son más adecuados para sus usuarios y cómo pueden determinar cuáles de las muchas formas de colaboración son mejores para ellos?

La colaboración en un entorno Microsoft 365 depende de las necesidades específicas del grupo o equipo. Para determinar qué herramientas de colaboración son mejores, considere preguntas como las siguientes:

- ¿Cuántas personas hay en el grupo o equipo? ¿Qué tan oportunos son los requisitos
- de comunicación del equipo? ¿Dónde están ubicados los miembros del grupo o
- equipo? ¿Los miembros del equipo tienen que compartir y editar documentos? ¿Qué
- otros medios son necesarios para el flujo de trabajo del equipo?
- 

Las respuestas a preguntas como estas pueden ayudar a los administradores a determinar qué componentes pueden beneficiar mejor a los usuarios en su entorno de colaboración. Tomemos, por ejemplo, un equipo de proyecto que a la vez

trabajen juntos en la misma sala, generando ideas sobre el proyecto y generando informes juntos. Ahora, sin embargo, los miembros del equipo están ubicados en varias ciudades diferentes y algunos viajan con frecuencia.

La comunicación básica del equipo podría ser por correo electrónico, especialmente si usaban un buzón grupal como el suministrado por un grupo de Office 365. Esto proporcionaría a todos acceso a todos los mensajes de correo electrónico generados por los miembros. Sin embargo, en un entorno de equipo, puede ser difícil mantener una conversación verdadera en el correo electrónico. Las respuestas pueden retrasarse y los usuarios pueden terminar sin responder a la última publicación. Un entorno de chat, como el proporcionado por Microsoft Teams, podría adaptarse mejor al grupo.

Para los requisitos de procesamiento de documentos, un sitio de grupo de SharePoint Online puede permitir que varios usuarios trabajen en el mismo documento, emulando el tipo de colaboración que puede ocurrir en una sola habitación. Los documentos almacenados en un sitio de SharePoint se pueden integrar fácilmente en un entorno de Microsoft Teams.

Microsoft Planner puede servir en una capacidad de gestión de proyectos, asignando tareas a usuarios específicos, manteniendo un cronograma para el grupo y generando citas de calendario y notificaciones por correo electrónico. La información del planificador también se puede integrar en los equipos.

Mientras los miembros del equipo están trabajando, ya sea por

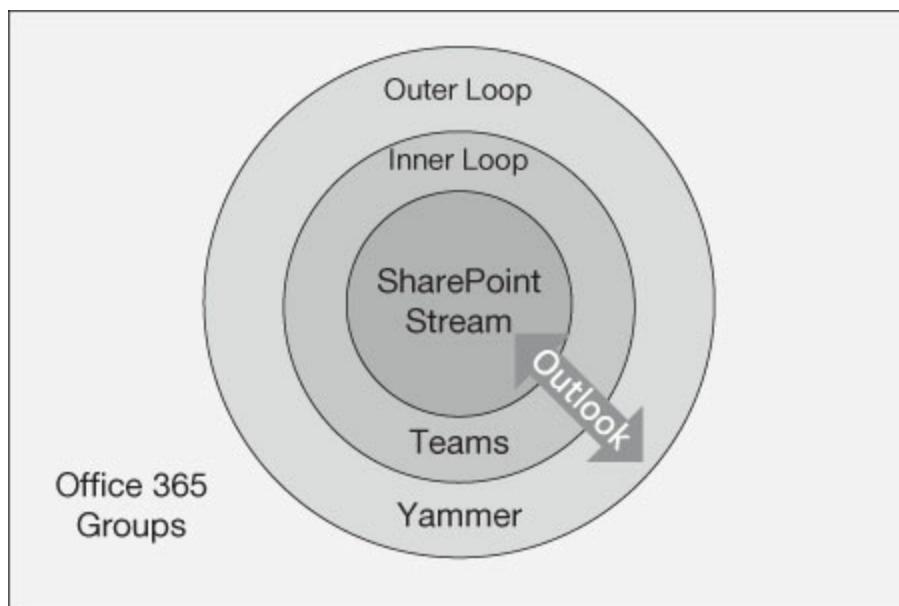
ellos mismos o en el chat, tomar notas puede ser un medio importante para mantener un registro de actividades. Microsoft OneNote permite a los usuarios mantener portátiles en la nube y compartirlos con los otros miembros del grupo. Los portátiles también se pueden integrar en el entorno de Teams.

Si bien el chat puede proporcionar un flujo de conversación constante e inmediato, las videoconferencias o presentaciones también pueden ser necesarias a intervalos regulares. Los equipos pueden proporcionar capacidad de llamadas, y Microsoft Streams puede mantener un registro de video de las llamadas, generando transcripciones e índices faciales para referencia futura. Esto, si bien un administrador puede decidir que Microsoft Teams es la herramienta preferible para crear un entorno de colaboración unificado para este grupo en particular, la solución real también puede involucrar a otros servicios de Microsoft 365.

Este ejemplo se basa en Teams, pero para un proyecto grupal que no requiere las capacidades de chat que proporciona Teams, muchos de los mismos servicios se pueden integrar en un sitio de grupo de SharePoint Online. Los administradores que están familiarizados con SharePoint podrían preferir atenerse a las herramientas que conocen en lugar de adoptar nuevas. Sin embargo, para los administradores, el uso más eficiente de los servicios en la nube de Microsoft 365 sería pensar en el producto general como una caja de herramientas y, después de familiarizarse con todas las herramientas disponibles,

elija los correctos para cada trabajo en particular.

Microsoft piensa en sus herramientas de colaboración en términos de los roles que pueden cumplir en una organización. Al igual que un diagrama de un sistema solar, el modelo de colaboración de Microsoft 365 consta de bucles externos e internos y un núcleo central, como se muestra en Figura 2-35 .



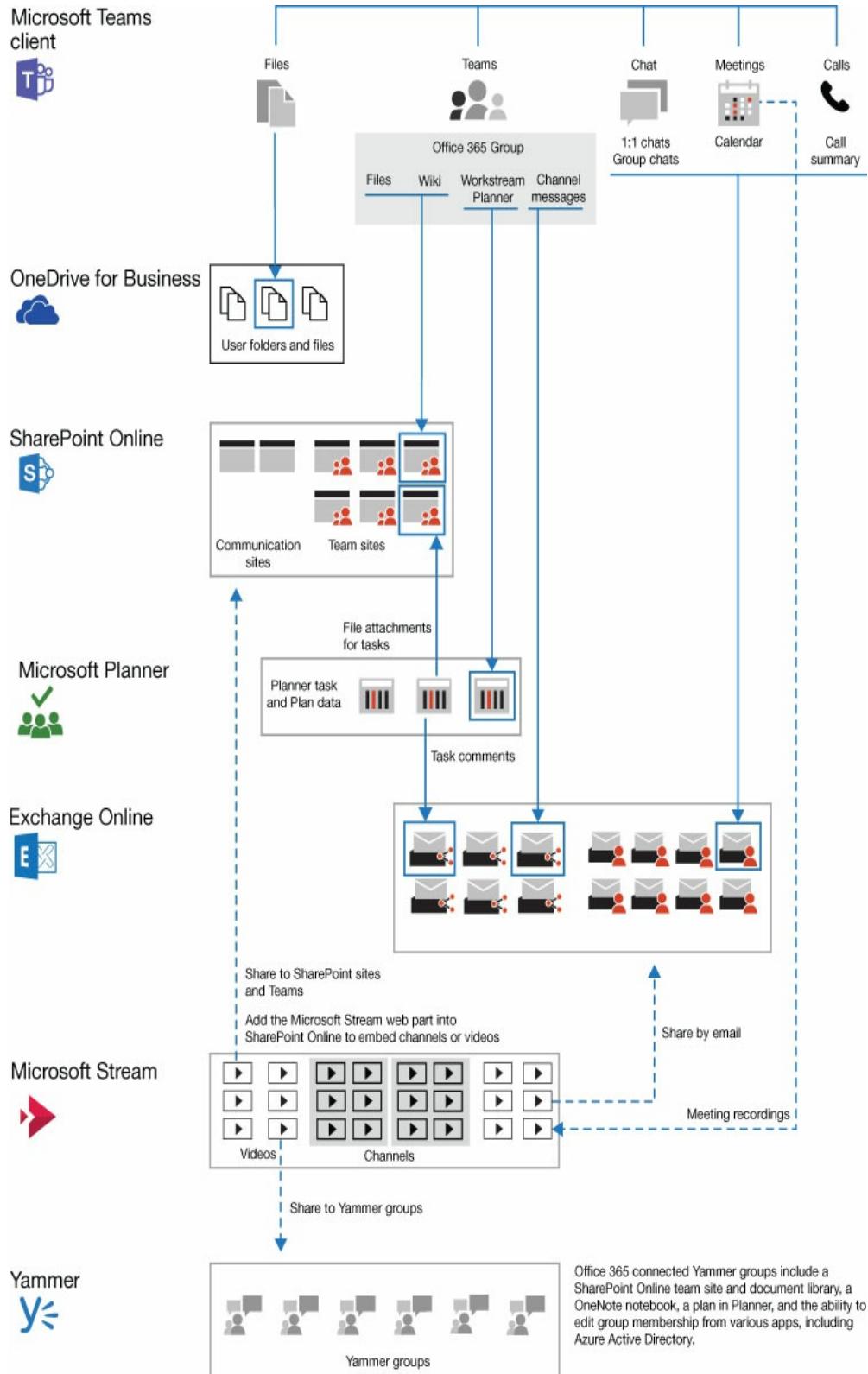
**FIGURA 2-35** El sistema de herramientas de colaboración

Microsoft 365

El bucle externo, que representa el grupo más grande de usuarios en la empresa, es atendido por Yammer, que proporciona un medio de comunicación que abarca la empresa. Teams presta servicio al bucle interno, que representa a las personas que los usuarios conocen y trabajan a diario. Servicios como SharePoint y Stream, en el centro del sistema, brindan servicios a ambos bucles, al igual que Outlook

Proporciona comunicación entre ambos. Subyacente a todo el modelo se encuentran los grupos de Office 365, que proporcionan servicios de identidad para toda la organización.

Las interrelaciones entre los servicios de Microsoft 365 pueden ser extremadamente complejas, con algunos componentes alimentando contenido a muchos de los otros. Por ejemplo, como se muestra en **Figura 2-36**, el servicio Microsoft Stream puede suministrar contenido de video a sitios de SharePoint Online, grupos de Yammer y enviar video directamente a los buzones de usuarios o grupos de Exchange Online. Los equipos de Microsoft pueden recibir el mismo video de los sitios de grupo de SharePoint Online. Stream también puede grabar video de las reuniones de Microsoft Teams y proporcionar ese video a otros servicios, creando una red de suministro y entrega de contenido que se mejora aún más por el intercambio de archivos y mensajes de correo electrónico.



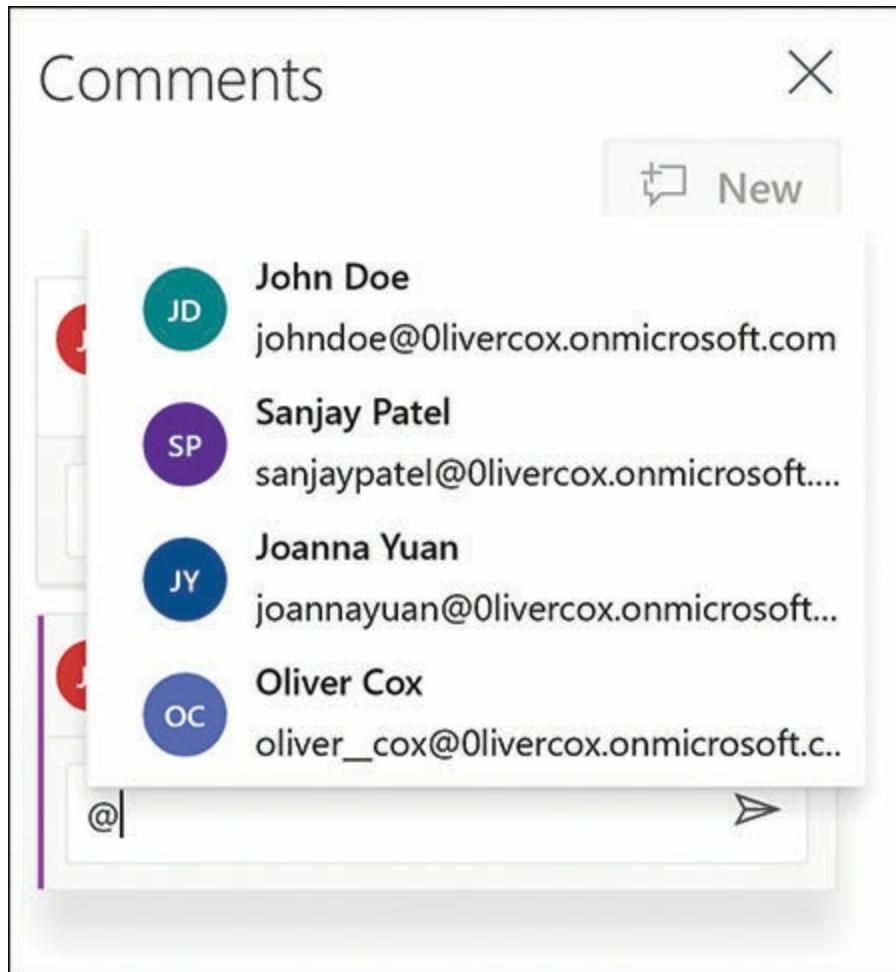
**FIGURA 2-36** Arquitectura lógica para equipos de Microsoft y servicios relacionados.

## Microsoft Graph

Por lo tanto, la colaboración en Microsoft 365 puede ser una cuestión de servicios basados en la nube que proporcionan contenido entre sí, integrando las funciones de múltiples servicios en una sola interfaz. Sin embargo, hay más en la colaboración de Microsoft 365 que simplemente colocar contenido Stream junto al contenido de SharePoint Online en una ventana de equipos. Microsoft Graph es una API de desarrollador que permite a las aplicaciones de Office 365 hacer sugerencias inteligentes sobre cómo los usuarios pueden aprovechar el contenido disponible para ellos.

Por ejemplo, al editar un documento de Word almacenado en un sitio de grupo de SharePoint, un usuario puede usar *@ menciona* para comunicarse con otros miembros del equipo. Al presionar la tecla @ en un comentario, aparece una lista de miembros del equipo, como se muestra en Figura 2-37 . Después de seleccionar un usuario de la lista y escribir un mensaje, presione el **Enviar**

El botón genera un correo electrónico que contiene el mensaje para el usuario seleccionado.



**FIGURA 2-37** Una lista de inserción @mention

Otra función de la capacidad @mention es que los usuarios inserten notas para sí mismos seleccionando **Que hacer** de la lista. Graph interpreta el contenido de la nota y, por ejemplo, si hay referencias a otros documentos en la biblioteca de SharePoint, muestra un **Insertar desde archivo** panel que contiene archivos sugeridos.

Microsoft Graph también puede evaluar los datos en un documento y sugerir posibles acciones. Por ejemplo, en

una hoja de cálculo de Excel que contiene una lista de países, haciendo clic en el **Geografía** botón en el **Datos** La pestaña agrega un ícono de información a cada celda. Al hacer clic en el ícono en una celda, se muestra información sobre el país que se encuentra en Internet, como se muestra en Figura 2-38 .

The screenshot shows an Excel spreadsheet with a list of countries in column A. Row 3 is selected, highlighting 'Burkina Faso'. A tooltip has appeared over the cell containing 'Burkina Faso', displaying detailed information about the country. The tooltip includes:

- Burkina Faso
- Capital: Ouagadougou
- Leader(s): Roch Marc Christian Kaboré (President), Christophe Joseph Marie Dabiré (Prime Minister)
- Population · 2017: 19,193,382
- Area · square km: (00)
- Powered by Bing

The tooltip also features a small image of the flag of Burkina Faso (red top half with a yellow star, green bottom half) and a link to 'Wikipedia · Public domain.' with a small icon.

**FIGURA 2-38** Información del país de Internet que se muestra en Excel

Seleccionando la lista de países y haciendo clic en el **Insertar datos** El botón muestra una lista de propiedades estadísticas, como se muestra en Figura 2-39 . Seleccionar una de las propiedades, como **Población**, inserta el dato apropiado para cada país en la celda adyacente.

	A	B	C
1			
2	United States		
3	Burkina Faso		
4	Myanmar		
5	Thailand		
6	France		
7	United Kingdom		
8		Out of pocket health expendit...	
9		Physicians per thousand	
10		Population	
11		Population: Income share four...	
		Population: Income share hig...	
		Population: Income share hig...	
		Population: Income share low...	
		Population: Income share low...	
		Population: Income share sec...	
		Population: Income share thir...	
		Population: Labor force partic...	
		Subdivisions	
		Tax revenue (%)	
		Time zone(s)	
		Total tax rate	

FIGURA 2-39 Insertar opciones de datos para seleccionados

países en Excel

Seleccionar el recién agregado **Población** figuras y haciendo clic en el **Análisis rápido** El botón muestra el menú de opciones que se muestra en Figura 2-40. , que le permite seleccionar opciones de formato y agregar tipos de gráficos y totales a la hoja de cálculo.

	A	B	C	D	E
1					
2	Burkina Faso	19,193,382			
3	Burkina Faso	19,193,382			
4	Myanmar	53,370,609			
5	Thailand	69,037,513			
6	France	67,118,648			
7	United Kingdom	66,022,273			
8					
9					
10					
11					
Ready					

The screenshot shows a Microsoft Excel spreadsheet with data in columns A and B. Row 2 contains the value '19,193,382' in cell B2, which is highlighted with a green selection bar. A context menu is open over this cell, titled 'Formatting'. The 'Formatting' tab is selected, showing several options: Data Bars, Color Scale, Icon Set, Greater Than, Top 10%, and Clear Format. Below the tabs, a note says 'Conditional Formatting uses rules to highlight interesting data.' The rest of the spreadsheet shows other country names and their population counts.

**FIGURA 2-40** Opciones de análisis rápido para datos de Excel

Los administradores y desarrolladores de Microsoft 365 también pueden mejorar los procesos de colaboración al usar Microsoft Flow para automatizar los flujos de trabajo que incorporan Graph

funciones y otros servicios. Por ejemplo, cuando los usuarios descubren un dispositivo que no funciona correctamente, pueden enviar una fotografía del mismo a un buzón asociado con un flujo. El flujo puede usar Graph para identificar el dispositivo en la fotografía, buscar un reemplazo en un inventario y generar una orden de envío que envíe la parte al usuario que informó el problema. El mismo tipo de proceso puede automatizar los servicios de soporte técnico, generar oportunidades de ventas basadas en la presencia de Internet de los usuarios y realizar cualquier cantidad de otras tareas sin intervención del usuario.

## Movilidad empresarial

Como se señaló anteriormente en este capítulo, el lugar de trabajo moderno ya no está restringido a una sola oficina, edificio o ciudad, e incluso si lo fuera, los trabajadores típicos tienen múltiples dispositivos que esperan usar para acceder a los recursos empresariales. . La movilidad se ha convertido en un elemento crítico de la administración moderna, y Microsoft 365 incluye las herramientas necesarias para permitir a los usuarios con teléfonos inteligentes, tabletas, computadoras portátiles y computadoras domésticas acceder a los archivos, aplicaciones y servicios empresariales que necesitan.

El primer obstáculo para la movilidad es el acceso a los datos, pero afortunadamente, Microsoft 365 permite a los usuarios, aplicaciones y servicios almacenar sus datos en la nube, por lo tanto

poniéndolo a disposición de cualquier dispositivo que tenga conexión a Internet. Es por esta razón que todos los usuarios de Microsoft 365 reciben almacenamiento en la nube de OneDrive para la Empresa y SharePoint Online también usa el almacenamiento en la nube.

El segundo problema es el acceso a las diversas aplicaciones y servicios de Microsoft 365. El producto tradicional de Office requería que los usuarios instalaran las aplicaciones de productividad, como Word, Excel y PowerPoint, en una computadora de escritorio o portátil. Los servicios de fondo, como Exchange y SharePoint, tuvieron que instalarse en servidores locales. Los usuarios en el sitio podían acceder a sus sitios de correo electrónico y SharePoint, pero para los usuarios que viajaban o trabajaban desde casa, se necesitaban arreglos especiales, como acceso remoto o conexiones de red privada virtual.

Con Microsoft 365, los usuarios todavía tienen la capacidad de instalar las aplicaciones de Office en sus computadoras, pero el producto también incluye las aplicaciones de Office en la web, que permiten a los usuarios trabajar en línea con documentos de Word, Excel y PowerPoint, utilizando cualquier dispositivo con navegador web y acceso a internet. Todos los servicios de back-end de Microsoft 365 están instalados en la nube, lo que proporciona a los usuarios acceso a su correo electrónico y otros servicios sin una conexión especial al centro de datos de la empresa. Aquí nuevamente, solo se necesita una conexión a Internet.

Además de la productividad tradicional de Office

aplicaciones, nuevos clientes como los de Teams y Yammer también están disponibles como aplicaciones basadas en la Web, que no requieren preparación especial. Microsoft 365 también incluye clientes de escritorio descargables para muchas de sus aplicaciones, disponibles en versiones para todas las principales plataformas móviles, incluidas Android, iOS, MacOS y Windows.

El tercer problema de movilidad, posiblemente el más crítico, se refiere a los dispositivos móviles. En los primeros días de la conectividad celular, las organizaciones proporcionaban a sus usuarios dispositivos móviles. Los dispositivos tenían capacidades relativamente limitadas, y los administradores retuvieron el control total sobre ellos.

Sin embargo, la cultura móvil actual es radicalmente diferente, ya que los teléfonos inteligentes se han vuelto omnipresentes y funcionan tanto como un símbolo de estado personal como una herramienta de trabajo. Algunas organizaciones sí proporcionan dispositivos móviles, pero los administradores ahora también deben acomodar a los trabajadores que desean utilizar sus dispositivos personales para acceder a los recursos empresariales, lo que plantea problemas complejos de seguridad y soporte.

Fue tarea de Microsoft desarrollar clientes que los trabajadores móviles puedan usar para acceder a sus datos, aplicaciones y servicios empresariales. Sin embargo, proporcionar dispositivos móviles con acceso de cliente es solo la mitad de la imagen. La otra mitad es garantizar que los recursos empresariales sensibles estén protegidos contra pérdidas, robos y ataques. Microsoft

proporciona herramientas que hacen esto posible, pero corresponde a los administradores de la empresa implementarlas de manera adecuada tanto para las necesidades de usabilidad del trabajador como para la sensibilidad de los datos.

## Movilidad empresarial + seguridad

El componente de Microsoft 365 relacionado con la administración de dispositivos móviles y su protección es Enterprise Mobility + Security (EMS). Las herramientas principales que componen EMS y las funciones que proporcionan para dispositivos móviles son las siguientes:

- **Azure Active Directory** Contiene las cuentas que proporcionan a los usuarios la capacidad de inicio de sesión único para todas las aplicaciones y servicios de Microsoft 365. Los administradores pueden configurar cuentas de usuario para requerir autenticación multifactor para mejorar la seguridad de los dispositivos móviles.
- **Microsoft Intune** Inscribe dispositivos móviles y los asocia con usuarios o grupos particulares, como se muestra en Figura 2-41 . Al usar Intune, los administradores pueden especificar si se debe usar la Administración de dispositivos móviles (MDM) o la Administración de aplicaciones móviles (MAM), especificar políticas de cumplimiento de dispositivos y crear políticas de configuración de dispositivos.
- **Protección de la información de Azure** Proporciona seguridad a nivel de documento mediante la aplicación de etiquetas que clasifican la sensibilidad de los archivos de información que contienen y la aplicación de protección a documentos específicos, en forma de cifrado, restricciones de usuario y otros medios.
- **Análisis avanzado de amenazas de Microsoft** Recopila información de muchas fuentes empresariales de Microsoft 365 y la analiza para anticipar, detectar y reaccionar ante ataques y otras amenazas de seguridad.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and a navigation bar with icons for Home, Microsoft Intune, Devices, and other account-related options. The main content area is titled 'Devices' under 'Microsoft Intune'. On the left, a sidebar menu includes 'Overview', 'Manage', 'All devices', 'Azure AD devices', 'Monitor', 'Device actions', 'Audit logs', 'Setup', 'TeamViewer Connector', and 'Device cleanup rules'. The main panel displays tenant information: Tenant name (Olivercox.onmicrosoft.com), MDM authority (Microsoft Intune), Tenant location (North America 0402), and Account status (Active). Below this, two sections are shown: 'Intune enrolled devices' (LAST UPDATED 7/20/2019, 8:17:08 PM) and 'Enrolled devices' (LAST UPDATED 7/20/2019, 8:17:08 PM). The 'Intune enrolled devices' section lists platform counts: Android (1), iOS (0), macOS (0), and Windows (0). The 'Enrolled devices' section shows a count of 1 device.

**FIGURA 2-41** La página de dispositivos de Microsoft Intune

*Nota:*

## Trabajando con

### Microsoft Intune

El portal de Microsoft Intune, a diferencia de la mayoría de las herramientas administrativas para Microsoft 365, no es accesible desde el Centro de administración de Microsoft 365. En cambio, los administradores deben iniciar sesión en el portal de Microsoft Azure y seleccionar Microsoft Intune de la lista Todos los servicios.

## Microsoft Intune

Microsoft Intune es la herramienta que los administradores usan para

permitir la inscripción de dispositivos personales de los usuarios en Microsoft 365 y regular sus capacidades. Mobile Device Management (MDM) permite a los administradores tomar un control casi completo sobre los dispositivos inscritos, incluso hasta el punto de emitir comandos remotos que borran todos los datos de la compañía en el dispositivo.

Para los usuarios a los que no les gusta la idea de que la organización ejerza ese tipo de control sobre su propiedad personal, Mobile Application Management (MAM) proporciona dispositivos solo con aplicaciones administradas, dejando el resto del dispositivo sin restricciones. Las opciones que elijan los administradores deben depender de la sensibilidad de los datos que podrían almacenarse en el dispositivo y de los términos de cumplimiento de seguridad que la organización debe cumplir.

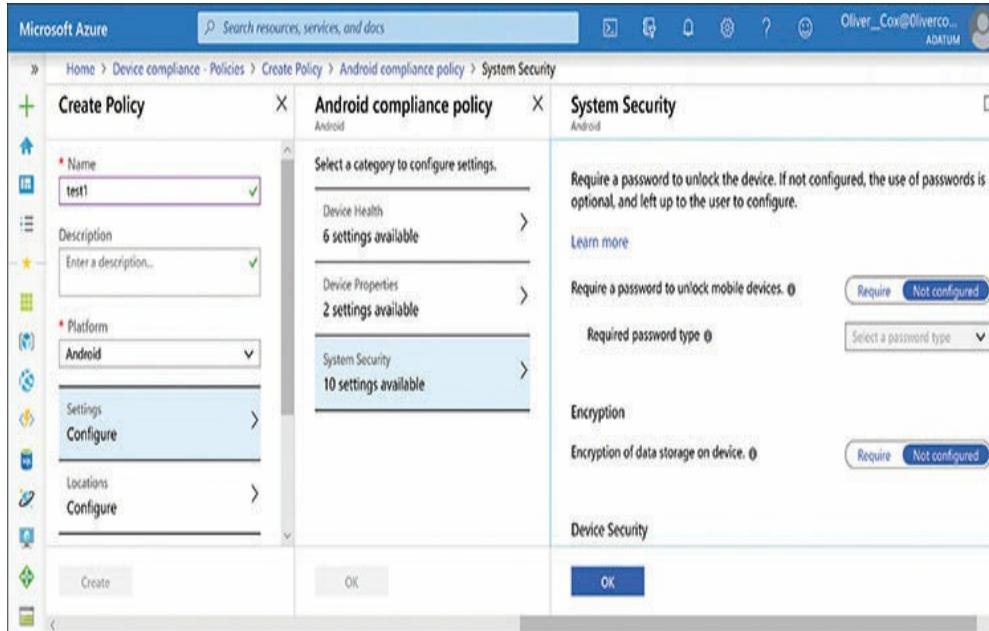
**Nota:**

### **MDM y MAM**

**Para obtener más información sobre la administración de dispositivos móviles y la administración de aplicaciones móviles, consulte la Fase 4 de " Comprender el modelo de implementación y lanzamiento de Microsoft ", Anteriormente en este capítulo.**

Las políticas de cumplimiento de dispositivos son reglas que especifican cómo se debe configurar un dispositivo para acceder a los servicios de Microsoft 365. Por ejemplo, una política puede requerir que los dispositivos móviles tengan una contraseña de desbloqueo, en lugar de un simple deslizamiento, como se muestra en Figura 2-42 , esos datos

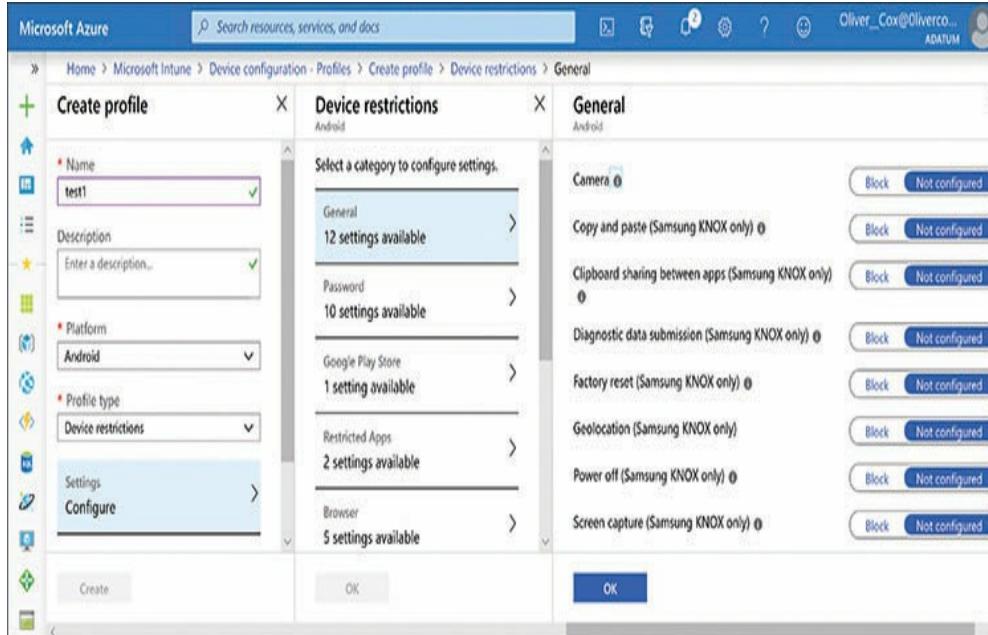
almacenarse en el dispositivo en forma cifrada y que el sistema operativo del dispositivo móvil se actualice a un nivel específico. Un dispositivo que no cumple con la configuración de la política de cumplimiento no se puede inscribir, e incluso cuando se inscribe con éxito, se debe verificar el cumplimiento a intervalos regulares para mantener su acceso a los servicios en la nube de Microsoft 365.



**FIGURA 2-42** Perfiles de cumplimiento de dispositivos en Microsoft Intune

Por lo general, proteger los datos empresariales en dispositivos móviles es una cuestión de restringir lo que el usuario del dispositivo puede hacer. En algunos casos, los administradores pueden querer evitar que los usuarios pongan en peligro los datos confidenciales. Otro problema de seguridad es la posibilidad de robo o destrucción de datos cuando un dispositivo móvil se pierde o es robado.

Los administradores pueden controlar las capacidades de los dispositivos móviles creando perfiles de configuración de dispositivos en Microsoft Intune para las diversas plataformas y habilitando o deshabilitando las funciones del dispositivo, como se muestra en Figura 2-43 .



**FIGURA 2-43** Perfiles de configuración de dispositivos en Microsoft Intune

Los administradores pueden especificar además qué aplicaciones se les permite ejecutar a los dispositivos móviles y también bloquearlos explícitamente para que no ejecuten ciertas aplicaciones. Claramente, la movilidad no es solo una cuestión de permitir que los dispositivos se conecten a un dominio de Microsoft 365; sus capacidades también deben ser restringidas.

## HABILIDAD 2.6: DESCRIBA EL ANÁLISIS

# CAPACIDADES EN MICROSOFT 365

---

Como se mencionó en otra parte, Microsoft 365 no es solo un paquete de aplicaciones y servicios. El producto incluye una variedad de herramientas analíticas que recopilan información de componentes en todo el entorno de Microsoft 365. Estas herramientas, llamadas análisis, pueden detectar violaciones de seguridad existentes y potenciales, rastrear el uso de las aplicaciones de Office 365 e incluso examinar los patrones de producción y colaboración de usuarios y grupos.

## Análisis avanzado de amenazas de Microsoft

*Microsoft Advanced Threat Analytics (ATA)* es un servicio local que recopila tráfico de los controladores de dominio de Active Directory y los registros de eventos y utiliza una inspección profunda de paquetes para detectar actividades sospechosas en la red y generar informes como el que se muestra en Figura 2-44. . Se incluye una licencia para Microsoft ATA como parte del paquete Enterprise Mobility + Security en Microsoft 365.



**FIGURA 2-44** Un informe de Microsoft Advanced Threat Analysis de un ataque de pasar el ticket

Algunos de los tipos de ataque conocidos que ATA puede detectar del tráfico capturado incluyen los siguientes:

- **Pase el boleto (PtT)** Este es un intento de utilizar un ticket de concesión de tickets Kerberos en múltiples sistemas para solicitar tickets de servicio Kerberos que brinden acceso a otros recursos.
- **Pass-the-Hash (PtH)** Este es un intento de omitir el proceso de autenticación NTLM al proporcionar un hash de contraseña capturado en lugar de una contraseña de texto sin cifrar.
- **Overpass-the-Hash** Esta es una variante del ataque Pass-the-Hash

se usa para penetrar la autenticación Kerberos, en la que el intruso intenta sustituir una clave en lugar de un hash.

- **PAC forjado** Este es un intento de penetrar una autenticación Kerberos utilizando un Certificado de Atributo Privilegiado (PAC) no autorizado.
- **Boleto dorado** Este es un intento de obtener acceso sin restricciones a todo un dominio de Active Directory tomando el control de su Servicio de distribución de claves (KDS).
- **Replicaciones maliciosas** Este es un intento de desencadenar un proceso de replicación de Active Directory por una computadora que no es un controlador de dominio.
- **Reconocimiento** Este es un intento de descubrir cuentas de usuario en un dominio de Active Directory mediante consultas DNS, SAM-R o Kerberos.
- **Fuerza bruta** Este es un ataque que intenta penetrar en un sistema mediante intentos repetidos de autenticación hasta que se descubren las credenciales correctas.
- **Ejecución remota** Este es un intento de usar credenciales comprometidas para ejecutar comandos remotos en un controlador de dominio.

ATA basa su análisis en las fases típicas de la infiltración de un atacante en la red e intenta detectar las actividades que se utilizan comúnmente durante estas fases. Al comprender los tipos de información que los atacantes intentan reunir durante las fases iniciales de una infiltración, ATA a menudo puede detectar un ataque mientras es inminente y antes de que la pérdida de datos real u otro daño esté en marcha. Las fases son las siguientes:

- **Reconocimiento** Esta es la fase en la que los atacantes recopilan información sobre la infraestructura de red, como los nombres de cuenta y las direcciones IP

- **Movimiento lateral** Esta es la fase en la que los atacantes intentan usar el conocimiento reunido durante la fase de reconocimiento para ampliar la superficie de ataque a otros recursos y otras computadoras
- **Persistencia** Esta es la fase en la que los atacantes capturan información adicional que les permitirá continuar el ataque después de la detección inicial, utilizando otros puntos de entrada y credenciales de usuario

Si bien ATA es capaz de detectar de manera determinista las amenazas conocidas, también puede informar sobre actividades sospechosas que no se ajustan a ninguna firma de amenaza conocida, pero que, sin embargo, parecen ser peligrosas, utilizando una técnica llamada Aprendizaje automático de comportamiento anormal.

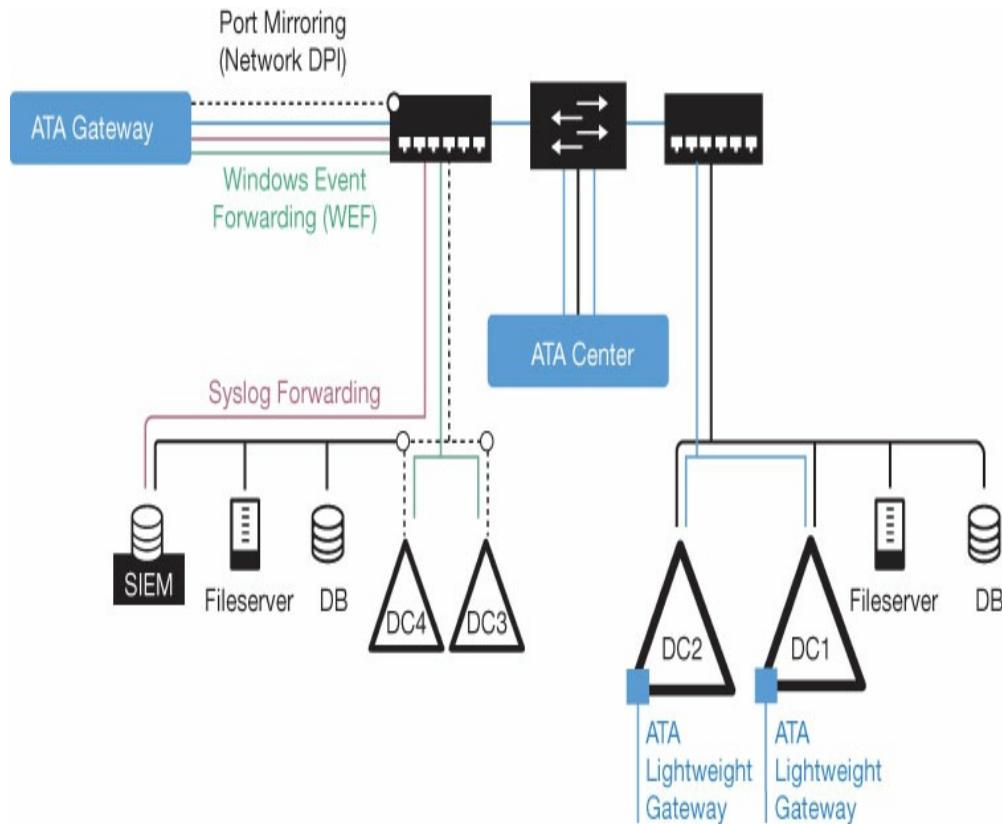
Algunos de los tipos de comportamiento anormal y ejemplos típicos de ellos son los siguientes:

- **Inicios de sesión anómalos** Tráfico de autenticación para una cuenta específica en computadoras donde la cuenta nunca se ha usado antes
- **Compartir contraseña** Autenticaciones múltiples en diferentes computadoras casi al mismo tiempo o en ubicaciones remotas
- **Movimiento lateral** Patrones de autenticación similares descubiertos en varias computadoras
- **Modificación grupal** Adiciones inusuales o frecuentes de usuarios a grupos sensibles, como aquellos con permisos administrativos

Para que ATA funcione de manera efectiva, debe capturar el tráfico de autenticación de los controladores de dominio de los Servicios de dominio de Active Directory locales. Para hacer esto, se requiere una puerta de enlace ATA, que es un servicio que utiliza un procedimiento llamado duplicación de puertos para duplicar el tráfico que se ejecuta hacia y desde los controladores de dominio de la red, como se muestra en Figura 2-45 . Se envía una copia del tráfico.

---

al Centro ATA para su análisis, mientras que la otra copia viaja a su destino original. Como alternativa, los administradores pueden instalar ATA Lightweight Gateway en los controladores de dominio.



**FIGURA 2-45** La arquitectura de Microsoft Advanced Threat Analytics

Antes de instalar ATA Center o cualquier ATA Gateways, los administradores deben descargar y ejecutar la Herramienta de dimensionamiento de ATA. Esta es una herramienta que mide los niveles de tráfico de la red contando la cantidad de paquetes. Después de funcionar durante 24 horas, la herramienta genera un

hoja de cálculo como la que se muestra en Figura 2-46 . Al hacer coincidir los valores de la hoja de cálculo con una tabla publicada, los administradores pueden determinar qué configuración de hardware se necesita para las computadoras ATA Center y ATA Gateway o ATA Lightweight Gateway.

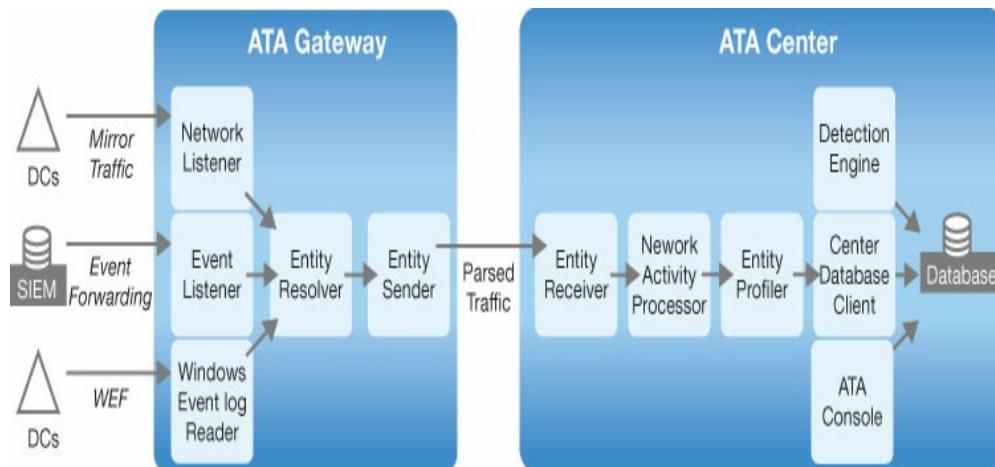
Number of DCs	4			
Number of Samples	69			
Overall Start Time UTC	2016-07-21 10:41:54			
Overall End Time UTC	2016-07-21 10:43:09			
Display DC Times as UTC/Local	Universal Time (UTC)			
Center	Max Packets/sec	Avg Packets/sec	Busy Packets/sec	Busy Packets/sec Start UTC
Grand Total	1,616	1,184	1,184	10:41:55
DC	Max Packets/sec	Avg Packets/sec	Busy Packets/sec	Busy Packets/sec Start Time
DC1	644	457	457	10:41:54
DC3	334	234	234	10:41:54
DC4	408	249	249	10:41:54
DC2	405	244	244	10:41:54
Total	1,792	1,184	1,184	10:43:08

**FIGURA 2-46** Salida de hoja de cálculo de la herramienta de dimensionamiento ATA

Una vez que las computadoras con el hardware apropiado están disponibles, los administradores pueden instalar el Centro ATA, conectarlo a Active Directory y luego instalar y configurar la Puerta de enlace ATA o la Puerta de enlace ligera ATA. Además del tráfico de Active Directory, ATA puede utilizar información de eventos de otros sistemas, que se recopila mediante el reenvío de eventos de Windows y se envía a la puerta de enlace.

Con los componentes en su lugar, la información del flujo procede como se muestra en Figura 2-47 . Controlador de dominio

el tráfico y los eventos de Windows se resuelven en la puerta de enlace de ATA y se transmiten al Centro de ATA, donde se analizan y almacenan en una base de datos MongoDB.

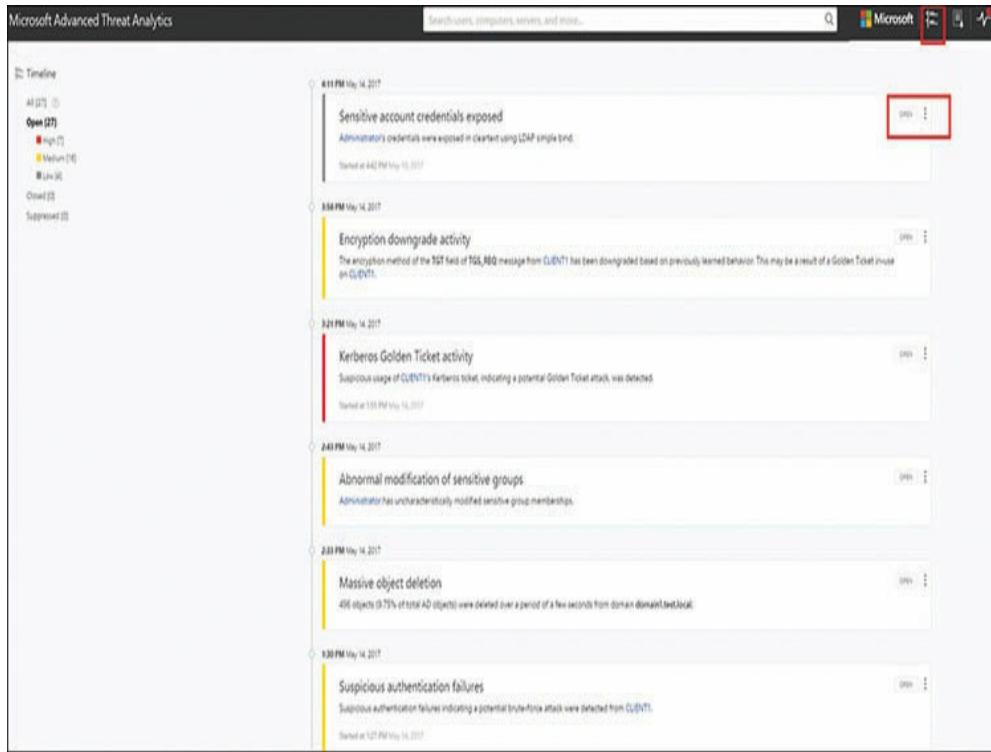


**FIGURA 2-47** Flujo de información de Microsoft Advanced Threat Analytics

A medida que ATA recopila información, utiliza algoritmos de comportamiento para establecer una línea de base de uso para cuentas y computadoras específicas. Una vez que la línea de base está en su lugar, una explosión repentina de actividad que difiere sustancialmente de la norma se considera anómala y sospechosa. Es posible que la actividad no esté asociada con el patrón conocido de un tipo de ataque específico, pero el hecho de que esté fuera de lo común es suficiente para que ATA lo señale como un signo de un posible ataque.

La computadora ATA Center también proporciona a los administradores acceso a la Consola ATA, como se muestra en Figura 2-48. , que muestra el más reciente \_\_\_\_\_.

actividades que ATA ha clasificado como sospechosas. Los administradores también pueden configurar ATA para avisarles de actividades sospechosas generando notificaciones del sistema, correos electrónicos o entradas de registro.



**FIGURA 2-48** La consola de Microsoft Advanced Threat Analytics

## Análisis de uso de Microsoft 365

La página Informes / Uso en el Centro de administración de Microsoft 365 puede mostrar información sobre los niveles de actividad en los diversos servicios de Microsoft 365 en forma de gráfico, como se muestra en Figura 2-49 . Los administradores pueden modificar los gráficos para mostrar 7, 30, 90 o 180 días de información. Microsoft

365 Usage Analytics es un servicio dentro de la herramienta de análisis empresarial de Power BI para rastrear cómo los trabajadores están utilizando los diversos componentes de Microsoft 365 durante los 12 meses anteriores con mucho más detalle.



**FIGURA 2-49** Un gráfico de uso del servicio en el Centro de administración de Microsoft

365

Los administradores pueden usar el servicio basado en Power BI para determinar qué herramientas están usando los trabajadores para realizar tipos específicos de tareas, qué componentes de Microsoft 365 se usan en exceso o qué no, y que rara vez se adoptan. Este tipo de información puede permitir a los administradores determinar si los trabajadores pueden necesitar capacitación para hacer un mejor uso de herramientas específicas que

están disponibles para ellos.

Por ejemplo, puede haber usuarios que se quejan de que les resulta difícil comunicarse a nivel de toda la empresa, porque generalmente pasan la mayor parte del tiempo con los miembros de su equipo inmediato. Es posible que estos usuarios no sepan que Yammer existe o no sepan cómo usarlo. Un breve tutorial podría resolver el problema de estos usuarios, así como aumentar la comunicación cruzada en toda la empresa.

Para usar Microsoft 365 Usage Analytics, un administrador debe abrir el Centro de administración de Microsoft 365, ir a la página Informes / Uso y, en la tarjeta Microsoft 365 Usage Analytics, que se muestra en Figura 250 haga clic **Empezar** para instanciar el proceso de recopilación de datos, que puede demorar hasta 48 horas.



## Microsoft 365 usage analytics

Get the most from your subscription.  
Analyze and explore usage data in  
Power BI.

Get started to opt in to Microsoft 365  
usage analytics.

[Get started](#)

**FIGURA 2-50** La tarjeta Microsoft 365 Usage Analytics en el Centro de administración de Microsoft 365

Cuando se completa el proceso de recopilación de datos, el administrador puede agregar el servicio Microsoft 365 Usage Analytics a la aplicación Power BI, autenticar la tenencia de la empresa y generar un tablero de datos basado en gráficos, como se muestra en Figura 2-51 .



**FIGURA 2-51** El panel de Microsoft 365 Usage Analytics

Al hacer clic en gráficos individuales, los administradores pueden ver información más detallada sobre factores de uso específicos, que incluyen lo siguiente:

- **Activación de oficina** Especifica el número y los tipos de dispositivos en los que los usuarios han instalado sus cinco copias de Office 365, según lo permitido por su licencia.
  
- **Adopción** Especifica cuántas licencias de Office 365 se han asignado a los usuarios cada mes, cuántas están realmente en uso y cuántas personas usan Office 365 por primera vez

- **Colaboración** Indica con qué frecuencia los usuarios colaboran accediendo a los documentos de otros usuarios almacenados en las bibliotecas de SharePoint Online o en OneDrive para la Empresa
- **Comunicación** Especifica qué herramientas de Microsoft 365 los trabajadores prefieren usar para comunicarse entre sí en la empresa, como el correo electrónico de Exchange, Teams, Yammer o Skype
- **Uso del producto** Rastrea el uso de actividades específicas dentro de cada servicio de Microsoft 365
- **Uso de almacenamiento** Rastrea el almacenamiento en la nube por usuario para sitios de SharePoint, OneDrive para empresas y buzones de Exchange
- **Acceso desde cualquier lugar** Especifica qué clientes y dispositivos utilizan los trabajadores para conectarse a correo electrónico, equipos, Yammer o Skype
- **Uso individual del servicio** Proporciona informes de actividad para servicios individuales de Microsoft 365, incluidos Exchange, Teams y Yammer.

Power BI también es personalizable, lo que permite a los administradores crear sus propios informes e incluso agregar sus propias fuentes de datos adicionales.

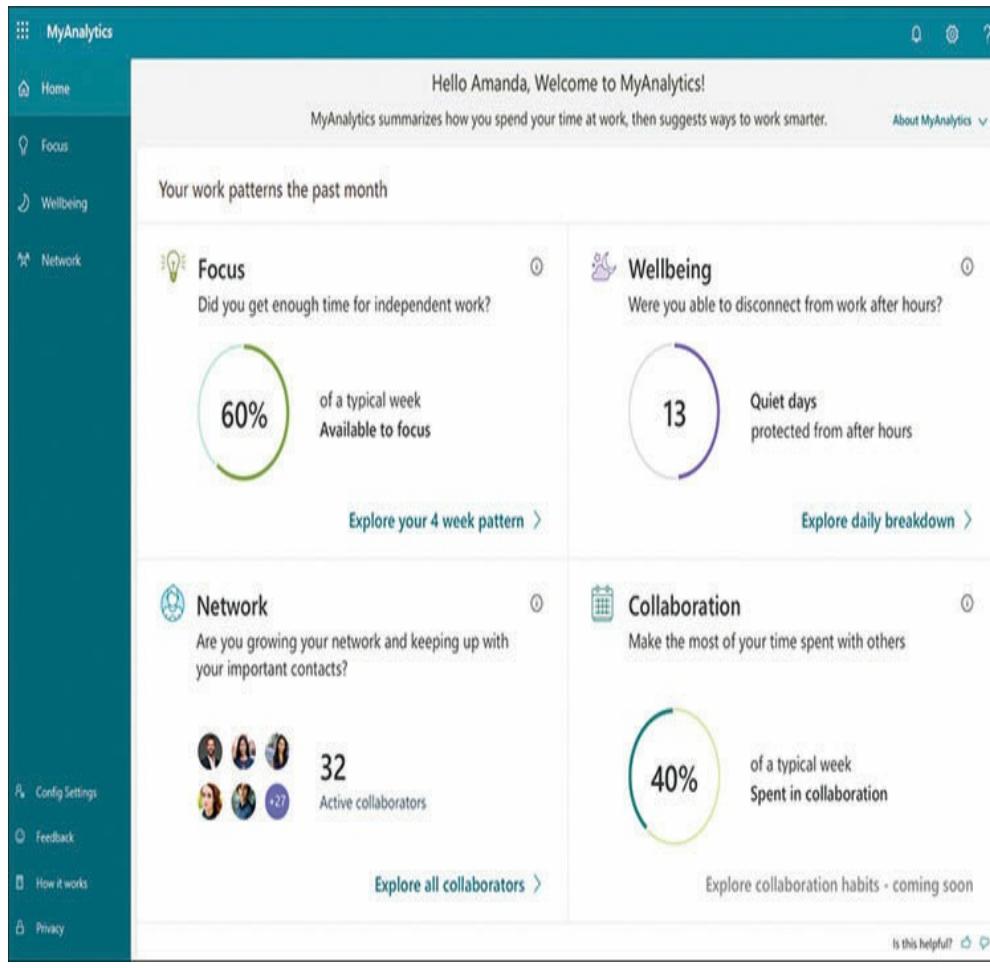
## MyAnalytics

Conocido por Microsoft como "el rastreador de actividad física para el trabajo", MyAnalytics es una herramienta de mantenimiento de registros de productividad personal que permite a los usuarios revisar cómo pasan su tiempo de trabajo y con quién lo pasan. Disponible para todos los usuarios de Office 365, MyAnalytics consiste en un panel que está disponible en la lista de aplicaciones de Office 365 y un complemento para Microsoft Outlook que muestra información de MyAnalytics como un panel separado en la interfaz estándar de Outlook.

MyAnalytics recopila información de los calendarios y buzones de Exchange Online de un usuario, chat de equipos e historial de llamadas, actividades de Skype for Business y, opcionalmente, actividades de aplicaciones de Windows 10. La información se almacena en el almacén de buzones de Exchange de cada usuario. Al compilar la información y mostrarla en una serie de gráficos, MyAnalytics intenta asesorar a los usuarios sobre qué tan bien están manejando su productividad y su tiempo libre.

El panel de MyAnalytics, que se muestra en Figura 2-52 , consta de cuatro paneles, como sigue:

- **Atención** Compara la cantidad de tiempo de trabajo que le queda al usuario para concentrarse en el esfuerzo individual, en comparación con el tiempo de trabajo dedicado a colaborar con los miembros del equipo. Basado en estos tiempos relativos, MyAnalytics puede ayudar al usuario a reservar una o dos horas por día para un trabajo individual enfocado y suprimir las comunicaciones entrantes durante esas horas.



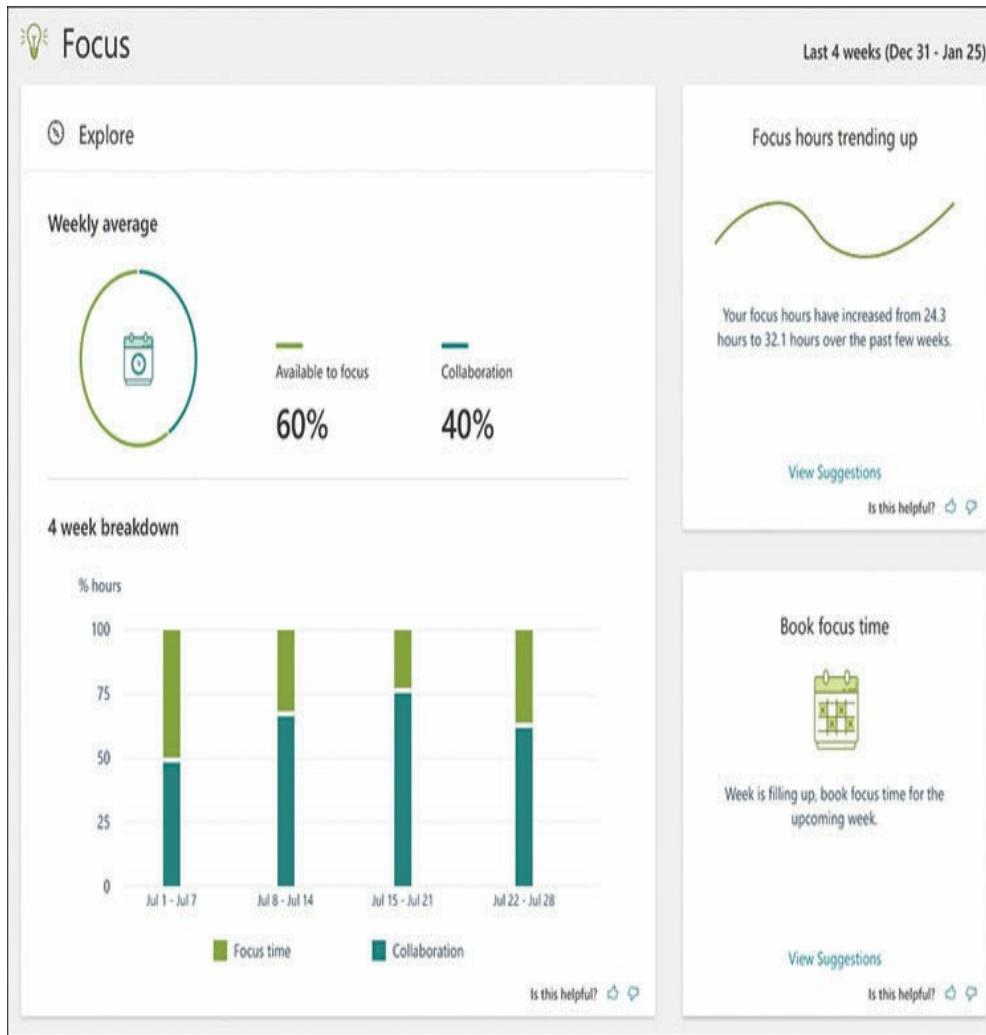
**FIGURA 2-52** El panel de MyAnalytics

- **Bienestar** Según los datos de calendario de Exchange y las actividades de comunicación, MyAnalytics analiza el tiempo del usuario fuera de las horas normales de trabajo y rastrea el tiempo dedicado a las actividades relacionadas con el trabajo. Los días en los que el usuario pasa menos de dos horas de tiempo libre en actividades laborales se designan como días tranquilos. Cuando un usuario no tiene suficientes días tranquilos, MyAnalytics hace recomendaciones para mejorar la calidad del tiempo libre del usuario.
- **Red** Basado en reuniones programadas, chats, llamadas y correos electrónicos, MyAnalytics rastrea la cantidad de tiempo que el usuario pasa con sus compañeros de trabajo y miembros del equipo más cercanos durante el mes anterior. Según los datos recopilados, MyAnalytics puede hacer

sugerencias para mejorar la comunicación del usuario con las personas designadas como importantes, como recomendaciones para programar reuniones adicionales y recordatorios para responder a llamadas y correos electrónicos.

- **Colaboración** Evalúa el tiempo del usuario dedicado en colaboración con los miembros del equipo, en comparación con el tiempo dedicado a otras actividades. Según los resultados, MyAnalytics podría recomendar que un usuario pase menos tiempo respondiendo correos electrónicos y llamadas telefónicas y más tiempo trabajando con colegas cercanos.

También hay páginas separadas para los paneles, en las que MyAnalytics muestra información y sugerencias más detalladas, como se muestra en Figura 2-53 .



**FIGURA 2-53** La página de enfoque de la herramienta MyAnalytics

MyAnalytics está diseñado para ser una herramienta personal de mejora personal para usuarios individuales. No está destinado a ser utilizado por los empleadores para monitorear o rastrear la productividad de los trabajadores, ni proporciona a los usuarios información personal sobre sus compañeros de trabajo.

## Analítica del lugar de trabajo

Workplace Analytics es similar a MyAnalytics, excepto que recopila información para toda la empresa en lugar de solo una persona. Al igual que MyAnalytics, la motivación principal para Workplace Analytics es proporcionar a la gerencia una idea de cómo los trabajadores pasan su tiempo y con quién lo pasan.

Workplace Analytics comienza con las mismas fuentes que MyAnalytics, como el correo electrónico de Exchange y los datos de calendario y el chat de Teams y el historial de llamadas. Sin embargo, los administradores también pueden incorporar información adicional en el análisis, como los datos de recursos humanos sobre los empleados, incluidos los títulos de trabajo, los niveles de gestión y las ubicaciones geográficas. Con esta información, el análisis puede calcular factores que no son realizables solo con los datos del servicio.

Basado en este análisis, Workplace Analytics genera métricas en las siguientes áreas:

- **Semana en la vida** Calcula el número promedio de horas que los empleados dedican a la colaboración en una semana seleccionada. El tiempo de colaboración se divide en horas dedicadas a reuniones y horas respondiendo correos electrónicos.
- **Gestión y coaching** Calcula el tiempo promedio que los empleados pasan en reuniones con su gerente presente, especificando también cuántas horas pasan en reuniones individuales con los gerentes.
- **Redes internas** Especifica el tamaño de la red y la amplitud de la red de colaboración de los empleados. El tamaño de la red es la cantidad de personas con las que colaboran los empleados en reuniones o correos electrónicos, mientras que la amplitud de la red es la cantidad de diferentes departamentos o divisiones con los que colaboran los empleados.

- **Colaboración de equipos** Calcula el uso que hacen los empleados de la comunicación de Microsoft Teams, incluida la cantidad de llamadas y mensajes de chat, así como la cantidad de tiempo que pasan en llamadas y sesiones de chat.
- **Colaboración externa** Calcula varias estadísticas que cuantifican la colaboración de los trabajadores con personas externas a la empresa, como el porcentaje de empleados que participan en colaboración externa y el porcentaje de su tiempo que pasan en colaboración externa.
- **Resumen de reuniones** Cuantifica la cantidad de tiempo que los empleados pasan en las reuniones y especifica la naturaleza de las reuniones en las que participan.

Como ejemplo de las capacidades analíticas de la herramienta, la página de resumen de Reuniones puede usar la información del calendario de Exchange para calcular cuánto tiempo pasan los trabajadores en las reuniones, como se muestra en Figura 2-54 ;

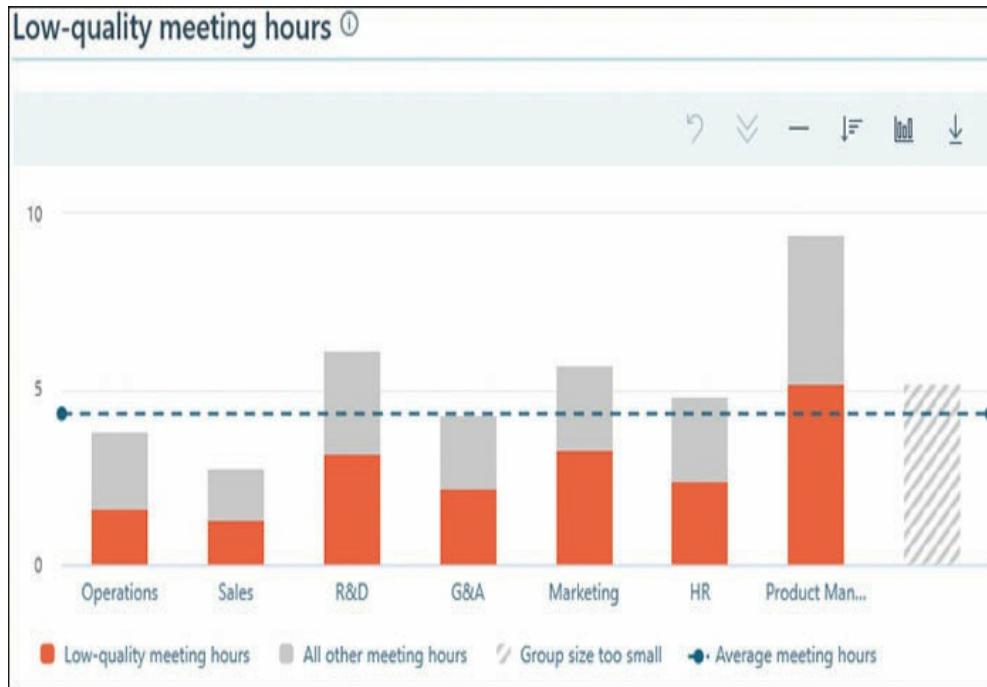
Además, las reuniones pueden cuantificar las reuniones de diferentes duraciones. Sin embargo, Workplace Analytics también puede usar las ubicaciones geográficas de los trabajadores (a partir de la información de Recursos Humanos) para determinar cuánto tiempo de viaje pasan para llegar a las reuniones.



**FIGURA 2-54** Gráfico de análisis del lugar de trabajo del tiempo dedicado a las reuniones

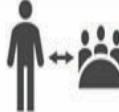
El análisis también puede identificar cuánto del total de la reunión consiste en tiempo de baja calidad, como se muestra en

**Figura 2-55**, se define como las horas de reunión durante las cuales un trabajador desempeña un papel redundante, está programado para asistir a otra reunión al mismo tiempo o realiza varias tareas al responder un correo electrónico en la reunión. Workplace Analytics puede explicar la importancia de estas estadísticas y sugerir formas de mejorar la asignación del tiempo de reunión al reducir estos factores negativos.



**FIGURA 2-55** Gráfico de análisis del lugar de trabajo del tiempo de baja calidad empleado en reuniones

Además de estas estadísticas predefinidas, Workplace Analytics también permite a los administradores crear sus propias consultas que utilizan los datos para responder preguntas sobre usuarios específicos, grupos de usuarios y actividades. Hay cuatro tipos de consultas compatibles, como se muestra en Figura 2-56 :

Ways to Query the Data																							
Query Type	Usage	Example	Output Schema																				
 Person Hours	Understand and compare the typical behaviors and collaboration trends for population subsets	Meeting Hours Initiated by individuals in Marketing with Sales Account Executives that are based in Canada or Mexico	<table border="1"> <thead> <tr> <th>Person ID</th><th>Date</th><th>Person attribute 1 (department)</th><th>Person attribute 2 (role)</th><th>Metric 1 (Mtg hrs customized)</th></tr> </thead> <tbody> <tr> <td>A</td><td>3/1/2017</td><td>Marketing</td><td>Brand Mgr.</td><td>11</td></tr> <tr> <td>B</td><td>3/1/2017</td><td>Marketing</td><td>Analyst</td><td>14</td></tr> </tbody> </table>	Person ID	Date	Person attribute 1 (department)	Person attribute 2 (role)	Metric 1 (Mtg hrs customized)	A	3/1/2017	Marketing	Brand Mgr.	11	B	3/1/2017	Marketing	Analyst	14					
Person ID	Date	Person attribute 1 (department)	Person attribute 2 (role)	Metric 1 (Mtg hrs customized)																			
A	3/1/2017	Marketing	Brand Mgr.	11																			
B	3/1/2017	Marketing	Analyst	14																			
 Meetings	Analyze individual meetings that fit specified criteria	Emails Sent during One Hour meetings Organized By Sales that also contain At Least 1 Marketing representative	<table border="1"> <thead> <tr> <th>Meeting ID</th><th>Start Date</th><th>Duration Hours</th><th># Attendees</th><th>Metric 1 (Emails Sent)</th><th>Subject</th></tr> </thead> <tbody> <tr> <td>A</td><td>3/1/2017</td><td>1</td><td>6</td><td>3</td><td>Pitch deck for customer visit</td></tr> <tr> <td>B</td><td>3/1/2017</td><td>1</td><td>37</td><td>14</td><td>Demo training for upcoming release</td></tr> </tbody> </table>	Meeting ID	Start Date	Duration Hours	# Attendees	Metric 1 (Emails Sent)	Subject	A	3/1/2017	1	6	3	Pitch deck for customer visit	B	3/1/2017	1	37	14	Demo training for upcoming release		
Meeting ID	Start Date	Duration Hours	# Attendees	Metric 1 (Emails Sent)	Subject																		
A	3/1/2017	1	6	3	Pitch deck for customer visit																		
B	3/1/2017	1	37	14	Demo training for upcoming release																		
 Group-to-Group	Study the collaboration between two groups	Meeting Hours Allocated by Region for employees in Marketing grouped by their Role	<table border="1"> <thead> <tr> <th>Group A</th><th>Group B</th><th>Date</th><th>Meeting Hours Allocated</th></tr> </thead> <tbody> <tr> <td>Brand Mgr</td><td>West</td><td>3/1/2017</td><td>62</td></tr> <tr> <td>Brand Mgr</td><td>South</td><td>3/1/2017</td><td>37</td></tr> </tbody> </table>	Group A	Group B	Date	Meeting Hours Allocated	Brand Mgr	West	3/1/2017	62	Brand Mgr	South	3/1/2017	37								
Group A	Group B	Date	Meeting Hours Allocated																				
Brand Mgr	West	3/1/2017	62																				
Brand Mgr	South	3/1/2017	37																				
 Person-to-Group	Compare collaboration trends between individuals and their collaborator groups	Meeting Hours Allocated by Sales Region and initiated by individuals in Marketing	<table border="1"> <thead> <tr> <th>Person ID</th><th>Group A</th><th>Date</th><th>Meeting Hours Allocated</th></tr> </thead> <tbody> <tr> <td>A</td><td>West</td><td>3/1/2017</td><td>42</td></tr> <tr> <td>B</td><td>Midwest</td><td>3/1/2017</td><td>26</td></tr> </tbody> </table>	Person ID	Group A	Date	Meeting Hours Allocated	A	West	3/1/2017	42	B	Midwest	3/1/2017	26								
Person ID	Group A	Date	Meeting Hours Allocated																				
A	West	3/1/2017	42																				
B	Midwest	3/1/2017	26																				

**FIGURA 2-56** Gráfico de tipos de consulta de Workplace Analytics

- **Persona** Proporciona información individualizada y detallada sobre la utilización del tiempo para un grupo de empleados (desidentificados)
- **Reunión** Proporciona información sobre la relación entre las propiedades de la reunión, como el tamaño, la duración, el tema y el organizador.
- **Grupo a grupo** Cuenta el tiempo que dos equipos o grupos de empleados pasaron interactuando
- **Persona a grupo** Cuenta el tiempo que un individuo pasó interactuando con un equipo o grupo específico

Por ejemplo, si la métrica de resumen de Reuniones indica que un número anormalmente grande de

se están celebrando reuniones de calidad, un administrador puede crear una consulta para tratar de identificar qué equipos o grupos de trabajadores participan con mayor frecuencia en estas reuniones y tratar de determinar por qué, con la esperanza de descubrir un medio para abordar el problema.

## RESUMEN

---

- Microsoft 365 consta de tres componentes principales: Windows 10, Office 365 y Enterprise Mobility + Security. Office 365 incluye servicios adicionales, incluidos Exchange Online, SharePoint Online y Microsoft Teams. Enterprise Mobility + Security incluye Azure Active Directory Premium, Microsoft Intune, Azure Information Protection y Advanced Threat Analytics.
- Algunos de los componentes de Microsoft 365 están disponibles como aplicaciones y servicios locales. Los incentivos para usar software basado en la nube en lugar de local incluyen gastos iniciales reducidos, actualizaciones de funciones más frecuentes y alta disponibilidad.
- La administración moderna es una evolución de los modelos tradicionales de implementación y soporte de TI para enfatizar la movilidad del cliente y los servicios y administración basados en la nube.
- Office 365 ProPlus incluye las aplicaciones de productividad de Office tradicionales e instalables, que incluyen Word, Excel y PowerPoint, así como servicios basados en la nube, como Exchange Online, SharePoint Online, Microsoft Teams y Yammer. En comparación con los productos locales, Office 2016 y Office 2019, Office 365 ofrece muchas ventajas, incluidas actualizaciones más frecuentes, licencias para hasta cinco dispositivos, soporte para dispositivos móviles y servicios de colaboración y correo electrónico basados en la nube.
- Microsoft 365 está diseñado para proporcionar a los usuarios la capacidad de trabajar en cualquier lugar, utilizando cualquier dispositivo. Al proporcionar colaboración basada en la nube

herramientas y permitiendo que los administradores administren el hardware Bring Your Own Device de los usuarios, Microsoft 365 admite un modelo de productividad más moderno.

- Microsoft 365 incluye herramientas de análisis que pueden recopilar información de aplicaciones y servicios en toda la empresa y usar para anticipar amenazas y mejorar la productividad de los trabajadores.

## EXPERIMENTO MENTAL

---

En este experimento mental, demuestre sus habilidades y conocimiento de los temas tratados en este capítulo. Puede encontrar respuestas a este experimento mental en la siguiente sección.

Alice está planeando un despliegue de Office para la nueva sucursal de su compañía en Chicago y está comparando las ventajas y desventajas de Office 365 y Office 2019. Se espera que la sucursal aumente a un máximo de 120 nuevos usuarios en un año, y Alice está tratando de anticipar las necesidades de los usuarios y mantenerse dentro de su presupuesto de desembolso inicial, que es relativamente limitado.

Alice quiere crear un entorno de trabajo lo más estable posible para minimizar el soporte técnico y los problemas de capacitación. Le preocupa la posibilidad de actualizaciones mensuales de características en Office 365, que podrían generar demasiados problemas de soporte y requerir capacitación adicional tanto para los usuarios como para el personal de soporte. Ella sabe que Office 2019 no recibe

actualizaciones de funciones.

La sucursal está conectada a Internet a través de una conexión con un proveedor local de servicios de Internet. La oficina principal de la compañía tiene servidores locales de Exchange y SharePoint, a los que se puede acceder a través de Internet. Alice se pregunta si sería más eficiente para los usuarios acceder a sus bibliotecas de correo y documentos en los servidores principales de la oficina o para ella usar los servicios de Exchange Online y SharePoint Online basados en la nube. Una tercera opción sería que instalara servidores locales de Exchange y SharePoint en la sucursal. También le preocupa la administración de Exchange y SharePoint porque preferiría que su personal en el sitio administre los nuevos procesos de incorporación y mantenimiento de usuarios.

Alice también está preocupada por la administración de identidad para los usuarios de sucursales y el tráfico de autenticación de Active Directory que generarán. La oficina de Nueva York tiene instalados controladores de dominio de Servicios de dominio de Active Directory, pero Alice aún no ha planeado instalar controladores de dominio en la sucursal. Es consciente de que Azure Active Directory puede proporcionar administración de identidad basada en la nube, pero le preocupa que los usuarios de sucursales a veces requieran acceso a los recursos almacenados en los servidores de Nueva York.

Después de una cuidadosa consideración de todos estos factores, Alice decidió elegir Office 365 y sus servicios en la nube.

para el despliegue de sucursales. Enumere cinco razones por las cuales su selección está justificada.

## PENSAMIENTO RESPUESTA DEL EXPERIMENTO

---

Alice puede abordar todas sus inquietudes implementando Office 365 y utilizando los servicios de Exchange Online y SharePoint Online basados en la nube por los siguientes motivos:

- Office 365 se puede configurar para recibir actualizaciones de características solo dos veces al año, lo que reduciría los posibles problemas de capacitación y soporte, en comparación con las actualizaciones mensuales.
- Debido a que está basado en suscripción, Office 365 tiene un desembolso de costo inicial mucho menor que Office 2019, que debe pagarse en su totalidad durante la implementación inicial.
- Los servicios basados en la nube disponibles con Office 365 brindan a los usuarios acceso a Exchange y SharePoint a través de un punto final cercano de Microsoft Global Network. Requerir que los usuarios accedan a los servidores de Exchange y SharePoint en Nueva York probablemente generará latencia de red adicional y, por lo tanto, reducirá la eficiencia del usuario. Exchange Online y SharePoint Online se administran a través de herramientas basadas en la web a las que puede acceder directamente el personal de soporte de la sucursal. La incorporación de nuevos usuarios en los servidores de Nueva York requeriría acceso remoto o participación del personal de Nueva York para completar los procesos de incorporación.
- Azure Active Directory permitiría que el personal de soporte de la sucursal administre las cuentas de los usuarios y disminuiría la latencia de la red que causaría la autenticación a través de los controladores de dominio de Nueva York. Azure AD también se puede configurar para sincronizarse con los controladores de dominio de Nueva York, lo que permite a los usuarios de sucursales recibir acceso autenticado a los recursos en los servidores de Nueva York.



# **Capítulo 3. Comprenda la seguridad, el cumplimiento, la privacidad y la confianza en Microsoft 365**

Microsoft 365 se concibió originalmente como un producto que presentaría a los usuarios herramientas familiares, como las aplicaciones de productividad de Office, y les permitiría colaborar de nuevas maneras, de manera más fácil, más eficiente y utilizando cualquier dispositivo en cualquier ubicación. Esta es una aspiración maravillosa, pero los diseñadores del producto pronto se dieron cuenta de que esta idea de colaboración universal planteaba problemas de seguridad, cumplimiento, privacidad y confianza que debían abordarse antes de que se pudiera realizar el ideal.

Por lo general, estos problemas son el principal impedimento para la adopción completa de Microsoft 365 para muchos profesionales de TI. La idea de almacenar datos confidenciales en la nube y permitir que los trabajadores usen sus propios dispositivos para acceder a esos datos es aterradora para los administradores para quienes la seguridad se está convirtiendo en un problema cada día más importante. Sin embargo, los diseñadores de Microsoft 365 se han esforzado mucho para abordar estos problemas y han creado un producto

eso, cuando se usa correctamente, debe satisfacer las preocupaciones de incluso los directores de TI más asustadizos.

### Habilidades en este capítulo:

- Comprender los conceptos de seguridad y cumplimiento con Microsoft 365 Comprender la \_\_\_\_\_
- protección y administración de identidades Comprender la necesidad de una administración de \_\_\_\_\_
- punto final unificada, escenarios de uso de seguridad y servicios \_\_\_\_\_  
\_\_\_\_\_
- Comprender el portal de confianza de servicio y el gerente de cumplimiento \_\_\_\_\_

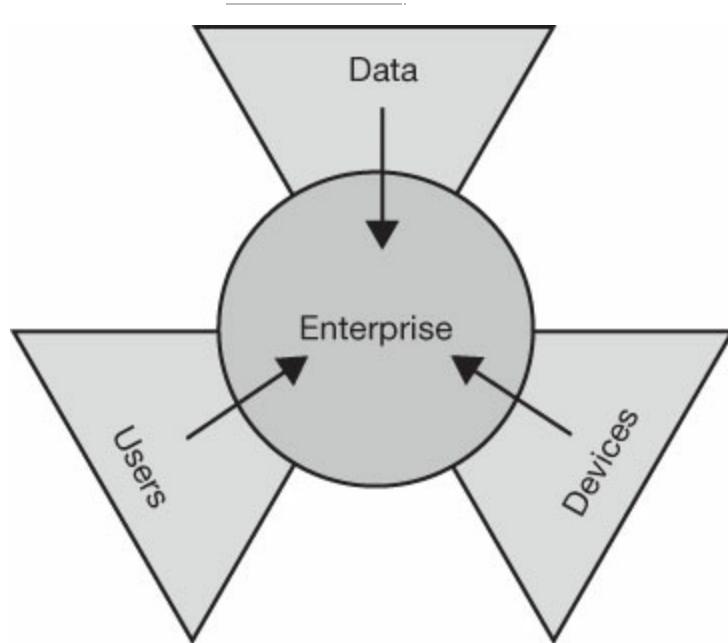
## HABILIDAD 3.1: ENTENDER LOS CONCEPTOS DE SEGURIDAD Y CUMPLIMIENTO CON MICROSOFT 365

---

En un momento, la seguridad de la empresa podría considerarse como un perímetro que rodea a una organización. Los datos permanecieron en gran medida dentro de los sitios de la organización y podían protegerse del acceso no autorizado mediante firewalls y barreras físicas. Incluso cuando los datos comenzaron a ser accesibles más allá de la organización utilizando sitios web de Internet y dispositivos portátiles, estos posibles vectores de ataque todavía eran propiedad y estaban administrados por la compañía.

Los activos que una organización necesita proteger, ahora conocidos como sus *finca digital*, han crecido enormemente en los últimos años y también los medios de entrada y salida de la empresa. Este estado digital ciertamente incluye

los datos de la compañía, pero también incluye a los usuarios que acceden a los datos y los sistemas y dispositivos por los cuales acceden a los datos. Los tres activos son puntos débiles potenciales en un sistema de seguridad empresarial, como se muestra en Figura 3-1 . Los tres necesitan protección.



**FIGURA 3-1** Los tipos de activos empresariales que necesitan protección

El compromiso con la nube requerido por los adoptantes de Microsoft 365 crea un nuevo vector de ataque. Sin embargo, para proteger completamente los datos de la empresa, los administradores de TI ahora deben preocuparse por la nube, y deben preocuparse por la seguridad de los dispositivos que no son directamente propiedad de la organización, no se encuentran dentro de la organización y, en algunos casos, propiedad de usuarios que ni siquiera son empleados de la organización.

Por lo tanto, el almacenamiento primario para los datos de una organización puede ubicarse en la nube o en servidores mantenidos en las instalaciones. En muchos casos, los datos se dividen entre los dos. Eso significa que los administradores deben ser responsables de la seguridad de ambos. Sin embargo, además de las ubicaciones de almacenamiento primario, los dispositivos que los trabajadores usan para acceder a los datos también son vectores de ataque potenciales. La creciente adopción del paradigma Traiga su propio dispositivo (BYOD) complica el proceso de asegurar los datos que podrían almacenarse en el bolsillo de alguien en un dispositivo que podría no ser completamente manejable por los administradores de la empresa.

El problema de seguridad también se extiende más allá de los extremos lógicos de la empresa a los socios, clientes y consultores con los que los empleados comparten datos. Estas personas usan sus propios sistemas y dispositivos que están aún más lejos del alcance de los administradores de la empresa. Todos estos vectores de ataque pueden proporcionar a los intrusos una forma de ingresar a la red empresarial, y una vez que los intrusos sofisticados están dentro, a menudo logran permanecer allí y extender su influencia.

Si bien siempre hay un cierto número de ciberdelincuentes casuales que son relativamente fáciles de rechazar, los intentos serios de penetración profesional que a menudo afectan a las grandes empresas pueden ser increíblemente sofisticados y tener lugar durante largos períodos de tiempo. Microsoft 365 incluye una poderosa variedad de herramientas de seguridad que lo hacen

Es posible que los administradores implementen varios tipos de protección sobre los datos de la compañía y los dispositivos que acceden a ellos, pero estas herramientas no son simples soluciones llave en mano. Los administradores empresariales deben diseñar un plan de seguridad que priorice la sensibilidad de los datos de la compañía, evalúe la vulnerabilidad de los sistemas y dispositivos en los que se almacenan los datos, identifique a los usuarios y sus necesidades de datos, y especifique cómo se utilizarán las herramientas de Microsoft 365.

## Gestión de riesgos

Por lo general, la información es el recurso más valioso que posee una empresa. Al considerar las medidas de seguridad para una red empresarial, el fin último de estas medidas es proteger la información. La protección contra usuarios o dispositivos no autorizados es realmente solo un medio de proteger los datos a los que esos usuarios pueden acceder y almacenar en esos dispositivos. Las computadoras y otros dispositivos de hardware tienen un valor monetario, pero las medidas de seguridad física de un centro de datos, por ejemplo, las cerraduras electrónicas de las puertas, los guardias de seguridad y los sistemas de extinción de incendios, están allí principalmente para proteger la información almacenada en el hardware y no tanto el hardware en sí.

El proceso de crear un plan de seguridad para una empresa se conoce como *gestión de riesgos*. Cuál es el

acto de identificar los activos que necesitan protección, determinar los peligros potenciales para esos activos, evaluar el impacto de esos peligros para la organización e implementar medidas de protección apropiadas para los activos y las amenazas. Microsoft 365 incluye una gran colección de herramientas que pueden ayudar con todas las fases de este proceso. Las tecnologías de seguridad en Microsoft 365 se dividen en cuatro áreas, de la siguiente manera:

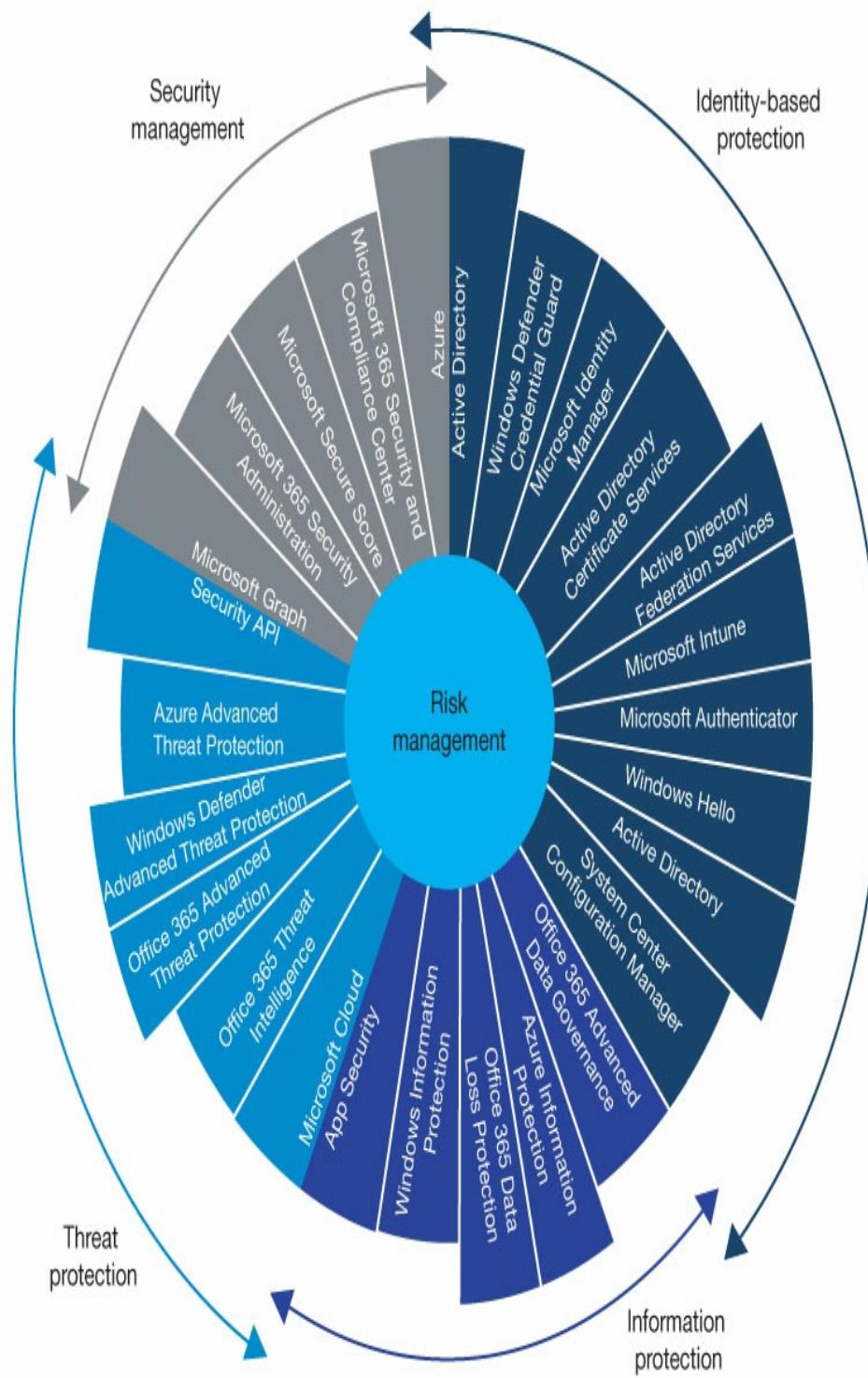
- Gestión de seguridad Protección basada
- en la identidad Protección de la
- información Protección contra amenazas
- 

Las tecnologías en cada una de estas áreas se muestran en

**Figura 3-2.** . Es poco probable que una organización que busca proteger su red empresarial necesite todas estas tecnologías. Considere que se trata de un juego de herramientas del que los administradores pueden seleccionar la herramienta adecuada para cada tarea. El grupo de Servicios Centrales y Operaciones de Ingeniería (CSEO) de Microsoft ha elegido las tecnologías que sobresalen de la rueda que se muestra en **Figura 3-2.** .

---

## Microsoft 365 technologies and their associated security areas



**FIGURA 3-2** Tecnologías de seguridad de Microsoft 365 utilizadas por el grupo CSEO de Microsoft

Por lo tanto, el primer paso del plan de gestión de riesgos es identificar los tipos de información que posee la organización y determinar el valor de cada tipo de información para el negocio.

**Identificar y valorar los activos de información.**

Las empresas a menudo generan grandes cantidades de datos, que se ajustan a varios niveles de sensibilidad. Por lo general, no es práctico para una organización implementar el último nivel de seguridad sobre todos sus datos, por lo que es necesario clasificar la información de acuerdo con su función y valor. Por lo tanto, el proceso de gestión de riesgos debe comenzar con un inventario de los activos de información de la organización y una determinación del valor de cada activo para la empresa, teniendo en cuenta su necesidad de confidencialidad, integridad y disponibilidad. Los factores a considerar al compilar dicho inventario se muestran en Tabla 3-1 .

**CUADRO 3-1** Factores de riesgo para el inventario de activos

FACTOR DE RIESGO	DESCRIPCIÓN	EJEMPLO
	Con acceso y divulgación de	¿Qué pasa si las contraseñas de los usuarios o

fide ntial ity	información confidencial de personas no autorizadas	Los números de la Seguridad Social fueron robados?
Integridad	Modificación o daño de información sensible por personas no autorizadas	¿Qué pasa si se cambia la información de nómina de la empresa o los diseños de productos?
Availabil ity	Prevención del acceso a información confidencial por parte de usuarios autorizados.	¿Qué sucede si la lista de clientes o el sitio web de la compañía se volvieron inaccesibles?

Las definiciones utilizadas para los tipos de información serán específicas de la naturaleza del negocio, al igual que su valor para el negocio. Por ejemplo, en el caso de una empresa que utiliza su sitio web para proporcionar información de soporte a los clientes, un ataque que hace que el sitio no esté disponible durante varios días sería un inconveniente. Sin embargo, para una empresa que vende sus productos exclusivamente en la web, la falta de disponibilidad de su sitio web de comercio electrónico durante varios días podría ser desastrosa.

Para una empresa grande, este tipo de inventario de activos no suele ser una provincia exclusiva del departamento de TI. Es probable que requiera la participación del personal de varios departamentos y en varios niveles de la organización, incluidos los de gestión, legales, contables e incluso clientes y socios externos a la empresa.

El valor de un recurso de información podría no

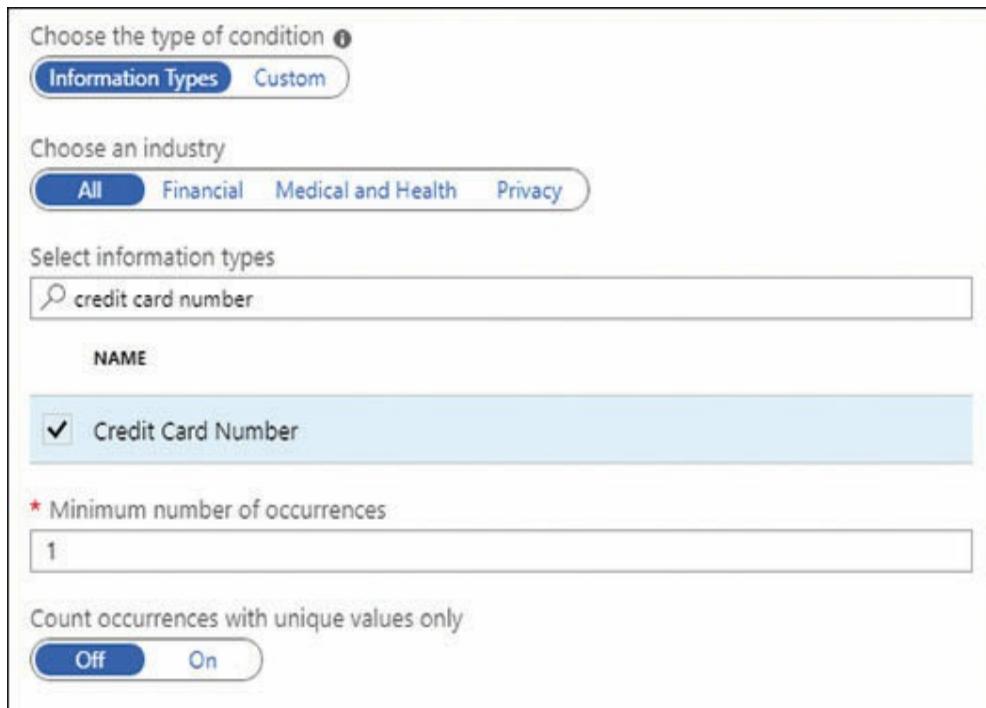
necesariamente se expresará en términos monetarios. El resultado de una amenaza de datos podría ser la pérdida de productividad, la creación de trabajo adicional para restaurar o recrear los datos, multas o sanciones para el gobierno o las agencias reguladoras, o incluso efectos más intangibles, como malas relaciones públicas o pérdida de confianza del cliente.

Para cuantificar los activos inventariados, la mejor práctica es crear una escala graduada que considere todos los factores de riesgo particulares del negocio. Una escala numérica general de 1 a 3 o una gradación de riesgo de bajo, medio o alto funcionaría, con un mayor número de calificaciones si las medidas de seguridad que los administradores eligen implementar lo justifican.

El valor o la sensibilidad de un activo de datos determinará la naturaleza de los mecanismos de seguridad que los administradores usan para protegerlo. Algunos tipos de datos pueden estar sujetos a especificaciones de cumplimiento legales o contractuales, que imponen límites estrictos sobre dónde y cómo se almacenan y quién puede acceder a ellos. Los requisitos de seguridad para estos datos más confidenciales pueden definir el valor más alto en la escala de riesgos, lo que puede requerir medidas de seguridad extremas, como almacenamiento local en un centro de datos seguro, cifrado y redundancia de datos, y permisos de acceso altamente restringidos.

Es posible que otros tipos de datos confidenciales ni siquiera estén sujetos a mecanismos de seguridad categóricamente amplios, como los que se aplican a carpetas de archivos o tipos de archivos específicos.

Microsoft 365 incluye la herramienta Azure Information Protection (AIP) que puede aplicar etiquetas a documentos que contienen información confidencial. Los administradores pueden configurar las etiquetas para activar varios tipos de seguridad, como marcas de agua, cifrado y acceso limitado. Si bien los usuarios y los administradores pueden aplicar manualmente las etiquetas a los documentos, AIP también puede detectar información confidencial en los documentos y aplicarles etiquetas automáticamente. Por ejemplo, cuando un usuario crea un documento de Word, los administradores pueden configurar AIP para detectar valores que parecen ser números de tarjetas de crédito, como se muestra en Figura 3-3 y aplique una etiqueta al archivo que requiera un grado específico de protección.



**FIGURA 3-3** Configuración AIP

Los datos que no amenazan en gran medida la confidencialidad, la integridad y la disponibilidad se encuentran en el extremo inferior de la escala de riesgos. Estos datos requerirán cierta protección, pero la seguridad en el extremo inferior de la escala podría estar limitada solo a los permisos de acceso al sistema de archivos.

## Inventario de hardware

Una vez que se ha evaluado la sensibilidad y el valor de los datos, el siguiente paso del proceso de diseño del plan de gestión de riesgos es considerar la tecnología utilizada para almacenar, acceder, transmitir y procesar esos datos. Esto incluye los servidores o servicios en la nube donde se almacenan los datos cuando están en reposo, los sistemas y dispositivos del cliente utilizados para acceder a los datos, los componentes de la red que transportan los datos entre los diversos sistemas y las aplicaciones que procesan los datos.

De la misma manera que los datos en sí mismos se inventariarían en la fase anterior, debe haber un inventario de todo el hardware involucrado en el almacenamiento de los datos. Esta información se puede utilizar para localizar la fuente precisa de una violación de seguridad y para ayudar a evitar que dispositivos no autorizados accedan a recursos seguros de la compañía.

Las ubicaciones de almacenamiento principales para toda la información confidencial de la empresa deben ser servidores ubicados en un entorno seguro, como un centro de datos o armario de servidores, o un servicio en la nube, que debe tener sus propias políticas de seguridad detalladas en el contrato de servicio.

Sin embargo, el proceso de compilar un inventario de los sistemas y dispositivos del cliente puede ser significativamente más complicado. Presumiblemente, las estaciones de trabajo ubicadas en los sitios de la empresa ya están inventariadas, pero deben considerarse las computadoras domésticas y los dispositivos móviles de los empleados, como teléfonos inteligentes y tabletas. Además, deben considerarse las computadoras y dispositivos que pertenecen a personas externas a la organización, como socios, consultores, trabajadores temporales y clientes.

Los administradores deben documentar cada dispositivo que entre en contacto con los datos de la empresa. El inventario debe incluir información como la siguiente:

- **Hacer** El fabricante del dispositivo.
- **Modelo** El nombre y número de modelo del fabricante del dispositivo.
- **Número de serie** El número de serie del fabricante del dispositivo.
- **Propietario** La persona u organización propietaria del dispositivo.
- **Usuario** La persona o personas que usan el dispositivo para acceder a los datos de la empresa.
- **Ubicación** El lugar donde está instalado el dispositivo o, si es móvil, la ubicación de la persona responsable del mismo.
- **ID de servicio** El número de identificación asignado de la organización propietaria, si corresponde
- **Sistema operativo** El sistema operativo instalado en el dispositivo.
- **versión del sistema operativo** La versión y compilación del sistema operativo que se ejecuta en el dispositivo
- **Proveedor de red** El proveedor utilizado por el dispositivo para acceder a Internet o la red de la empresa.

- **Aplicaciones** Las aplicaciones en el dispositivo que se utilizan para acceder a los datos de la empresa.

- **Información utilizada** Los tipos específicos de datos de la empresa a los que puede acceder el dispositivo

Para las estaciones de trabajo que son propiedad de la organización, esta información generalmente se compila durante el proceso de implementación del sistema y probablemente se pueda importar al inventario. Para los sistemas y dispositivos propiedad de los empleados, el proceso de recopilación de información debe ser requerido antes de que se permita el acceso a datos confidenciales de la empresa.

La verificación de la información del inventario puede ser difícil para los usuarios que son viajeros frecuentes o usuarios de computadoras en el hogar, pero en el modelo de administración moderno implementado por Microsoft 365, el control estricto de los dispositivos de hardware es un elemento esencial de la seguridad empresarial. Para los dispositivos propiedad de personas que no son empleados de la organización, como los clientes, los aspectos diplomáticos de la aplicación de estas políticas pueden ser aún más difíciles, pero los administradores pueden mitigarlos creando un nivel de riesgo que brinde acceso a estos usuarios solo a una clase limitada de información que no es extremadamente sensible.

Además de los sistemas y dispositivos que acceden a los datos de la compañía, la tecnología de redes también puede presentar un elemento de riesgo. El vector de ataque potencial más obvio son los dispositivos de red inalámbricos, que son vulnerables

a ataques externos en una variedad de formas. Microsoft 365 incluye Microsoft Intune, que permite a los administradores crear perfiles de red Wi-Fi que contienen claves previamente compartidas y otras medidas de seguridad que evitan que dispositivos no autorizados se conecten a una red inalámbrica de la compañía. También hay algunos tipos de datos extremadamente confidenciales que pueden requerir un manejo especial incluso para redes cableadas, como las regulaciones de cumplimiento que requieren que los cables de red estén encerrados en conductos sellados para protección contra escuchas telefónicas. Los dispositivos de seguridad basados en hardware, como los firewalls, también deben incluirse en el inventario.

Cuando el hardware que accede a información confidencial se ve comprometido, se supone que los datos también se ven comprometidos. Los administradores pueden usar el inventario de hardware para asegurarse de que los sistemas operativos y las aplicaciones en los dispositivos estén actualizados con parches de seguridad y que los antivirus y otras herramientas de seguridad estén actualizados. Los administradores también pueden usar las herramientas de Microsoft 365 para crear políticas de cumplimiento para que los dispositivos no puedan acceder a los recursos de la red a menos que cumplan con requisitos específicos, incluido el software actualizado.

Los elementos de seguridad de hardware de un plan de gestión de riesgos pueden ir más allá de las capacidades de las herramientas en Microsoft 365. La protección del hardware puede incluir otros mecanismos, incluidos los siguientes:

- **Seguridad física** Las medidas de seguridad basadas en software no pueden

proteja los datos almacenados en una computadora si los intrusos tienen acceso físico a la máquina.

Incluso si los intrusos no pueden comprometer los datos, siempre pueden destruirlos, lo que puede ser igual de perjudicial para la organización. Las medidas físicas, incluso aquellas tan simples como una puerta cerrada, son elementos básicos de cualquier plan de gestión de riesgos. Para los dispositivos móviles, que siempre son vulnerables a la pérdida o el robo, los administradores pueden usar la administración de dispositivos móviles de Microsoft Intune para implementar la solución de hardware definitiva: borrar de forma remota los datos del dispositivo.

- **Alta disponibilidad** Además de la intrusión maliciosa o criminal, los dispositivos de hardware también pueden sufrir fallas por el desgaste o la destrucción por desastres naturales, como incendios, terremotos y condiciones climáticas extremas. Las medidas de alta disponibilidad, como las matrices RAID, los servidores redundantes y los centros de datos duplicados, pueden preservar los datos contra pérdidas y garantizar que los datos permanezcan disponibles para los usuarios. Para los datos de Microsoft 365 almacenados en la nube, Microsoft Global Network mantiene centros de datos en ubicaciones de todo el mundo, como se muestra en

Figura 3-4 , proporcionando a los suscriptores una tasa de disponibilidad del 99.9 por ciento.

- **Recuperación de desastres** Las copias de seguridad de datos y la sincronización en la nube pueden permitir la restauración de datos confidenciales, incluso después de un ataque o un desastre, los datos originales o el hardware en el que están almacenados no se pueden usar.



**FIGURA 3-4** Ubicaciones del centro de datos de Microsoft Global Network

### Clasificación de usuarios

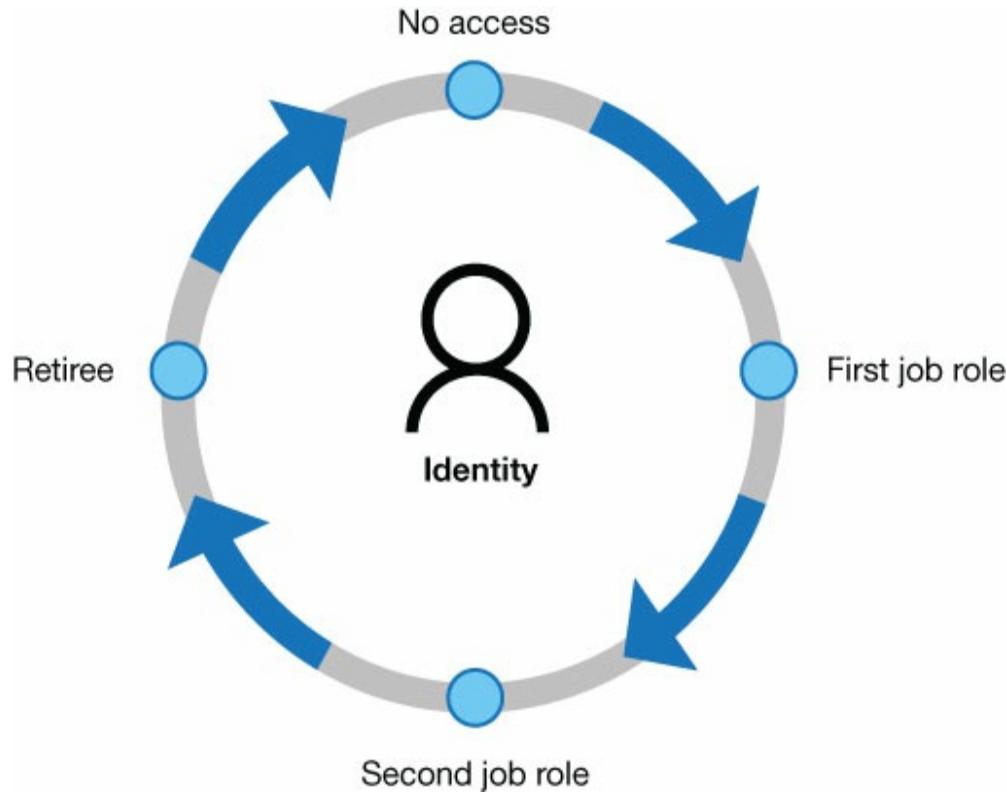
El tercer elemento del patrimonio digital que debe considerarse al crear un plan de gestión de riesgos son las personas que realmente acceden a los datos. Los usuarios, ya sea de manera deliberada o inadvertida, son una vulnerabilidad constante, si no una amenaza real, a los datos de la organización. Después de cuantificar los activos de información de la organización y su valor y después de inventariar el hardware utilizado para almacenar, acceder,

transmitir y procesar la información, el siguiente paso es enumerar las personas que tienen acceso a la información.

Las personas con acceso a la información de la organización ciertamente incluyen empleados que están autorizados para crear, ver y modificar los datos. Sin embargo, un equipo de gestión de riesgos debe considerar la posibilidad de que otras personas también accedan a los datos. Cualquier persona con acceso físico a las computadoras en las que se almacenan los datos o desde los cuales se puede acceder es una amenaza potencial. Esto incluye personal de limpieza y mantenimiento, personal de reparación e incluso guardias de seguridad. Incluso si un individuo no tiene las credenciales necesarias para iniciar sesión en una computadora, aún es posible que una persona robe o destruya la computadora o le quite un disco duro.

Un plan de gestión de riesgos debe incluir una lista de todas las personas que tienen acceso a información confidencial y a qué información exacta pueden acceder. Las políticas de control de acceso deben estar diseñadas para proporcionar a los usuarios permisos solo para los datos que necesitan y no más. Dentro de la organización, los administradores a menudo hacen esto definiendo roles, otorgando a los roles acceso a los datos requeridos y luego asignando individuos a esos roles. Esto simplifica el proceso de autorizar a nuevos usuarios, trasladar usuarios a otros trabajos y desautorizar a los usuarios salientes. Los administradores pueden crear un ciclo de vida ordenado para la identidad de cada usuario individual, como se muestra en Figura 3-5 .

---



**FIGURA 3-5** Ciclo de vida de identidad para un usuario individual

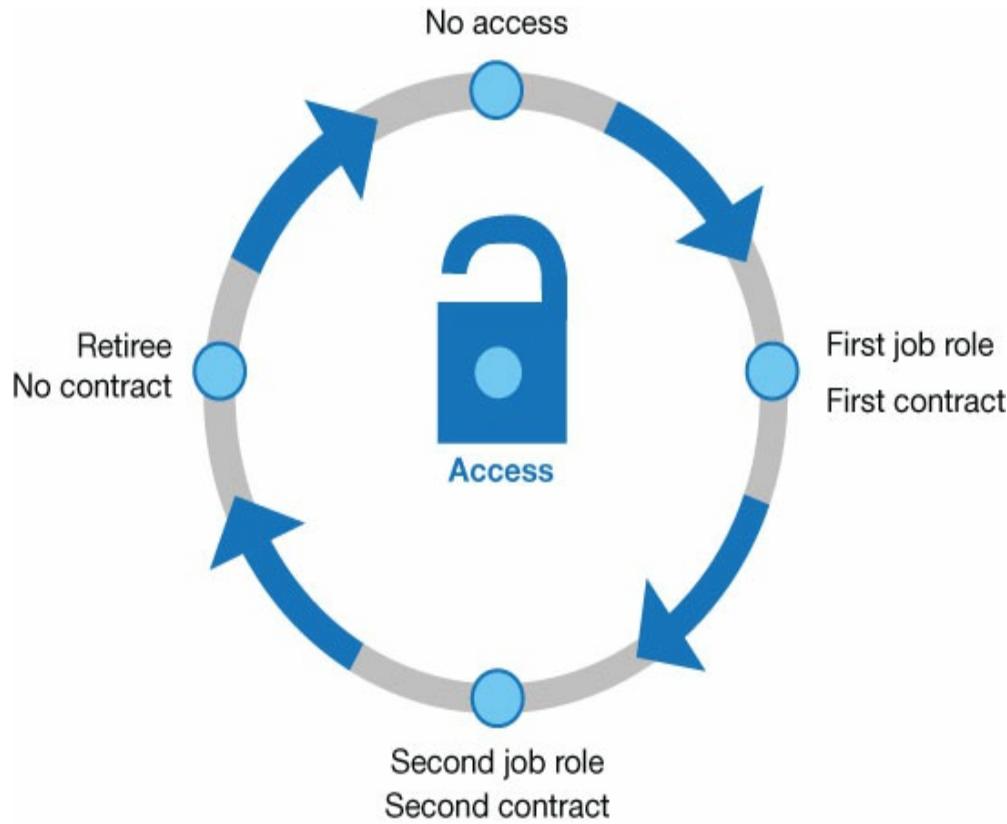
Toda persona a la que se le conceda acceso a los datos de la empresa debe tener una cuenta de usuario individual, incluidas las personas que trabajan temporalmente en el sitio. Cualquier conveniencia que pueda realizarse creando cuentas de invitados genéricas y asignándolas a usuarios temporales, según sea necesario, se anulará por la dificultad que estas cuentas pueden causar al investigar un incidente que involucre la pérdida de datos o el acceso no autorizado.

El plan también debe incluir los medios para garantizar que las personas que inician sesión en las computadoras sean en realidad las personas que pretenden ser. Las políticas de contraseña pueden

asegúrese de que los usuarios creen contraseñas lo suficientemente largas y complejas y cámbielas regularmente. Microsoft 365 también incluye varios mecanismos de autenticación mejorados, que incluyen opciones de autenticación multifactor que requieren un escaneo de huellas digitales o un código enviado a un teléfono móvil además de una contraseña.

Los usuarios con privilegios administrativos presentan una mayor amenaza potencial para los datos de la empresa. El plan de gestión de riesgos debe incluir políticas que requieran que los administradores usen cuentas de usuario estándar para todas las funciones de trabajo típicas y cuentas de administrador solo para tareas que requieren privilegios adicionales. Esto no solo ayuda a proteger los datos de la compañía de daños accidentales o eliminación, sino que también reduce la posibilidad de instalación de software no autorizada, ya sea intencional o no. Las cuentas de usuario con acceso privilegiado deben tener sus propias políticas de ciclo de vida con una supervisión y control más estrictos, como se muestra en **Figura 3-6**.

---



**FIGURA 3-6** Ciclo de vida para una cuenta de usuario con acceso privilegiado

Por supuesto, incluso los usuarios autorizados pueden ser una amenaza, y el plan de gestión de riesgos debe definir los medios específicos por los cuales los nuevos empleados son examinados, lo que debe incluir verificaciones de antecedentes nacionales (o internacionales), historiales de crédito y confirmación de títulos y otras credenciales. Para las organizaciones que trabajan con datos que son extremadamente confidenciales, podría ser necesaria una investigación más extensa de las nuevas contrataciones.

Los usuarios internos son una fuente importante de incidentes de seguridad, aunque los incidentes pueden ser involuntarios

así como deliberado. Los trabajadores descontentos y el espionaje industrial son, sin duda, causas legítimas de robo o pérdida de datos, pero los resbalones simples, como dejar desatendida una computadora iniciada, pueden ser igualmente peligrosos. Además de abordar las amenazas maliciosas, un plan de gestión de riesgos debe dedicar suficiente atención a las amenazas accidentales.

## Anticipando amenazas

Podría decirse que la parte más difícil del proceso de planificación de la gestión de riesgos es tratar de anticipar todas las posibles amenazas que podrían afectar los datos de la compañía en el futuro. Los tres factores de riesgo básicos para los datos (confidencialidad, integridad y disponibilidad) pueden explotarse de varias maneras específicas, pero las categorías de amenazas generales se enumeran en Tabla 3-2. .

**CUADRO 3-2** Posibilidades de amenaza de gestión de riesgos

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Robo de datos por empleado interno	Alteración accidental de los datos por parte del usuario interno.	Daño accidental o destrucción de datos por parte del usuario interno
Robo de datos por intrusos externos	Alteración intencional de datos por empleado interno	Daño intencional o destrucción de datos por parte del usuario interno

Divulgación involuntaria de datos	Alteración intencional de datos por intrusos externos	Daño intencional o destrucción de datos por intrusos externos
		Daño o destrucción de datos por desastre natural

El núcleo del proceso de gestión de riesgos es anticipar las posibles amenazas en detalle y utilizar la información recopilada anteriormente en los inventarios de datos, hardware y usuarios para estimar la gravedad y la probabilidad de cada amenaza. Por ejemplo, la amenaza de revelar las cifras de ventas de clientes de la compañía cuando un usuario que viaja pierde su teléfono inteligente es mucho más probable que la amenaza de que un competidor ingrese a la sede de la compañía por la noche y piratee una estación de trabajo para robar la misma información. La gravedad de la amenaza en los dos escenarios es la misma, pero es más probable que se pierda un teléfono inteligente, por lo que los administradores deben hacer un mayor esfuerzo para mitigar esa posibilidad.

En otro ejemplo, el intento de robo de un competidor podría resultar en el robo de esas mismas cifras de ventas de clientes; en otro escenario, este mismo intento de robo podría causar daños deliberados a los servidores web de la compañía, lo que podría hacer que el sitio de comercio electrónico de la compañía cayera por varios días. La probabilidad de estos escenarios es aproximadamente la misma, pero el daño del servidor web está lejos

amenaza más grave porque interrumpe el flujo de ingresos de la empresa. Por lo tanto, la amenaza más severa justifica un mayor intento de prevención.

Microsoft 365 proporciona herramientas que los administradores pueden usar para predecir, detectar y responder a amenazas de seguridad. Sin embargo, un plan integral de gestión de riesgos va más allá de este tipo de herramientas e incorpora políticas e incluye políticas de compras, políticas de contratación, políticas de construcción y políticas de administración.

## Actualizando el plan

La gestión de riesgos no es un evento único; Debe ser un proceso continuo para ser efectivo. Las amenazas de seguridad continúan evolucionando a un ritmo rápido, por lo que la protección contra ellas también debe evolucionar. Al menos una vez al año, el equipo de gestión de riesgos debe repetir todo el proceso de evaluación, actualizando los inventarios de toda la información, el hardware y los activos humanos de la organización para garantizar que no se hayan producido cambios sin el conocimiento de la empresa. El equipo también debe actualizar la gravedad de la amenaza y la matriz de probabilidad. Las amenazas nuevas o actualizadas requerirán nuevas herramientas de seguridad, procedimientos y políticas para proporcionar protección contra ellos.

Además de las actualizaciones internas del plan de gestión de riesgos, una organización puede querer involucrar a contratistas externos para realizar una evaluación de vulnerabilidad, que es una evaluación de las amenazas en un

infraestructura de seguridad de la organización. Según el tamaño de la organización y la naturaleza actual de sus posibles amenazas, una evaluación de vulnerabilidad puede ser un procedimiento menor y relativamente económico o una tarea compleja y costosa.

Algunos de los tipos específicos de evaluaciones de vulnerabilidad son los siguientes:

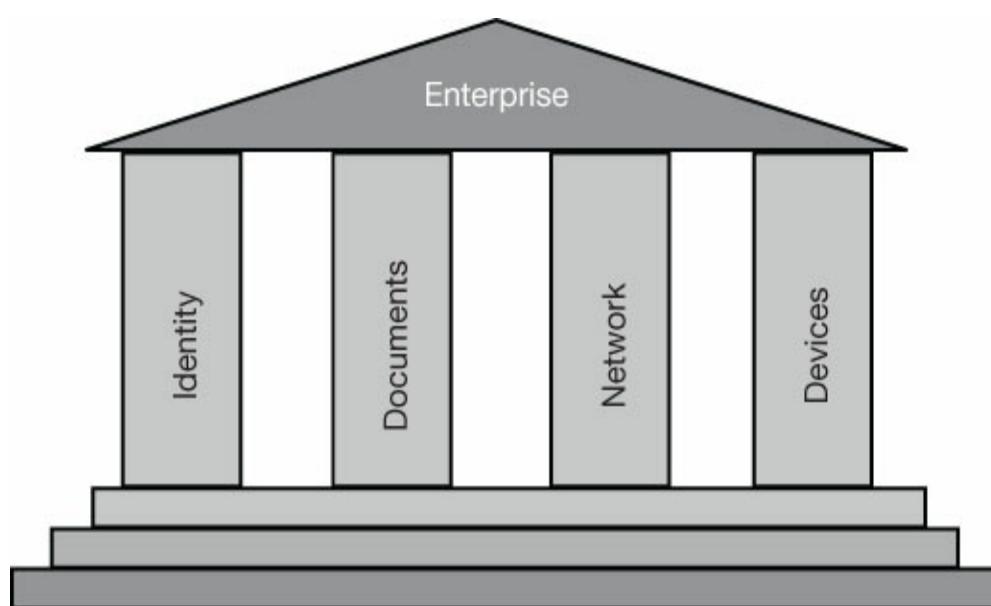
- **Escaneo de red** Identifica vías de posibles amenazas a través de la red interna y las conexiones a Internet, incluidas las configuraciones de enrutador, firewall y red privada virtual (VPN)
- **Escaneo de red inalámbrica** Evalúa las redes Wi-Fi de la organización para detectar vulnerabilidades, incluida la configuración incorrecta, la ubicación de la antena y los puntos de acceso no autorizados
- **Escaneo de host** Identifica vulnerabilidades en servidores, estaciones de trabajo y otros hosts de red, incluidos escaneos de puertos y servicios, ajustes de configuración e históricos de actualizaciones
- **Escaneo de aplicación** Examina los servidores web y otros servidores accesibles por Internet para detectar vulnerabilidades de software y problemas de configuración
- **Escaneo de base de datos** Identifica amenazas específicas de la base de datos en servidores de bases de datos y en las propias bases de datos.

Otro posible método para evaluar las vulnerabilidades de seguridad en el sistema de gestión de riesgos de una organización es realizar una prueba de penetración. Una prueba de penetración es un procedimiento en el que se contrata a un contratista externo para intentar un ataque a los sistemas de la compañía para determinar si las vulnerabilidades potenciales identificadas en el proceso de gestión de riesgos son vulnerabilidades reales y evaluar la

procedimientos de respuesta de la organización.

## Pilares de seguridad clave

Microsoft 365 proporciona una variedad de herramientas y servicios de seguridad que los administradores empresariales pueden usar para proteger los diversos elementos de sus organizaciones. Según la información recopilada durante la planificación de la gestión de riesgos, el equipo puede establecer prioridades que dicten el grado de seguridad requerido y los elementos específicos que requieren atención prioritaria. Una implementación de seguridad integral debe distribuir la protección entre los cuatro pilares principales que respaldan la infraestructura empresarial, como se muestra en Figura 3-7 .



**FIGURA 3-7** Los cuatro pilares de seguridad clave

Estos pilares son los siguientes:

- **Identidad** El proceso mediante el cual un usuario se autentica y luego se autoriza para acceder a recursos protegidos
- **Documentos** Las funciones por las cuales los recursos de datos de la organización están protegidos contra el acceso no autorizado
- **Red** Los medios cableados e inalámbricos que transportan señales de datos, los componentes que proporcionan conectividad a Internet y los protocolos utilizados para codificar las señales, todos los cuales son potencialmente vulnerables a los ataques.
- **Dispositivos** Las computadoras, teléfonos inteligentes y otros dispositivos que acceden a documentos y otros datos a través de la red

Estos cuatro elementos funcionan juntos para permitir a los usuarios acceder a los datos que necesitan, y Microsoft 365 incluye herramientas que pueden proporcionar protección en cada una de estas áreas. Según las necesidades de la organización y las posibles amenazas identificadas, los administradores pueden modificar el grado de protección aplicado en cada uno de estos pilares. Las herramientas y procedimientos que Microsoft 365 proporciona para estas cuatro áreas de seguridad principales se describen en las siguientes secciones.

## Identidad

Es fácil construir una casa perfectamente segura; solo omita todas las ventanas y puertas. Tus posesiones estarán a salvo, pero no podrás acceder a ellas. De la misma manera, sería fácil construir una red perfectamente segura al establecer un perímetro formidable alrededor de los recursos sensibles y no dejar que nadie lo atraviese. Esto no tendría sentido, por supuesto. Los trabajadores necesitan acceso a esos recursos sensibles, y las identidades son

la base de ese acceso. En redes empresariales, un *identidad* es una colección de atributos que describen de forma exclusiva un *director de seguridad*, es decir, un individuo específico y los recursos a los que se le permite acceder.

Para que los datos sean seguros, los tipos de protección más fundamentales son garantizar que las personas que acceden a los datos realmente sean quienes dicen ser y que a las personas se les haya otorgado los niveles adecuados de acceso a los datos que necesitan. El proceso de confirmar la identidad de un usuario en la red se llama *autenticación*,

y el proceso de otorgar a un usuario acceso a datos o servicios específicos es *autorización*. Asegurar las identidades de los usuarios de la red es el proceso de hacer que estos procedimientos sean lo más seguros e impenetrables posible.

Las identidades de los usuarios de una organización son el objetivo principal de los ciberdelincuentes porque robar el nombre y las credenciales de un usuario permite al atacante acceder a todo lo que el usuario sabe sobre la empresa. Las noticias informan regularmente el robo de grandes bloques de identidades de las principales empresas, que ponen en peligro no solo los datos confidenciales de las empresas, sino también la vida personal de sus empleados. Por ejemplo, el robo de los nombres, las direcciones y los números de la Seguridad Social que forman parte de los registros de recursos humanos de cualquier organización dejan a los usuarios expuestos al fraude crediticio y a muchas otras intrusiones criminales. Para la organización, el robo de identidad puede ser catastrófico de muchas maneras, lo que resulta en datos

robo, daño o destrucción que pueden evitar que la empresa haga negocios y le cueste grandes cantidades de dinero.

Los ataques que intentan robar identidades de usuario pueden ser extremadamente simples o increíblemente sofisticados. Una violación de seguridad importante para una organización puede comenzar con un intruso llamando a un usuario desprevenido por teléfono y alegando ser Jack alguien del mantenimiento de la cuenta en el departamento de TI y convenciendo al empleado para que revele el nombre de usuario y la contraseña. Una vez que el intruso tiene las credenciales de un usuario, se hace más fácil para el intruso obtener otras. Este tipo de movimiento lateral dentro de la infraestructura de seguridad de la organización puede ser un proceso lento y metódico que finalmente proporciona acceso a una identidad con acceso de alto nivel a la red y conduce a un evento de seguridad importante. Esta es la razón por la cual los administradores deben esforzarse para proteger todas las identidades de la organización, no solo las que tienen privilegios elevados.

### **En Microsoft 365, *Azure Active Directory (Azure AD)***

permite a los administradores crear identidades de usuario y realiza los procesos de autenticación y autorización, como se muestra en Figura 3-8 .

Azure AD es un servicio de directorio que es una alternativa basada en la nube para

*Servicios de dominio de Active Directory (AD DS)*, que ha sido el servicio de directorio local para redes Windows desde 1999. El objetivo principal en la creación de

Azure AD es la capacidad de dar servicio a las identidades y realizar autenticaciones y autorizaciones para recursos basados en la nube. Este es un elemento esencial de la administración de Microsoft 365.

The screenshot shows the Azure Active Directory admin center interface. The top navigation bar includes links for Dashboard, Users - All users, Documentation, and a user profile for Oliver\_Cox@Oliverco... ADATUM. The main content area is titled 'Users - All users' under 'Adatum - Azure Active Directory'. It features a search bar with 'Search by name or email' and a dropdown for 'Show' (set to 'All users'). Below is a table with columns: NAME, USER NAME, USER TYPE, and SOURCE. The table lists five users:

NAME	USER NAME	USER TYPE	SOURCE
Joanna Yuan	joannayuan@Olivercox.onmicrosoft.com	Member	Azure Active Directory
John Doe	johndoe@Olivercox.onmicrosoft.com	Member	Azure Active Directory
Oliver Cox	Oliver_Cox@Olivercox.onmicrosoft.com	Member	Azure Active Directory
Sanjay Patel	sanjaypatel@Olivercox.onmicrosoft.com	Member	Azure Active Directory

**FIGURA 3-8** Centro de administración de Azure Active Directory

Una implementación de Active Directory basada en Azure es necesaria para Microsoft 365 porque AD DS se limita a proporcionar funciones de seguridad locales. Los usuarios deben tener acceso a la red local para iniciar sesión en los controladores de dominio AD DS de su organización. La única forma en que un usuario remoto puede autenticarse en la red de la empresa mediante AD DS es establecer una conexión a un servidor local, como una conexión de red privada virtual (VPN). Azure AD está estrictamente basado en la nube y

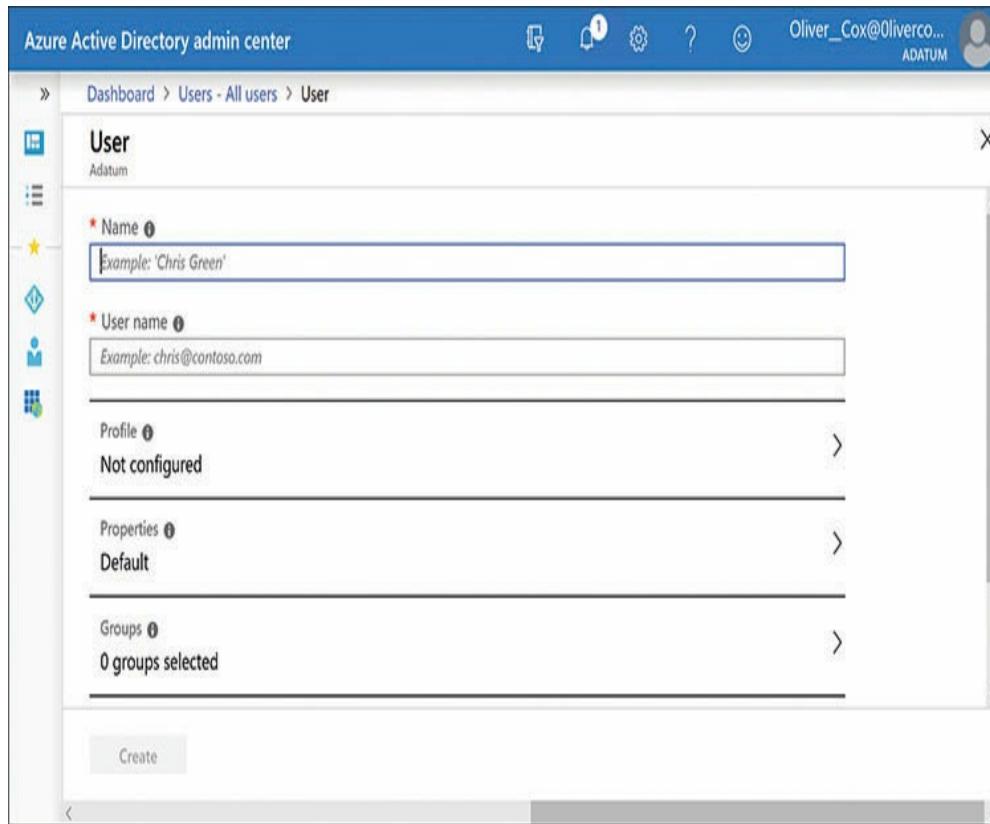
permite a los usuarios que trabajan en cualquier lugar y con cualquier dispositivo iniciar sesión en la red Microsoft 365 de la organización y obtener acceso a sus servicios. Otra ventaja de un servicio de directorio basado en la nube es que los administradores pueden crear identidades para personas externas a la organización, como socios, clientes, proveedores o consultores, que necesitan acceso ocasional o restringido a los recursos de la empresa.

*Nota:* **Usar Azure AD  
con AD DS**

**Azure Active Directory y los Servicios de dominio de Active Directory no son mutuamente excluyentes. Para una organización que ya tiene una infraestructura de AD DS, es posible implementar Azure AD y crear identidades híbridas sincronizando los dos servicios de directorio. Para obtener más información, consulte "Comprender la protección y gestión de identidad", más adelante en este capítulo.**

Crear una identidad en Microsoft 365 es una simple cuestión de proporcionar valores de nombre en una forma como la del Centro de administración de Azure Active Directory que se muestra en

Figura 3-9 . El Centro de administración de Microsoft 365 contiene un formulario similar que también permite al creador de la identidad asignar licencias de productos, como una licencia de Microsoft 365, al usuario. Si bien la creación de identidades es un proceso rápido y fácil, asegurarlas puede ser considerablemente más complicado.



**FIGURA 3-9** Crear una cuenta de usuario de Azure AD

El medio tradicional de autenticar la identidad de un usuario es que el individuo proporcione un nombre de cuenta y una contraseña. En Microsoft 365, los administradores pueden crear políticas de contraseña que obligan a los usuarios a crear contraseñas largas y complejas y cambiarlas con frecuencia. Sin embargo, las contraseñas siempre están sujetas a posibles debilidades que las convierten en un mecanismo de autenticación difícil de manejar, que incluye lo siguiente:

- Los usuarios pueden tener dificultades para recordar contraseñas largas o complejas y escribirlos en ubicaciones no seguras.
- Los usuarios pueden compartir sus contraseñas con compañeros de trabajo por el bien de

conveniencia.

- Los usuarios con cuentas dedicadas que tienen privilegios elevados pueden usar en exceso sus contraseñas administrativas para las tareas cotidianas. Los usuarios pueden proporcionar las mismas contraseñas para múltiples servicios o recursos, agravando el daño si se compromete una contraseña en un servidor.
- Los usuarios pueden ser engañados para que proporcionen sus contraseñas mediante ataques de phishing o de ingeniería social.
- Las identidades de los usuarios pueden verse comprometidas cuando sus contraseñas están sujetas a ataques de repetición, en el que un intruso retransmite una contraseña capturada para obtener acceso a un recurso protegido. Las contraseñas de los usuarios pueden verse comprometidas por el malware que ● captura las pulsaciones del teclado y las transmite a un intruso.
- Algunos usuarios pueden ser implacablemente inteligentes al descubrir formas de evadir las políticas de contraseña que se les imponen.

Debido a que algunas de las debilidades de la autenticación basada en contraseña son causadas por fallas humanas en lugar de fallas tecnológicas, el proceso de fortalecer las contraseñas de los usuarios suele ser educativo. Los administradores pueden diseñar políticas para mitigar algunas debilidades de la contraseña, aunque puede ser difícil instar a los usuarios a cumplirlas.

Por ejemplo, una contraseña de 20 caracteres, generada aleatoriamente, asignada por el administrador sería extremadamente difícil de comprometer para los atacantes, pero podría ser igualmente difícil sofocar la insurrección directa que podría resultar de los usuarios obligados a usarlos. Debido a las complicaciones inherentes al uso de

contraseñas, Microsoft 365 admite otros tipos de mecanismos de autenticación que los administradores pueden usar en lugar de (o junto con) las contraseñas.

Windows Hello para empresas es un mecanismo de autenticación de escritorio que puede reemplazar las contraseñas con certificados o autenticación de pares de claves mediante un PIN o una credencial biométrica, como un escaneo de huellas digitales o un proceso de reconocimiento facial infrarrojo. Microsoft Authenticator es una aplicación de dispositivo móvil que permite a los usuarios iniciar sesión en una cuenta de Microsoft mediante una combinación de mecanismos de autenticación, incluidos PIN, datos biométricos y códigos de acceso únicos (OTP).

***Nota:***

**Protección de identidad**

Para obtener más información sobre la protección de identidades, consulte "Comprender la protección y gestión de identidades", más adelante en este capítulo.

## Documentos

Como se señaló anteriormente en este capítulo, prácticamente todos los mecanismos de seguridad en Microsoft 365 están destinados en última instancia a proteger la información de la empresa, y los documentos son uno de los contenedores principales para esa información. El método tradicional para asegurar documentos es aplicarles permisos de control de acceso. Los permisos toman la forma de listas de control de acceso que se almacenan como

atributos de archivos y carpetas individuales. Un *lista de control de acceso (ACL)* consiste en múltiples *entradas de control de acceso (ACE)*, cada uno de los cuales especifica un principal de seguridad, como un usuario o grupo, y los permisos que otorgan al principal ciertos tipos de acceso al archivo o carpeta.

Los permisos especifican quién puede acceder a los documentos y qué acciones pueden realizar los usuarios. Por ejemplo, un usuario podría leer un documento pero no modificarlo, mientras que otro usuario ni siquiera podría ver que el documento existe. Los permisos han existido durante décadas, y permiten a los usuarios y administradores restringir el acceso a documentos particulares, pero deben aplicarse manualmente y son difíciles de administrar para una gran colección de documentos. Alguien también debe realizar un seguimiento de qué documentos contienen información confidencial que requiere protección adicional.

Por lo tanto, Microsoft 365 incluye mecanismos de seguridad, como Azure Information Protection (AIP) y Data Loss Prevention (DLP), que pueden proteger los documentos de otras formas. El proceso de identificar documentos que contienen datos confidenciales y protegerlos consta de los siguientes cuatro pasos:

- **Descubrimiento** La ubicación de los documentos que contienen información confidencial, ya sea mediante detección automática basada en patrones de datos establecidos o solicitando a los usuarios que apliquen etiquetas de clasificación
- **Clasificación** La aplicación de etiquetas a documentos que contienen

información sensible que indica qué tipos de protección se les debe aplicar

- **Protección** La implementación de mecanismos de seguridad específicos para documentos basados en las etiquetas de clasificación que se les han aplicado
- **Supervisión** El proceso de rastrear tendencias, actividades y eventos de acceso a documentos y tomar medidas cuando sea necesario

El proceso de descubrir documentos que contienen información sensible depende en gran medida de la naturaleza de la organización, los tipos de negocios en los que se dedica y las políticas o regulaciones que debe cumplir. Herramientas como la prevención de pérdida de datos tienen tipos de información confidencial preconfigurados que permiten el descubrimiento automático de documentos que contienen patrones de datos comunes, como números de tarjeta de crédito y de Seguridad Social. Además, los administradores pueden crear tipos de información confidencial personalizados que pueden descubrir documentos que contienen palabras clave específicas basadas en la industria y patrones de datos.

Al igual que una etiqueta física, las etiquetas de sensibilidad proporcionadas por herramientas como AIP y DLP pueden advertir a los usuarios que un documento contiene información confidencial y recomendar que se tomen ciertas medidas. Las etiquetas persisten con los documentos a medida que viajan a diferentes sistemas y se abren en otras aplicaciones de Office, incluso en otras plataformas informáticas. Sin embargo, las etiquetas AIP y DLP también se pueden configurar para aplicar varios tipos de protección, como las que se muestran en Figura 3-10 . los

las etiquetas pueden hacer que los documentos se cifren, tanto en reposo como en tránsito; limitado al uso con aplicaciones específicas; restringido a usuarios o dispositivos específicos; o configurado para caducar e incluso eliminarse después de una vida útil especificada.

## Protect sensitive information across devices, cloud services, and on-premises



**FIGURA 3-10** Mecanismos de protección de documentos de Microsoft 365

Una vez que se completan las fases de clasificación y protección de documentos, los administradores siguen siendo responsables de monitorear los informes y alertas generados por las herramientas de seguridad. Por ejemplo, los intentos repetidos de acceder o compartir documentos protegidos por el mismo usuario o dispositivo pueden indicar la presencia de un

violación de seguridad, incluso si los intentos fallan. El proceso de monitoreo también debe incluir la reparación para que un administrador que advierte un comportamiento anómalo pueda intervenir revocando los privilegios de acceso a documentos o poniendo en cuarentena los archivos.

## Red

El modelo tradicional de seguridad de red requiere la construcción de un perímetro que rodea las instalaciones de la empresa; Este modelo tradicional tiene servidores, estaciones de trabajo y usuarios ubicados dentro del perímetro y firewalls que los protegen al filtrar el tráfico no deseado. Los usuarios remotos pueden conectarse a recursos empresariales solo estableciendo una conexión segura a un servidor de acceso remoto ubicado en una DMZ en la red perimetral. Una instalación de Microsoft 365 coloca recursos sustanciales y potencialmente vulnerables fuera del perímetro en la nube, lo que requiere un modelo de seguridad de red revisado.

Los usuarios remotos aún pueden conectarse a servidores locales para algunas funciones, pero otros se conectarán directamente a servicios en la nube. Además, el nuevo énfasis en los dispositivos móviles significa que los usuarios accederán a los recursos empresariales desde una variedad más amplia de ubicaciones, incluidas las ubicaciones públicas, como hoteles y cafeterías, sobre las cuales la compañía no tiene control.

El proceso de implementación de Microsoft 365 comienza con

una evaluación y posiblemente un rediseño de la red para garantizar que se optimice el ancho de banda de Internet y la proximidad al punto final de la nube de Microsoft más cercano. Además, la adaptación del modelo de seguridad a una infraestructura de red que incluye servicios en la nube requiere un cambio en el énfasis de la seguridad del perímetro a la seguridad del punto final, en el que el enfoque se centra más en asegurar las ubicaciones de los datos y las ubicaciones de los usuarios que acceden a los datos que en el medio de red que los conecta.

*Nota:*

## Microsoft 365

### Despliegue

Para un examen más detallado del proceso de implementación de Microsoft 365, consulte "Comprender el concepto de administración moderna", en Capítulo 2 , " Comprender los servicios y conceptos básicos de Microsoft 365 . "

Si bien el perímetro de seguridad alrededor del centro de datos existente debe permanecer en vigencia, la carga en los firewalls podría disminuir sustancialmente por la migración a los servicios en la nube. En algunos casos, las barreras de firewall pueden tener que debilitarse deliberadamente para permitir que el tráfico de Office 365 llegue a la nube. Sin embargo, esto no significa que los medios estándar para proteger los firewalls en sí, como cambiar sus nombres de usuario y contraseñas administrativas de forma regular, puedan abandonarse.

La seguridad de red de punto final significa que las características de protección integradas en los servicios en la nube de Microsoft 365 asumen un papel más destacado en la estrategia de seguridad empresarial. Los administradores de Microsoft 365 no tienen control sobre el tráfico de red que llega a los servicios en la nube, ni pueden erigir un perímetro alrededor de cada dispositivo remoto o móvil que acceda a los servicios empresariales. Por lo tanto, en lugar de tratar de bloquear el tráfico malicioso con firewalls, la seguridad proviene de mecanismos como la autenticación multifactor, la prevención de pérdida de datos y la seguridad de la aplicación en la nube.

Esto no significa que las redes mismas dejen de ser vulnerables o que puedan quedar desprotegidas. Los administradores deben tener cuidado con las amenazas que siempre han afectado a las redes, incluidas las capturas de paquetes no autorizadas, las redes Wi-Fi sin protección y los puntos de acceso no autorizados. Por ejemplo, si una empresa permite que tanto los dispositivos administrados como los no administrados accedan a los recursos de la compañía, independientemente de las políticas que usen para controlar ese acceso, sigue siendo una buena idea mantener los dispositivos administrados en una red inalámbrica separada de los no administrados. Además, las redes Wi-Fi internas aún deben estar protegidas por protocolos de seguridad y encriptación apropiados, y sus contraseñas administrativas y claves previamente compartidas deben modificarse regularmente.

## Dispositivos

Si una de las dos principales innovaciones de Microsoft 365 es el uso de servicios basados en la nube, el otro es la capacidad de los usuarios de acceder a esos servicios utilizando muchos tipos diferentes de dispositivos que se ejecutan en varias plataformas informáticas y funcionan en cualquier ubicación que tenga Internet acceso. Como se señaló anteriormente, las conexiones VPN han permitido a los usuarios remotos acceder a la red de la compañía desde su hogar o mientras viajan, utilizando una computadora portátil o de escritorio. Las VPN usan una técnica llamada *tunelización* para proteger los datos a medida que se transmiten a través de Internet. En los años posteriores, hubo algunos dispositivos móviles, casi siempre suministrados a los usuarios por la empresa, que podían acceder a una red remota, pero con una utilidad limitada, como el correo electrónico solamente. En la actualidad, Microsoft 365 permite a los usuarios remotos que trabajan con computadoras de escritorio, computadoras portátiles, tabletas y teléfonos inteligentes acceder a prácticamente cualquier servicio o recurso empresarial al que puedan acceder utilizando una estación de trabajo local. El truco, sin embargo, no es solo hacer posible este acceso, sino también hacerlo seguro.

La seguridad del dispositivo en Microsoft 365, por lo tanto, debe abordar dos problemas relativamente nuevos:

- Dispositivos móviles que operan con frecuencia fuera del perímetro de protección de la organización.
- El uso creciente de dispositivos móviles que no son seleccionados y propiedad de la compañía

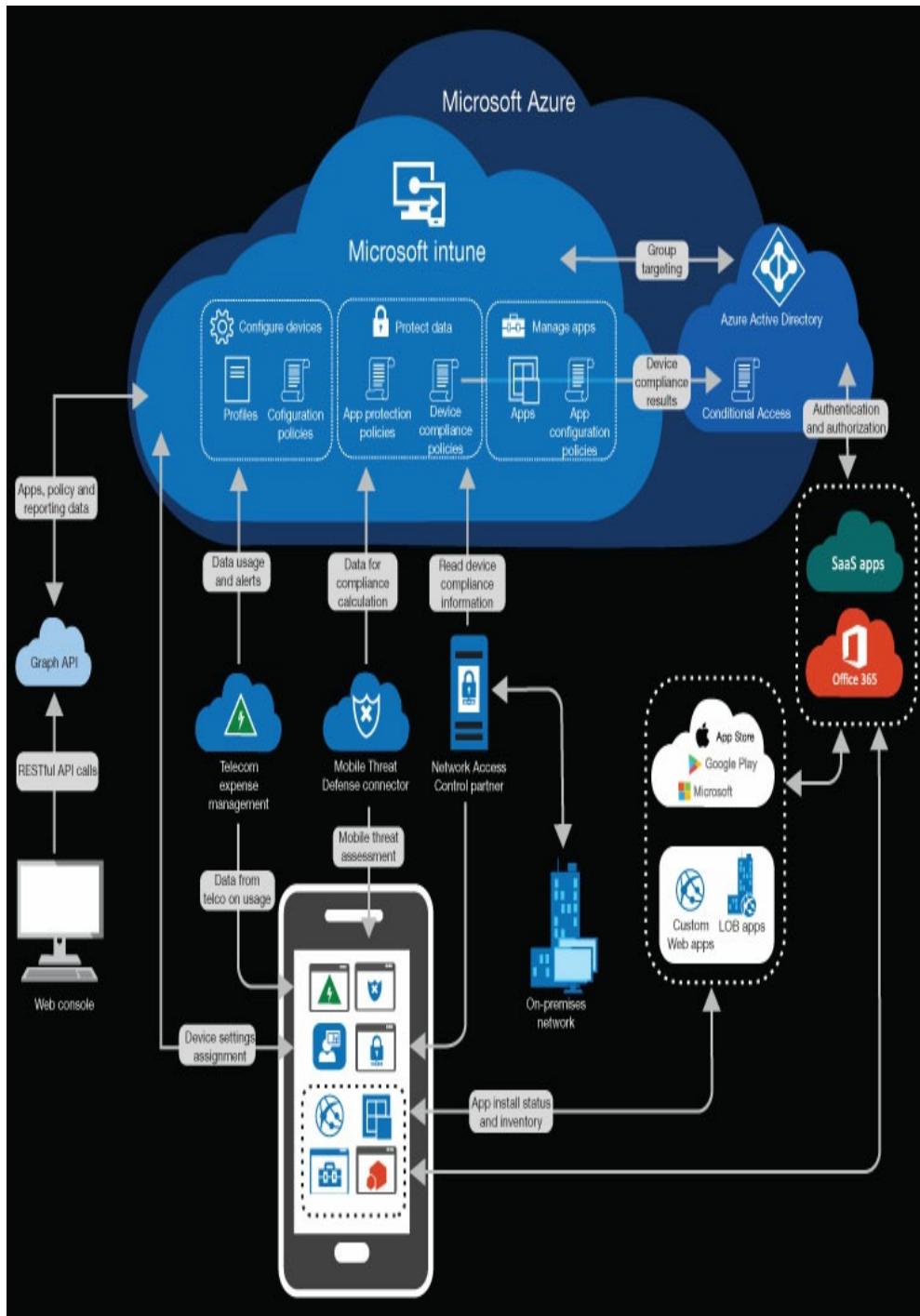
Porque los dispositivos móviles pueden acceder a todos y cada uno

Es importante que exista algún medio para proteger esa información de las amenazas a las que están sujetos todos los dispositivos móviles, incluida la pérdida, el robo y el uso indebido.

Si bien los administradores aún pueden usar las medidas tradicionales de control de acceso, como los permisos del sistema de archivos, para regular quién puede trabajar con los datos confidenciales de la organización, son los servicios Azure Active Directory y Microsoft Intune los principales responsables de garantizar que los dispositivos utilizados para acceder a los datos están a salvo. Microsoft 365 admite una gran cantidad de plataformas de computación móvil, incluidas las siguientes:

- Windows 10
- Android
- Android Enterprise iOS
- macOS
- 

La interacción entre dispositivos móviles y los servicios en la nube de Microsoft 365 es compleja, como se muestra en Figura 3-11 ; sin embargo, como puede ver en el diagrama, Microsoft Intune funciona como un centro de intercambio de información para muchos de estos servicios y usa Azure AD para autenticación y autorización.



**FIGURA 3-11 Arquitectura de servicio de Microsoft Intune**

Aunque la organización podría admitir un BYOD

(Traiga su propio dispositivo) para sus usuarios, es esencial que esos dispositivos estén sujetos a algún tipo de seguridad de punto final empresarial. Esta es la función principal de Microsoft Intune, que es la herramienta de administración de puntos finales de Microsoft 365; Los administradores usan Intune para inscribir los dispositivos de los usuarios y ejercer cierto grado de administración sobre ellos. Al crear políticas de cumplimiento de salud utilizando Intune, se puede verificar el cumplimiento de dichas políticas por parte de los dispositivos inscritos antes de que Azure AD los autorice a acceder a los servicios e información de la empresa. Esto se conoce como *acceso condicional*

Debido a que Azure AD e Intune operan en la nube, pueden funcionar fuera del perímetro de las instalaciones de la empresa, al igual que los dispositivos móviles, y pueden controlar el acceso a los otros servicios de Microsoft 365 desde cualquier ubicación.

El proceso de asegurar los dispositivos comienza con su inscripción usando Microsoft Intune, momento en el cual un administrador debe decidir qué tipo de administración se impondrá en el dispositivo. Mobile Device Management (MDM) le otorga a la organización un control casi completo sobre el dispositivo, lo que requiere que el usuario cumpla con todas las políticas empresariales. MDM incluso permite que un administrador realice un borrado remoto de todo el dispositivo en caso de pérdida o robo, lo que garantiza que los datos confidenciales no se vean comprometidos.

MDM está destinado principalmente para su uso en empresas

dispositivos propios; Puede ser problemático para algunos usuarios a quienes no les guste la idea de otorgar a la organización un control tan completo sobre su propiedad personal. Por ejemplo, las políticas de MDM pueden requerir que los usuarios de teléfonos inteligentes inicien sesión con una contraseña o usen otro mecanismo de autenticación cada vez que usan sus teléfonos, algo que los usuarios pueden encontrar inconveniente.

La alternativa es la Administración de aplicaciones móviles (MAM), que proporciona a los administradores control sobre aplicaciones específicas que se ejecutan en un dispositivo, pero no proporciona control sobre todo el dispositivo en sí. Por ejemplo, una política similar en MAM puede requerir que los usuarios inicien sesión cuando usan Microsoft Exchange para acceder a su correo electrónico, pero no tienen que iniciar sesión cada vez que encienden sus teléfonos. MAM también permite a los administradores borrar los datos de la empresa del teléfono, pero solo se pueden borrar los datos asociados con las aplicaciones administradas.

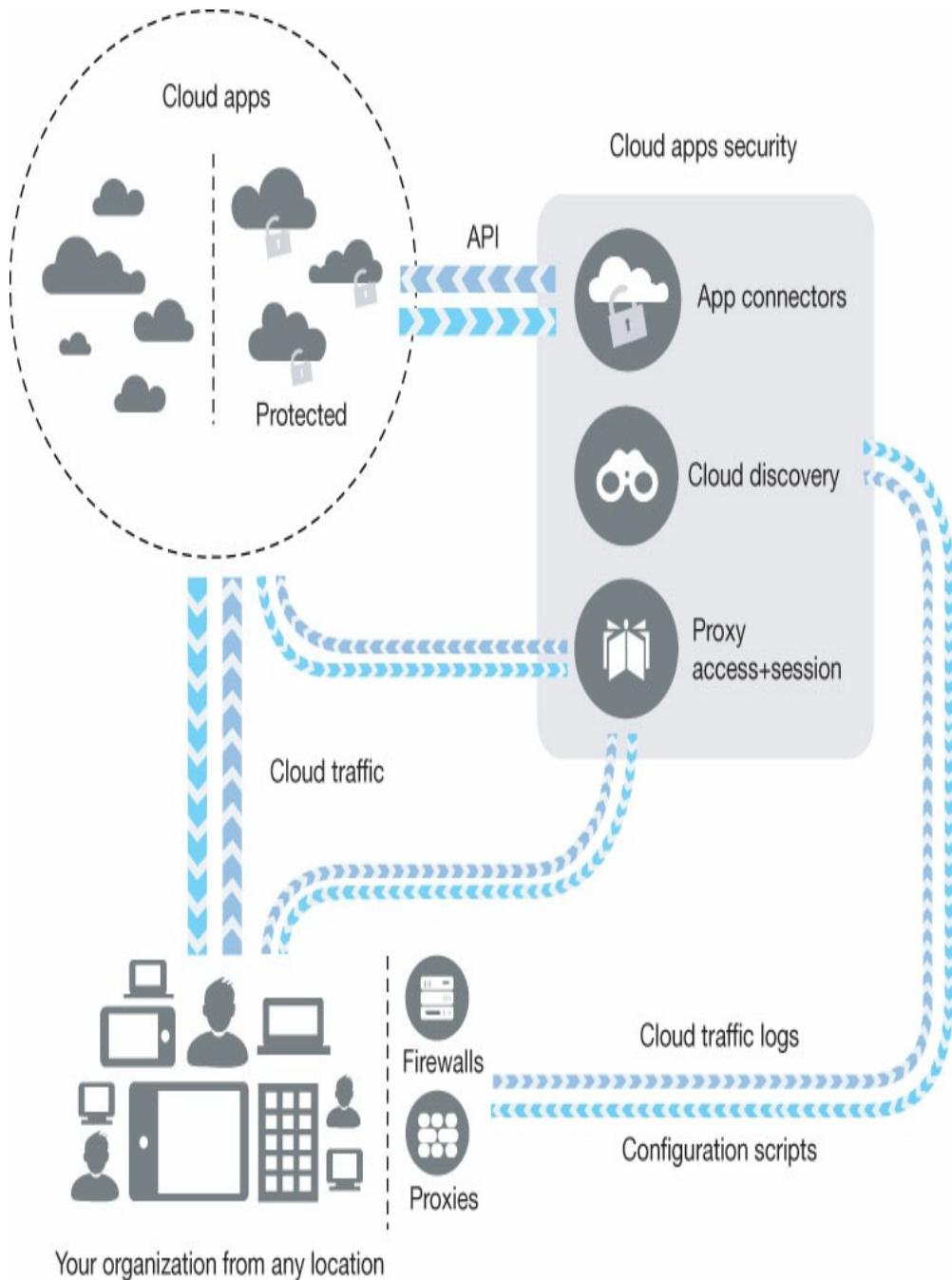
Cloud App Security es otra herramienta de Microsoft 365 para dispositivos móviles y otros; Cloud App Security es una aplicación de agente de seguridad de acceso a la nube que escanea los recursos de red para detectar las aplicaciones en la nube que los usuarios están ejecutando, y detecta los productos no autorizados de Infraestructura como servicio (IaaS) y Plataforma como servicio (PaaS) que podrían estar en uso. El objetivo aquí es detectar "TI en la sombra", es decir, aplicaciones en la nube que no tienen

aprobado por el departamento de TI y que podría ser una amenaza para la seguridad de la red empresarial.

Cloud Discovery es el proceso mediante el cual Cloud App Security examina los registros de tráfico de firewalls y servidores proxy y compara la información con el catálogo de aplicaciones en la nube de Microsoft, que contiene más de 16,000 aplicaciones en la nube. El catálogo incluye una evaluación de cada aplicación como una amenaza potencial, y los puntajes se basan en más de 70 factores de riesgo.

Una vez que Cloud App Security ha compilado un informe de las aplicaciones en la nube que se están utilizando, los administradores pueden sancionar las aplicaciones que desean que los empleados usen y anular las que no quieren que usen. Para las aplicaciones autorizadas, Cloud App Security admite el uso de API proporcionadas por los proveedores de aplicaciones en la nube. Estas API permiten que Cloud App Security funcione como intermediario entre las aplicaciones en la nube y los usuarios de la empresa, como se muestra en

Figura 3-12 , accediendo a registros de actividad, cuentas de usuario y fuentes de datos. Cloud App Security puede usar esta información para monitorear el uso, aplicar políticas y detectar amenazas.



**FIGURA 3-12** Interacciones de Cloud App Security con una red empresarial y aplicaciones en la nube

### **Comprobación rápida**

- ¿Cuál de los siguientes no es uno de los cuatro pilares de seguridad clave que protegen la infraestructura empresarial?
  - Documentos de
  - identidad
  - Dispositivos en la
  - nube

### **Respuesta de verificación rápida**

- La nube no es uno de los cuatro pilares clave de seguridad. El cuarto pilar correcto es la red.

## **HABILIDAD 3.2: ENTENDER LA PROTECCIÓN Y LA GESTIÓN DE LA IDENTIDAD**

---

Las identidades son el problema de seguridad fundamental en Microsoft 365 o en cualquier entorno de red. Las identidades son las puertas y ventanas que proporcionan entrada y salida al entorno de red empresarial. Son esenciales si alguien va a poder utilizar la información almacenada por los servicios empresariales. Por lo tanto, proteger esas identidades del uso indebido es una prioridad principal en el diseño, implementación y mantenimiento de una red empresarial.

Una identidad es una representación lógica de un usuario en un entorno de red. Para los usuarios, una identidad es un nombre que escriben para iniciar sesión en la red, junto con una contraseña o algún otro medio de autenticación. Para los administradores, una identidad es una colección de atributos asociados con un individuo en particular, como se muestra en

**Figura 3-13 .** El nombre de inicio de sesión es uno de esos atributos, pero puede haber muchos otros, incluida información personal, como la dirección de su casa, número de teléfono, cargo, etc.

The screenshot shows the 'Sanjay Patel - Profile' page in the Azure portal. The left sidebar lists various management sections: Profile (selected), Directory role, Groups, Applications, Licenses, Devices, Azure resources, Authentication methods, Sign-ins, Audit logs, Troubleshooting + Support, Troubleshoot, and New support request. The main content area displays the user's profile details under the 'Profile' tab. Key information includes:

Name	First name	Last name
Sanjay Patel	Sanjay	Patel
User name	User type	
sanjaypatel@olivercox.onmicrosoft.com	Member	
Object ID	Source	
77e8ffcf-899c-41e6-91eb-0...	Azure Active Directory	

Below this, there are sections for Job info, Settings, and Contact info, each with edit links. The Contact info section contains:

Street address	State or province	Country or region
123 Broadway	NY	USA
City	ZIP or postal code	Office phone
New York	10012	+1 2125551112

### **FIGURA 3-13 Atributos de usuario en el Centro de administración de Azure**

#### Active Directory

Una identidad también incluye típicamente una lista de los grupos a los que el individuo es miembro. Los administradores usan grupos para asignar derechos y permisos a individuos. Cuando a un grupo se le asignan derechos y permisos para acceder a los recursos de la red, todos los miembros del grupo heredan automáticamente esos derechos y permisos. Esta es una alternativa eficiente para asignar múltiples derechos y permisos a cada identidad de usuario individualmente.

## **Identidades**

Cada computadora o dispositivo móvil tiene la capacidad de mantener la identidad de un usuario y emplearla para proteger el acceso del dispositivo a cualquier otra persona. Sin embargo, cuando un usuario desea acceder a aplicaciones, servicios o datos desde la red de su empresa, se necesita otra identidad; Los administradores de la red crean y mantienen esta identidad y la almacenan en la propia red, no en la computadora del usuario u otro dispositivo.

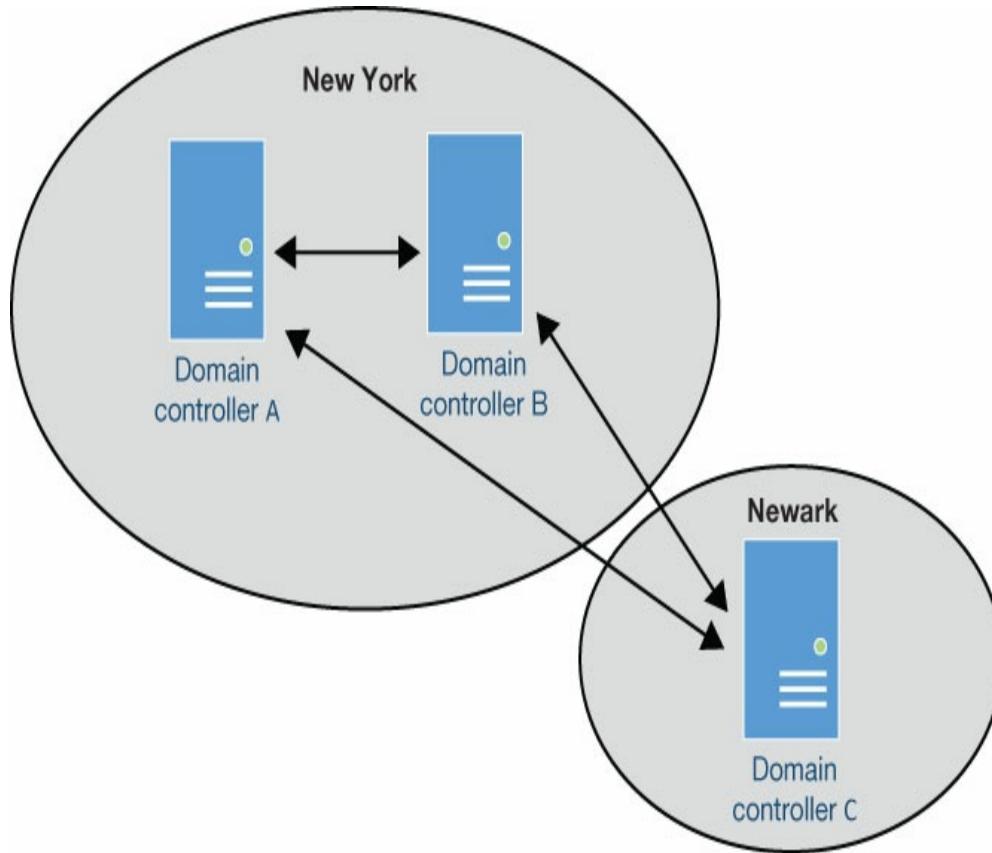
## **Identidades locales**

A partir de la versión de Windows 2000 Server, las identidades empresariales se almacenaron en Active Directory, que es un servicio de directorio local que todavía es un

parte del producto Windows 2019 Server, aunque ahora se llama Servicios de dominio de Active Directory (AD DS). La instalación de la función AD DS en una computadora que ejecuta Windows Server le permite funcionar como un controlador de dominio, que contiene una base de datos orientada a objetos de identidades de usuario y otros recursos de red, incluidos grupos, computadoras y aplicaciones. AD DS es una base de datos jerárquica basada en el dominio que utiliza objetos de unidades organizativas y contenedores para separar a los usuarios y otros recursos en colecciones lógicas, que generalmente representan las divisiones departamentales o geográficas de la empresa.

Por lo general, las redes empresariales tienen múltiples controladores de dominio, que los administradores configuran para sincronizar los contenidos de sus bases de datos AD DS entre sí, con fines de tolerancia a fallas y alta disponibilidad. AD DS utiliza la replicación maestra múltiple, lo que significa que los administradores pueden crear o modificar usuarios y otros objetos en cualquier controlador de dominio, y los cambios se replicarán en todos los demás controladores de dominio, como se muestra en **Figura 3-14**.

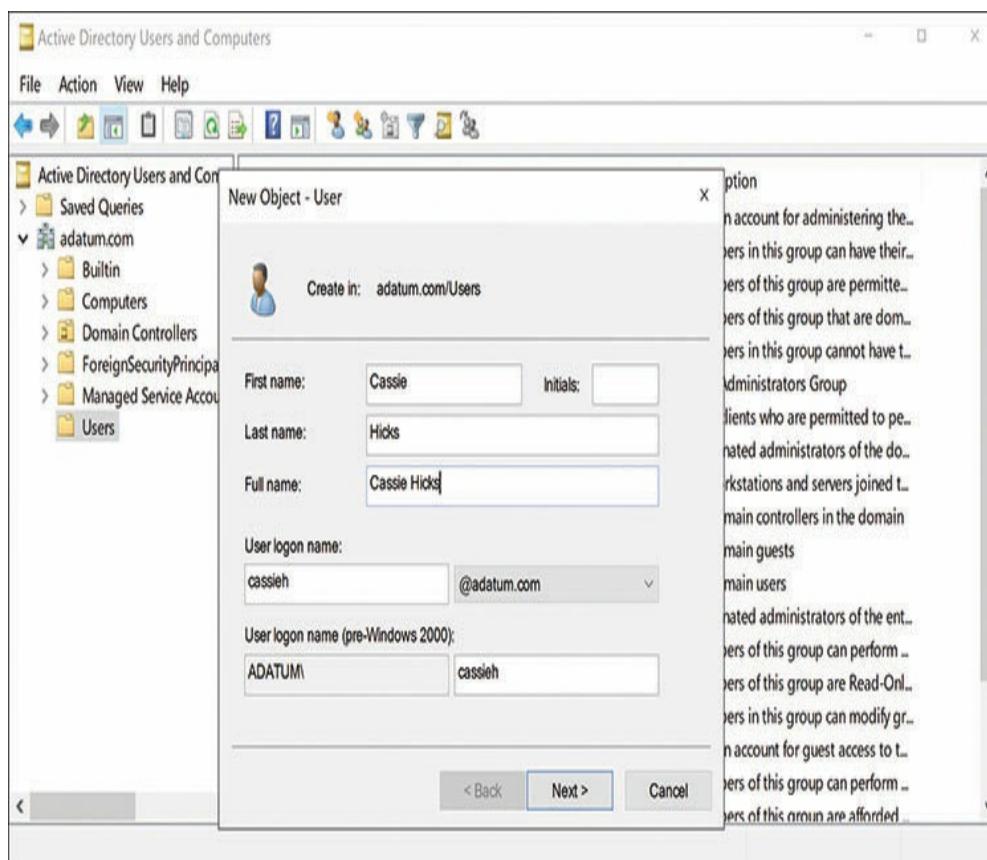
---



**FIGURA 3-14** Servicios de dominio de Active Directory replicación maestra múltiple

Los administradores pueden crear objetos de usuario de AD DS utilizando herramientas gráficas, como Usuarios y equipos de Active Directory, como se muestra en **Figura 3-15** o herramientas de línea de comandos, como el *New-ADUser* cmdlet en Windows PowerShell. Los objetos de usuario en AD DS son estrictamente *Identidades locales*. Los controladores de dominio deben ubicarse dentro del perímetro de la red y no son accesibles directamente desde Internet. Cuando los usuarios acceden a recursos locales, sus identidades se autentican

y autorizado por el controlador de dominio más cercano, que utiliza un protocolo llamado Kerberos para realizar un complicado procedimiento de autenticación basado en tickets. Los usuarios fuera del perímetro de la red solo pueden iniciar sesión en AD DS en la red estableciendo una conexión VPN a un servidor de acceso remoto. Esto proporciona a los usuarios una presencia en la red interna, lo que les permite acceder a los recursos internos.



**FIGURA 3-15** El nuevo objeto: cuadro de diálogo Usuario en la consola de Usuarios y equipos de Active Directory

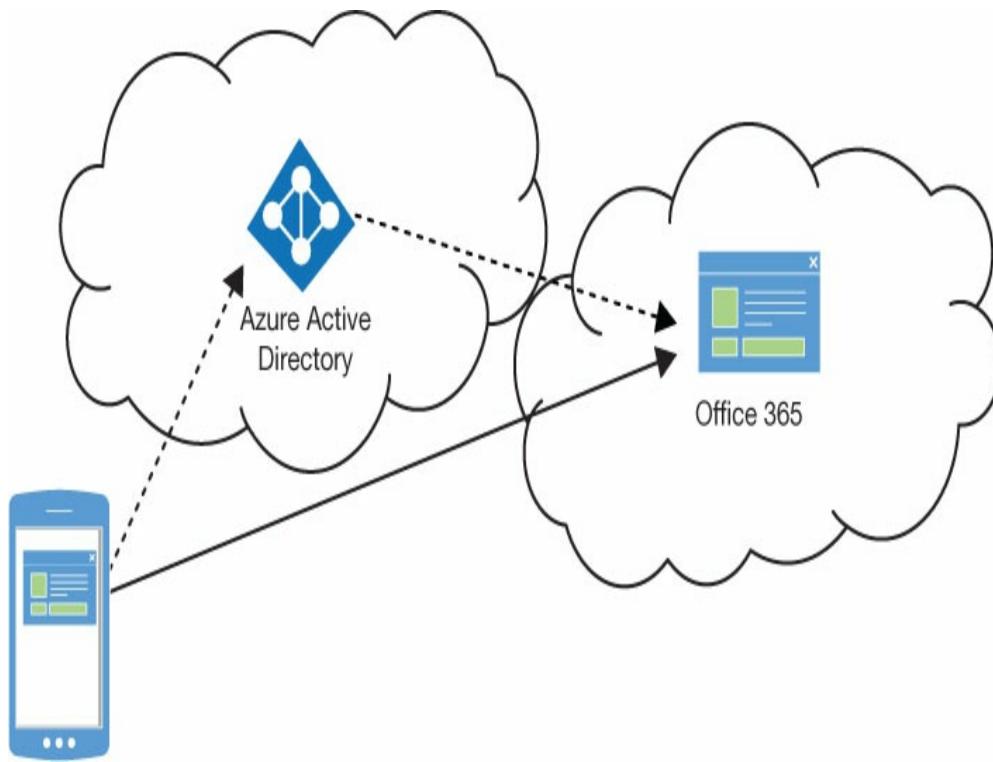
#### Identidades de la nube

Debido a que AD DS solo puede realizar sus funciones cuando el usuario y los recursos a los que se accede están ubicados en las instalaciones, no es una solución viable para aplicaciones y servicios basados en la nube. Por lo tanto, Microsoft tuvo que idear una solución alternativa de autenticación y autorización para sus productos basados en la nube, como Microsoft 365. Esta solución es Azure Active Directory (Azure AD), una alternativa (o complemento) de servicio de directorio basado en la nube a AD DS en qué administradores crean

*identidades de nubes*

Microsoft 365 confía en el servicio Azure Active Directory para la administración de su identidad, y todos los servicios de Microsoft 365 usan Azure AD para autenticación y autorización. Los suscriptores de Microsoft 365 (así como los suscriptores de Office 365 y Windows Azure) se convierten en inquilinos de Azure AD automáticamente. Cuando un usuario accede a una aplicación de Office 365 en la nube, como se muestra en

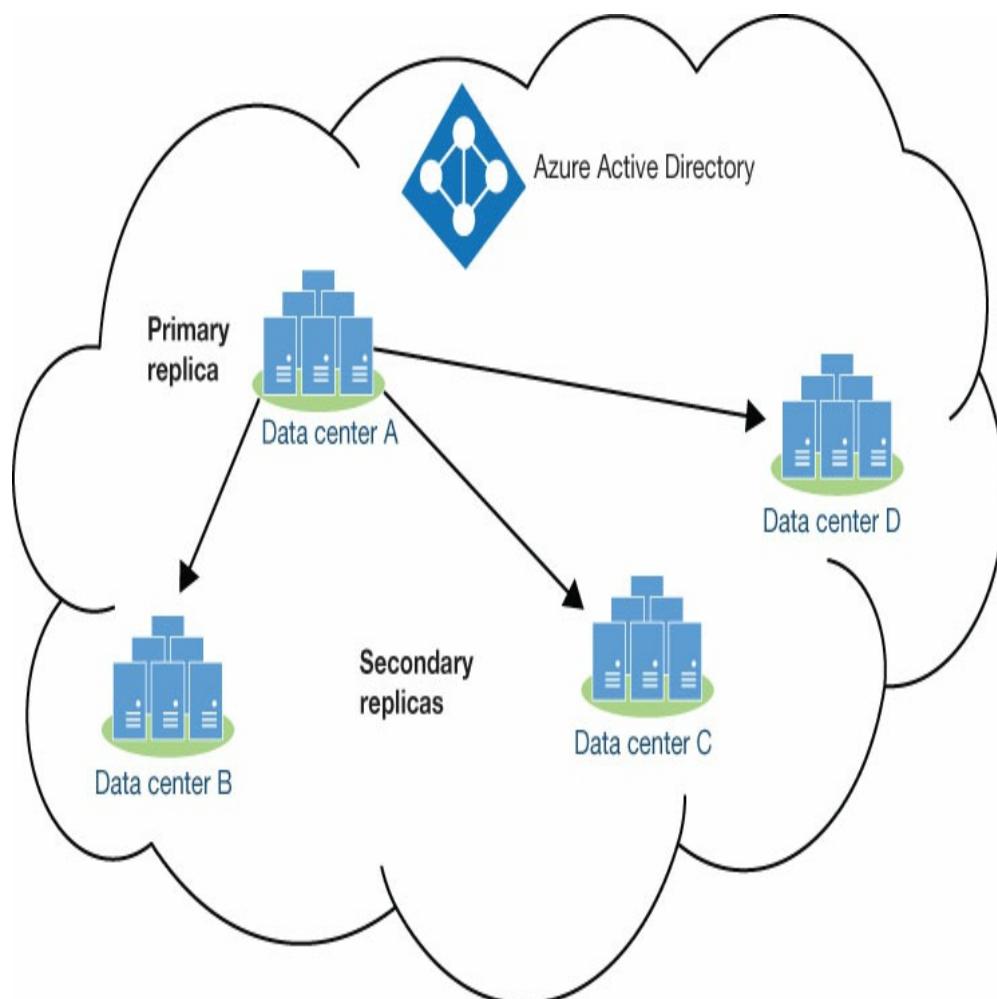
**Figura 3-16 , Azure AD es el intermediario invisible que confirma la identidad del usuario con los mecanismos de autenticación que los administradores de Microsoft 365 han seleccionado. Del mismo modo, Azure AD autoriza el acceso del usuario a la aplicación y a los archivos que el usuario abre en la aplicación.**



**FIGURA 3-16** Azure Active Directory proporciona servicios de autenticación y autorización para aplicaciones y servicios de Microsoft 365

A diferencia de AD DS, no es necesario que los administradores instalen varios controladores de dominio para Azure AD o configuren la replicación de directorios. Una tenencia de Azure AD se replica automáticamente en varios centros de datos en la red global de Microsoft. Además, a diferencia de AD DS, Azure AD usa un solo modelo de replicación maestra. Solo hay una réplica principal de un inquilino de Azure AD, y todos los usuarios nuevos y las modificaciones de la cuenta se escriben en esa réplica principal. Los cambios se replican automáticamente en múltiples réplicas secundarias en diferentes

centros de datos, como se muestra en Figura 3-17. Todas las solicitudes de lectura entrantes son manejadas por las réplicas secundarias, utilizando la réplica más cercana al usuario, la aplicación o el servicio solicitante. Como hay muchas réplicas secundarias, el servicio Azure AD siempre está disponible. Debido a que solo hay una réplica principal, funciona de manera diferente mediante el uso de un procedimiento de conmutación por error determinista.



**FIGURA 3-17** Replicación maestra única de Azure Active Directory

Para crear usuarios en Azure AD, los administradores pueden usar varias herramientas diferentes, incluido el Centro de administración de Microsoft 365 y el Centro de administración de Azure Active Directory. La autenticación y autorización de Azure ID también se basan en tokens, pero los protocolos y procedimientos que usa Azure AD son diferentes de los que usa AD DS. En lugar de Kerberos, Azure AD usa OAuth 2.0 u OpenID Connect.

## Identidades híbridas

Es importante comprender que Azure Active Directory no pretende ser un reemplazo de los Servicios de dominio de Active Directory, ni son intercambiables. Si una organización tiene servidores internos y una implementación local de AD DS, no debe esperar poder migrar sus identidades de usuario de AD DS a Azure AD y luego desaprobar sus controladores de dominio AD DS. Es igualmente importante comprender que Microsoft 365 requiere Azure AD; No es posible utilizar las identidades de AD DS para autenticar y autorizar a los usuarios para las aplicaciones y servicios de Microsoft 365. Lo contrario también es cierto; no es posible usar las identidades de Azure AD para proporcionar servicios de autenticación y autorización para recursos locales.

Sin embargo, es posible usar Azure AD y AD DS juntos, creando lo que se conoce como identidades híbridas. UNA *identidad híbrida* es una cuenta de usuario que existe tanto en

Directorios de Azure AD y AD DS con el mismo conjunto de atributos. El escenario habitual para el uso de identidades híbridas es una organización que tiene una infraestructura AD DS existente, pero que está considerando una expansión en la nube mediante el uso de productos de Software como Servicio (SaaS), como Office 365. La organización podría tener cientos o miles de identidades locales, pero la posibilidad de tener que volver a crearlas en Azure AD y luego mantener dos identidades para cada usuario podría ser un factor decisivo en la organización que elige no usar servicios en la nube.

Las identidades híbridas son una solución a este problema. Debido a que se supone que las identidades de AD DS ya existen, la creación de identidades híbridas es una cuestión de sincronizarlas de AD DS a Azure AD. Para hacer esto, los administradores deben instalar una herramienta llamada Azure AD Connect en la red local, que accede al directorio de AD DS en un controlador de dominio y replica todas las cuentas de usuario que encuentra en Azure AD (junto con sus contraseñas y otros atributos) .

***Nota:***

**primero**

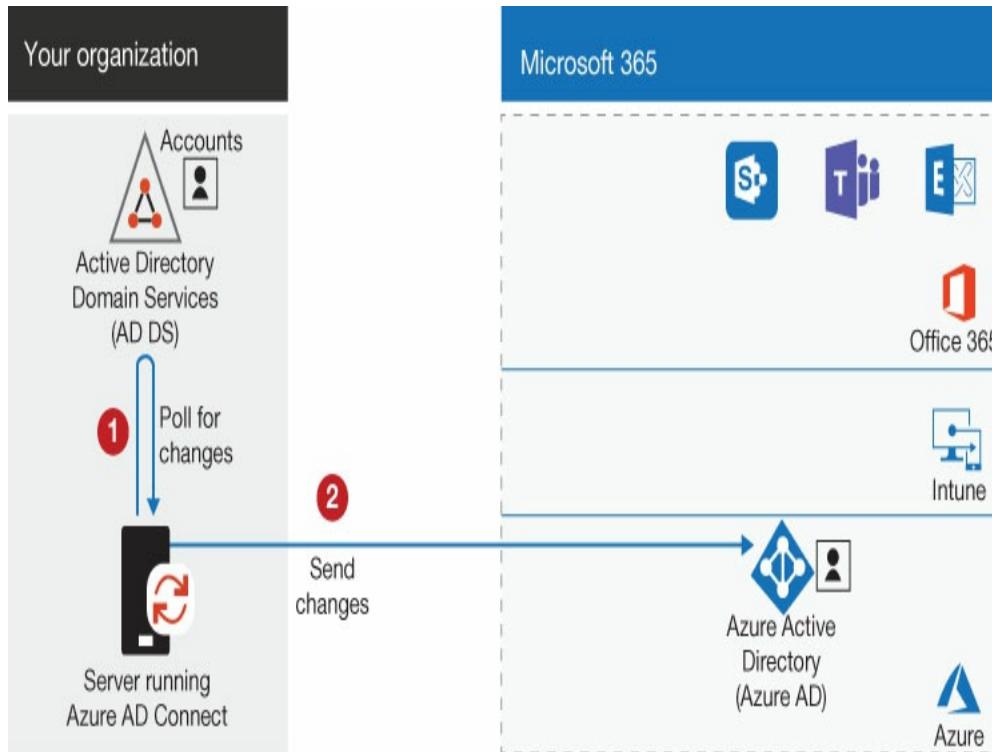
## **Sincronización**

**Cuando Azure AD Connect sincroniza las identidades locales de AD DS con Azure AD por primera vez, se crean nuevas identidades en la nube para los usuarios, pero las licencias de los productos no se les asignan automáticamente. Por lo tanto, en un nuevo**

**Implementación de identidad híbrida de Microsoft 365, los administradores deben agregar licencias de Microsoft 365 a los usuarios en Azure AD después de que se complete la primera sincronización. Los administradores pueden agregar licencias a los usuarios de Azure AD individualmente, pero el proceso también se puede realizar dinámicamente haciendo que la asignación de la licencia sea el resultado de la pertenencia a un grupo.**

Las contraseñas en AD DS se almacenan como un hash (un algoritmo matemático unidireccional que no se puede revertir para extraer la contraseña) y, de manera predeterminada, Azure AD Connect aplica otro algoritmo hash al hash AD DS. Por lo tanto, la contraseña transmitida por Azure AD Connect a la nube está asegurada por ser un hash de un hash. Las contraseñas en Azure AD nunca se almacenan en texto sin formato, ni se cifran con un algoritmo reversible.

Después de la sincronización inicial, Azure AD Connect continúa detectando los cambios realizados en las identidades de AD DS y replica esos cambios en las identidades de Azure AD correspondientes en la nube, como se muestra en Figura 3-18 . Por lo tanto, los administradores que administran identidades híbridas deben usar las herramientas de AD DS, como Usuarios y equipos de Active Directory, para realizar cambios en las cuentas de usuario locales. Debido a que la replicación de identidad fluye en una sola dirección, desde AD DS a Azure AD, nadie debe realizar cambios directamente en las identidades de la nube utilizando las herramientas de Microsoft 365.



**FIGURA 3-18** Sincronización de identidad de Azure AD

Connect

*Nota:*

## Azure AD

### Proxy de aplicación

Si bien Azure AD no reemplaza a AD DS, puede proporcionar a los usuarios remotos acceso a aplicaciones web internas mediante una función llamada Proxy de aplicación. Application Proxy consiste en un servicio que se ejecuta en la nube y un conector que los administradores instalan en un servidor local. Cuando los clientes remotos intentan acceder a la aplicación web interna con una URL, son dirigidos a una página de inicio de sesión de Azure AD, donde se autentican mediante una identidad de Azure AD. Luego, los clientes pasan el token que recibieron como resultado del inicio de sesión al Servicio de proxy de aplicación, que lo reenvía a

**Application Proxy Connector en la red interna. El conector reenvía la solicitud del usuario a la aplicación web interna, que devuelve su respuesta al cliente a través del conector y el Servicio de proxy de aplicación.**

Las identidades híbridas pueden simplificar el proceso de administración de identidad para los administradores, pero también pueden simplificar la experiencia del usuario. Para los administradores que agregan servicios en la nube a una infraestructura local existente, el objetivo principal debe ser hacer que el acceso de los usuarios a las aplicaciones en la nube sea lo más invisible posible. Una forma de hacer esto es implementar *inicio de sesión único (SSO)* para que los usuarios puedan autenticarse con sus credenciales conocidas de AD DS y recibir acceso a los servicios en la nube sin tener que iniciar sesión nuevamente, ya sea en el nivel de Azure AD o en las aplicaciones individuales. Otra opción, llamada *inicio de sesión único sin interrupciones*, permite a los usuarios conectados a la red empresarial iniciar sesión automáticamente sin ninguna autenticación interactiva. El inicio de sesión sin interrupciones es compatible con los métodos de sincronización de contraseña y autenticación de paso, pero no es compatible con el método de autenticación federado.

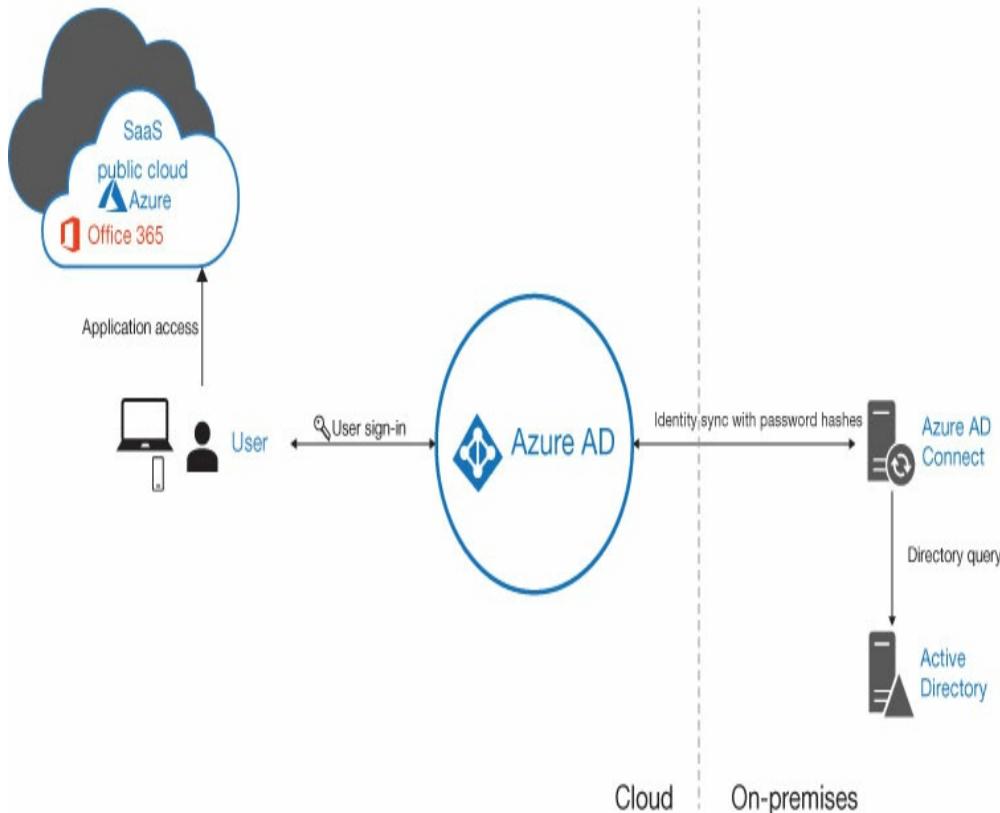
Durante el proceso de instalación de Azure AD Connect, un administrador debe seleccionar el método de autenticación que Azure AD usará para proporcionar acceso a los usuarios

a la nube de recursos. Hay tres opciones para elegir, de la siguiente manera:

- **Sincronización de hash de contraseña de Azure AD** La forma más simple de los métodos de autenticación de Azure AD Connect, que no requiere infraestructura adicional para implementar. Azure AD Connect crea un hash del hash de contraseña de AD DS de cada usuario y lo aplica a la identidad de ID de Azure correspondiente. Esto permite a los usuarios acceder a los recursos locales y en la nube utilizando la misma contraseña, como se muestra en

Figura 3-19 . Azure AD Connect actualiza las contraseñas de identidad en la nube cada dos minutos  
sin interrumpir una sesión en curso cuando se produce un cambio de contraseña. Debido a que el modelo de sincronización de hash de contraseña se implementa completamente en la nube, comparte la alta disponibilidad de los otros servicios en la nube de Microsoft. Para garantizar un funcionamiento continuo, Microsoft recomienda la instalación de Azure AD Connect en dos o más servidores en espera, preferiblemente en diferentes ubicaciones.

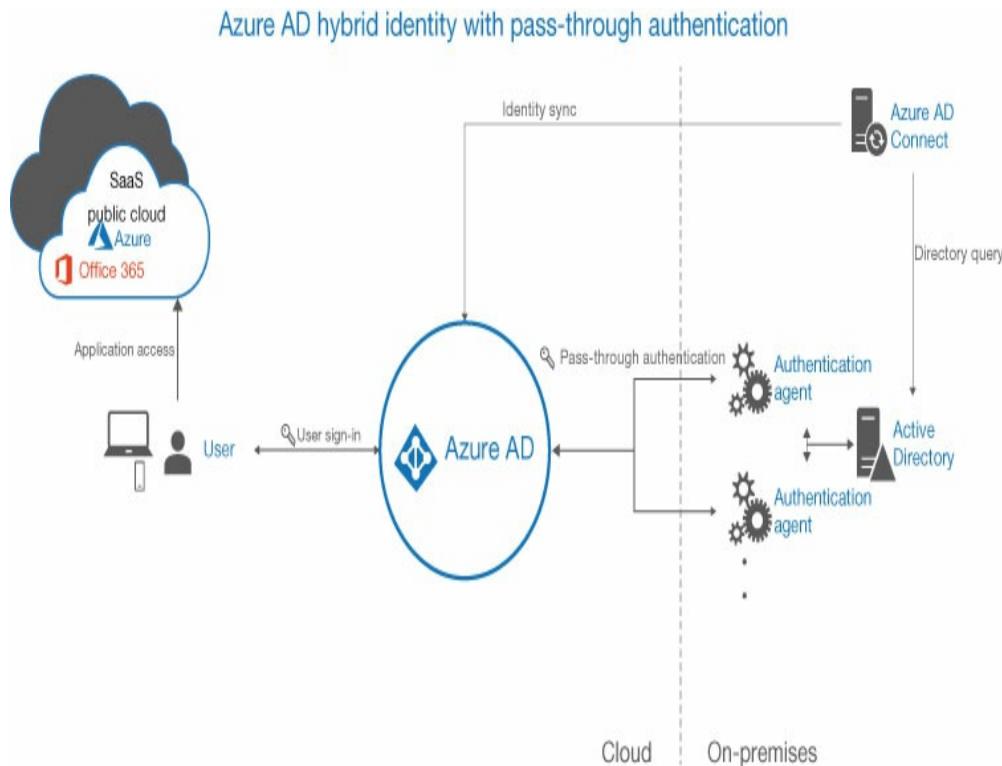
## Azure AD hybrid identity with password hash sync



**FIGURA 3-19** Sincronización de hash de contraseña de Azure AD

- **Autenticación de paso de Azure AD** Evita toda validación de contraseña basada en la nube mediante el uso de un agente de autenticación de paso ligero instalado en servidores locales. (Microsoft recomienda tres). Cuando los usuarios inician sesión en Azure AD, sus solicitudes se reenvían al agente, que las envía a su vez (en forma cifrada) a un controlador de dominio para validar a los usuarios contra sus identidades locales en AD DS , como se muestra en **Figura 320** . Los agentes solo requieren acceso saliente a Internet y acceso a un controlador de dominio AD DS , por lo que no pueden ubicarse en una red perimetral. El resultado final es la misma experiencia de usuario que la sincronización de hash de contraseña, pero este método evita el almacenamiento de contraseñas de usuario en la nube en cualquier forma y permite

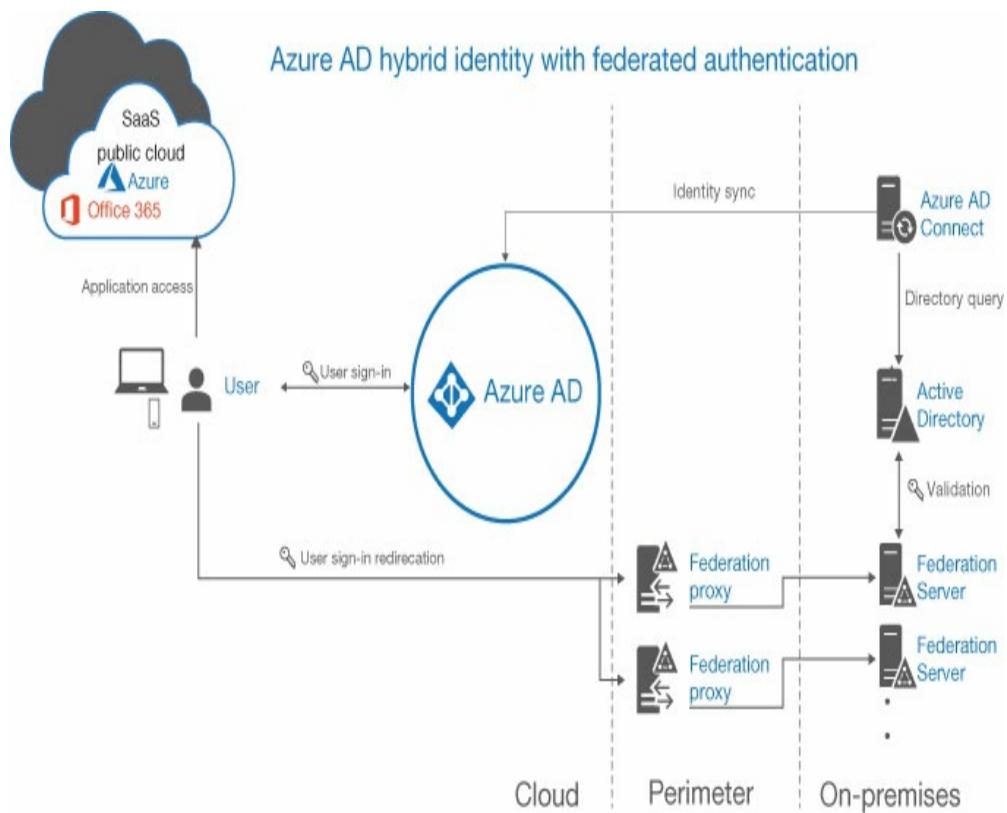
administradores para aplicar políticas de seguridad de Active Directory locales, como cuentas deshabilitadas o caducadas, y permite el horario de inicio de sesión y cumple con los requisitos de seguridad contratados. También es posible implementar la sincronización de hash de contraseña además de la autenticación de paso para funcionar como una copia de seguridad en caso de una falla local que impide que los agentes funcionen.



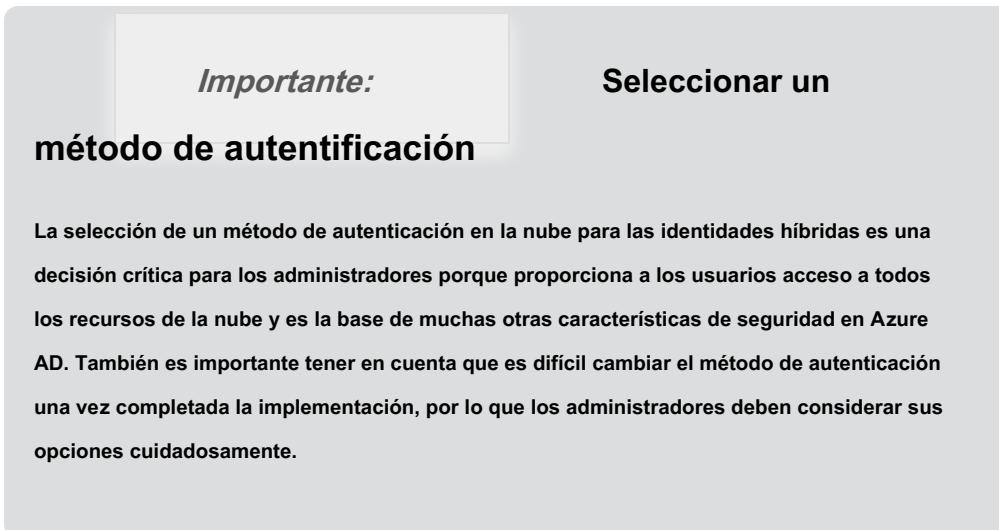
**FIGURA 3-20 Autenticación de paso de Azure AD**

- **Autenticación Federada** Descarga el proceso de autenticación a una solución externa en la que la organización confía, como los Servicios de federación de Active Directory de Microsoft (AD FS). La configuración y gestión del proceso de autenticación, así como la experiencia del usuario, son responsabilidad del sistema federado; Azure AD no está involucrado. Según los requisitos de seguridad de la organización, el proceso de inicio de sesión con el sistema federado puede ser más simple o más complicado que el de Azure AD. El sistema federado generalmente consiste en un clúster de servidores con equilibrio de carga, denominado

una granja, para fines de alta disponibilidad y tolerancia a fallas. Debido a que los servidores de federación requieren acceso a los controladores de dominio de Azure AD y AD DS, los propios servidores (o intermediarios proxy) deben ubicarse en la DMZ de una red perimetral local, como se muestra en **Figura 3-21**. Las organizaciones suelen optar por la opción de autenticación federada porque desean (o se ven obligadas a) usar un método de autenticación que Azure AD no admite, como certificados o tarjetas inteligentes. El hardware, el software y la infraestructura administrativa adicionales que requiere el método de autenticación federado pueden ser un gasto adicional significativo; En muchos casos, las organizaciones que eligen esta opción lo hacen porque ya han invertido en la infraestructura. También es posible implementar la sincronización de hash de contraseña además de la autenticación federada, de modo que funcione como una copia de seguridad en caso de una falla local que impida el funcionamiento de los servidores de federación o sus servidores proxy.



**FIGURA 3-21 Autenticación federada**



## Autenticación

Si las identidades son las puertas y ventanas en el entorno de red empresarial, las autenticaciones son las cerraduras que las mantienen seguras. Un administrador puede otorgar a un usuario específico los permisos necesarios para acceder a un archivo, una aplicación o un servicio, pero esto no significa nada a menos que haya alguna forma de garantizar que la persona que usa esos permisos sea realmente la persona a quien se le asignó. La autenticación es cómo los individuos realmente prueban sus identidades.

Hay tres medios básicos para autenticar la identidad de un individuo. El individuo debe suministrar uno o más de los siguientes:

- **Algo que sabes** Una información que solo el

posee individualmente, como una contraseña o PIN

- **Algo que eres** Una característica que es exclusiva del individuo, como una huella digital o un escaneo facial
- **Algo que tienes** Un elemento único que posee el individuo, como una tarjeta de identificación o un teléfono inteligente

## Autenticación de contraseña

Una contraseña es *algo que sabes* y este ha sido el medio estándar para autenticar las identidades de los usuarios durante muchos años. La autenticación de contraseña no cuesta nada de implementar, y puede ser relativamente segura. Sin embargo, hay muchos defectos posibles en el modelo de autenticación de contraseña. Por ejemplo, las contraseñas pueden olvidarse, compartirse, anotarse, adivinarse fácilmente o ser demasiado simples.

Para evitar que los usuarios creen contraseñas que brinden muy poca seguridad, existen políticas que especifican reglas para la creación y mantenimiento de contraseñas. Los sistemas operativos y los servicios de directorio, como Azure AD y AD DS, incluyen herramientas que los administradores pueden usar para crear y aplicar dichas políticas.

En Azure AD, las cuentas de usuario están sujetas a las siguientes políticas de contraseña:

- **Personajes permitidos** Especifica los caracteres que los usuarios pueden usar al crear contraseñas, incluidos los caracteres alfabéticos en mayúsculas y minúsculas, números, espacios en blanco y la mayoría de los símbolos.
- **Restricciones de contraseña** Especifica que las contraseñas deben tener de 8 a 256 caracteres y deben contener tres de los siguientes cuatro

tipos de caracteres: mayúsculas, minúsculas, números y símbolos.

- **Duración de caducidad de contraseñas** Especifica que las contraseñas caducan en 90 días de forma predeterminada. El valor puede modificarse utilizando el *Set-MsolUser* Cmdlet de PowerShell.
- **Notificación de caducidad de contraseña** Especifica que el usuario recibirá una notificación de caducidad de la contraseña 14 días antes de que la contraseña caduque. El valor puede modificarse utilizando el *Set-MsolPasswordPolicy* Cmdlet de PowerShell.
- **Caducidad de contraseña** Especifica un valor predeterminado de Falso, lo que indica que la contraseña caducará después del intervalo de duración de caducidad de Contraseñas. El valor puede modificarse utilizando el *Set-MsolUser* Cmdlet de PowerShell.
- **Historial de cambio de contraseña** Especifica que los usuarios no pueden reutilizar la misma contraseña al cambiar las contraseñas.
- **Historial de restablecimiento de contraseña** Especifica que los usuarios pueden reutilizar la misma contraseña cuando restablecen una contraseña olvidada.
- **Bloqueo de cuenta** Hace que los usuarios se bloquen de sus cuentas durante un minuto después de 10 intentos de inicio de sesión fallidos pero únicos. Intentos fallidos adicionales resultan en intervalos de bloqueo más largos.

En AD DS, los administradores pueden configurar la contraseña mediante la directiva de grupo. Las configuraciones disponibles tienen nombres ligeramente diferentes, pero sus funciones son esencialmente las mismas.

Estas políticas de contraseña están diseñadas para evitar que los usuarios creen contraseñas que sean demasiado simples por conveniencia, pero la seguridad de la contraseña es difícil de aplicar para los administradores. Los usuarios aún pueden crear contraseñas que serían fáciles de adivinar para los atacantes usando, por ejemplo, los nombres y cumpleaños de sus hijos. Tampoco hay una configuración de software que pueda evitar que los usuarios

de escribir sus contraseñas o compartirlas con sus compañeros de trabajo.

A medida que las amenazas a la seguridad de la red se vuelven cada vez más graves, los administradores han buscado formas de mejorar la seguridad del proceso de autenticación. Ha habido métodos de autenticación alternativos disponibles durante muchos años, que posiblemente podrían aumentar o reemplazar las contraseñas, pero hasta hace relativamente poco tiempo, estas tecnologías eran demasiado caras o inconvenientes para ser prácticas para la base de usuarios promedio. Sin embargo, la mayor necesidad de protección de identidad ha llevado estas tecnologías de autenticación a un mercado más amplio, lo que resulta en precios más bajos y la necesidad aumenta constantemente. Microsoft 365 incluye la capacidad de mejorar la seguridad del proceso de autenticación de varias maneras.

## Autenticación multifactorial

La autenticación multifactor es un procedimiento en el que los usuarios prueban sus identidades de dos o más formas. Por lo general, además de una contraseña: *algo que sabes*—Proporcionan un factor de autenticación diferente: *algo que eres* o *algo que tienes*

### ALGO QUE ERES

los *algo que eres* Suele ser algún tipo de exploración biométrica. La característica Windows Hello para empresas en Windows 10 admite la autenticación multifactor con

escaneos biométricos como uno de los factores. También es posible usar la aplicación Microsoft Authenticator para dispositivos móviles como un escáner biométrico que permite a los usuarios acceder a los recursos de Microsoft 365 sin contraseña.

Los lectores de huellas digitales son económicos y se están convirtiendo en una característica cada vez más común en las computadoras portátiles y otros dispositivos móviles. También hay teclados del mercado de accesorios para computadoras de escritorio con lectores de huellas digitales integrados también. Los escaneos de huellas digitales no proporcionan seguridad impenetrable; Es posible que las huellas digitales se puedan duplicar, y un escaneo de un dedo probablemente seguiría funcionando, incluso si no estuviera conectado a su propietario. Sin embargo, en combinación con una contraseña, los escaneos de huellas dactilares proporcionan una solución de autenticación multifactor que no puede ser penetrada de manera casual.

El reconocimiento facial es otro tipo de exploración biométrica que Windows Hello puede usar para la autenticación multifactor. Las cámaras son omnipresentes en la sociedad moderna, por lo que parece que los costos de hardware de un sistema de reconocimiento facial son mínimos. Sin embargo, este no es el caso, al menos con los productos de reconocimiento facial de Microsoft. El reconocimiento facial plantea cuestiones tanto de seguridad como de privacidad. Si una computadora puede reconocer la cara de una persona como un factor de seguridad, ¿qué detendría a un intruso de mostrar una foto de la persona a la cámara? ¿Y dónde se envía la imagen de la cara del usuario para realizar la autenticación?

Microsoft tiene respuestas a ambas preguntas. Windows Hello para empresas admite el uso del reconocimiento facial para la autenticación del usuario, pero requiere una cámara con una fuente de luz infrarroja separada y un sensor de infrarrojo cercano. El principal problema con los sistemas de reconocimiento facial en dispositivos personales es que las personas pueden usarlos en cualquier tipo de iluminación. Las imágenes de infrarrojo cercano proporcionan una imagen consistente independientemente de las condiciones de luz visible. Windows Hello tampoco almacena imágenes de la cara del usuario y nunca las transmite a otras ubicaciones para la autenticación. Cuando un usuario se inscribe por primera vez en Windows Hello, el Marco biométrico de Windows procesa una imagen facial dentro del dispositivo y la almacena como un perfil de inscripción. En intentos de autenticación posteriores, el sistema realiza el mismo proceso y compara los resultados con el perfil.

#### **ALGO QUE TIENES**

Mientras que la *algo que tienes* en la autenticación multifactor puede ser una tarjeta inteligente o alguna otra forma de identificación, en Microsoft 365, generalmente es un teléfono celular. Esta es una opción más práctica porque la mayoría de las personas hoy en día llevan teléfonos celulares con ellos, mientras que los lectores de tarjetas son mucho menos comunes.

Ya se ha vuelto común que los sitios web de Internet requieran un factor de autenticación secundario, generalmente en forma de código (llamado contraseña de un solo uso u OTP) enviado al teléfono celular del usuario como una llamada o un mensaje de texto. los

el usuario proporciona el código en el sitio web y se otorga la autorización.

Microsoft 365 admite este método para la autenticación multifactor de las identidades de Azure AD de los usuarios, entre otros.

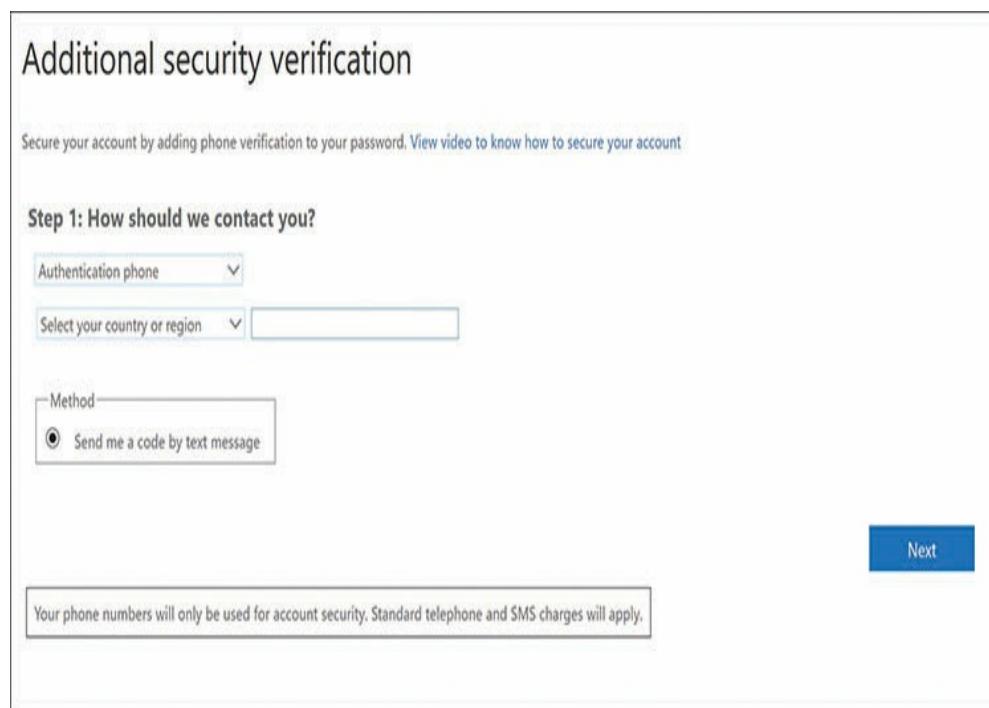
Las opciones basadas en el teléfono celular para Azure AD Multifactor Authentication (MFA) son las siguientes:

- **Texto SMS del código OTP al teléfono móvil** Despues de que el usuario complete la autenticación de contraseña, Azure AD envía un mensaje de texto que contiene un código OTP al número de teléfono preconfigurado del usuario. El usuario escribe el código en la pantalla de inicio de sesión para completar la autenticación.
- **Llamada de voz automatizada a teléfono móvil** Una vez que el usuario completa la autenticación de contraseña, Azure AD genera una llamada de voz automatizada al número de teléfono preconfigurado del usuario. El usuario responde la llamada y presiona la tecla # del teléfono para completar la autenticación.
- **Notificación a la aplicación móvil** Una vez que el usuario completa la autenticación de contraseña, Azure AD envía una notificación a la aplicación Microsoft Authenticator en el teléfono inteligente del usuario. El usuario toca el botón Verificar en la aplicación para completar la autenticación.
- **Código de verificación en la aplicación móvil** La aplicación Microsoft Authenticator genera un nuevo código de verificación OATH cada 30 segundos. Despues de que el usuario complete la autenticación de contraseña, el usuario escribe el código de verificación actual de la aplicación Microsoft Authenticator en la pantalla de inicio de sesión para completar la autenticación.

Por supuesto, los teléfonos celulares pueden perderse, ser robados o destruidos, por lo que cualquier método de autenticación que dependa de ellos no será completamente seguro, pero en combinación con una contraseña, proporcionan una barrera significativa contra el atacante estándar. La autenticación multifactor no es necesaria para Microsoft 365, pero

se está convirtiendo rápidamente en un *de facto* estándar para la seguridad de la red, en gran parte porque muchos administradores están descubriendo que han alcanzado el límite de autenticación de contraseña, en lo que respecta a la tolerancia de los usuarios.

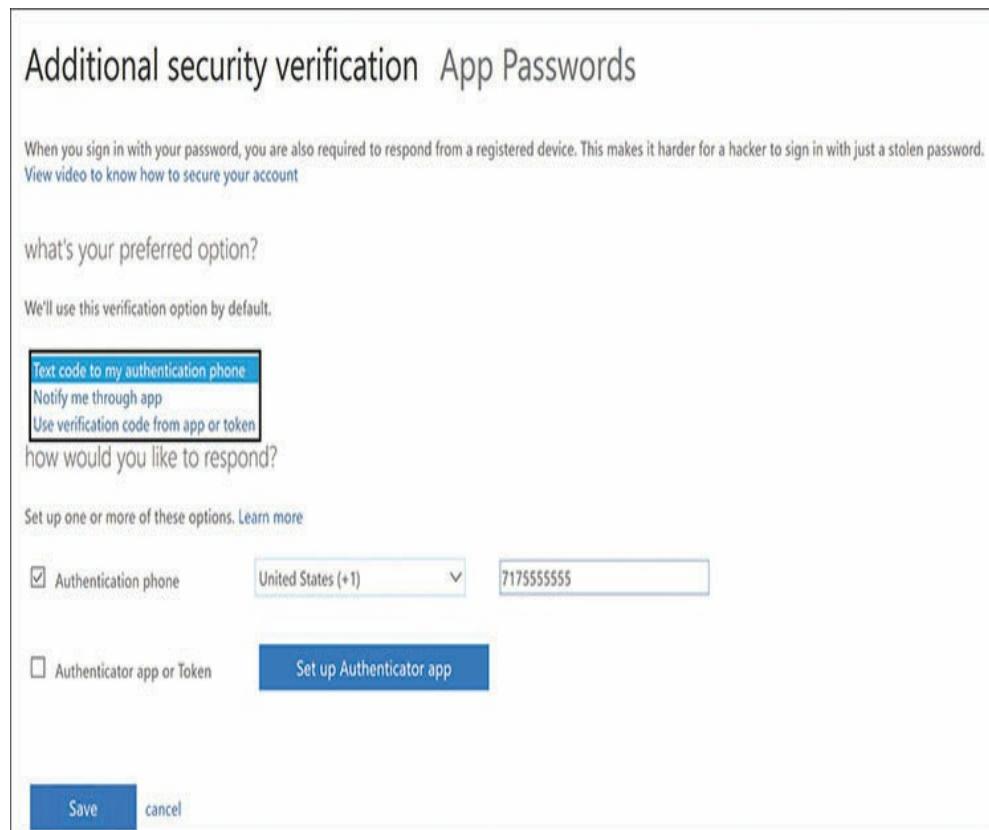
Los administradores pueden habilitar la autenticación multifactor para usuarios específicos mediante el Centro de administración de Azure Active Directory. La próxima vez que los usuarios inicien sesión, una pantalla les informa que se requiere más información. Otra pantalla, que se muestra en Figura 3-22., luego les permite ingresar un número de teléfono y especificar si el contacto inicial con un usuario debe ser a través de un código enviado al teléfono celular del usuario o mediante una aplicación móvil, como Microsoft Authenticator.



**FIGURA 3-22** La autenticación multifactor inicial

## interfaz de configuración

Después de la autenticación multifactorial exitosa inicial, aparece otra pantalla, como se muestra en Figura 3-23., en el que los usuarios pueden seleccionar entre las opciones de autenticación basadas en teléfonos celulares enumeradas anteriormente y configurar un número de teléfono o la aplicación Authenticator.



**FIGURA 3-23** La segunda verificación de seguridad adicional: pantalla de contraseñas de aplicaciones

## Protección de identidad

Todas las identidades son una fuente potencial de riesgo para todo

red, no importa qué nivel de privilegios posean. Una vez que los atacantes comprometen una identidad, se vuelve relativamente fácil para ellos extenderse lateralmente dentro de la empresa y comprometer a otros. Por esa razón, los administradores deben hacer todo lo posible para proteger todas las identidades, no solo las que tienen privilegios administrativos.

Una de las innovaciones clave de Microsoft 365 es el mayor énfasis en la detección y corrección proactiva de amenazas. Azure AD puede proporcionar este tipo de seguridad para cuentas de usuario con una característica llamada Azure AD Identity Protection. Identity Protection funciona evaluando las actividades de inicio de sesión de las cuentas de usuarios individuales y asignándoles niveles de riesgo que aumentan cuando ocurren múltiples eventos negativos. Hay dos niveles de riesgo asociados con cada identidad, como sigue:

- **Riesgo de inicio de sesión** La probabilidad de que un individuo no autorizado intente autenticarse con la identidad de otra persona
- **Riesgo del usuario** Una probabilidad acumulada de que una identidad específica haya sido comprometida

Azure AD Identity Protection reconoce los siguientes eventos de riesgo y modifica los dos niveles de riesgo de una identidad según el orden y la frecuencia en que ocurren:

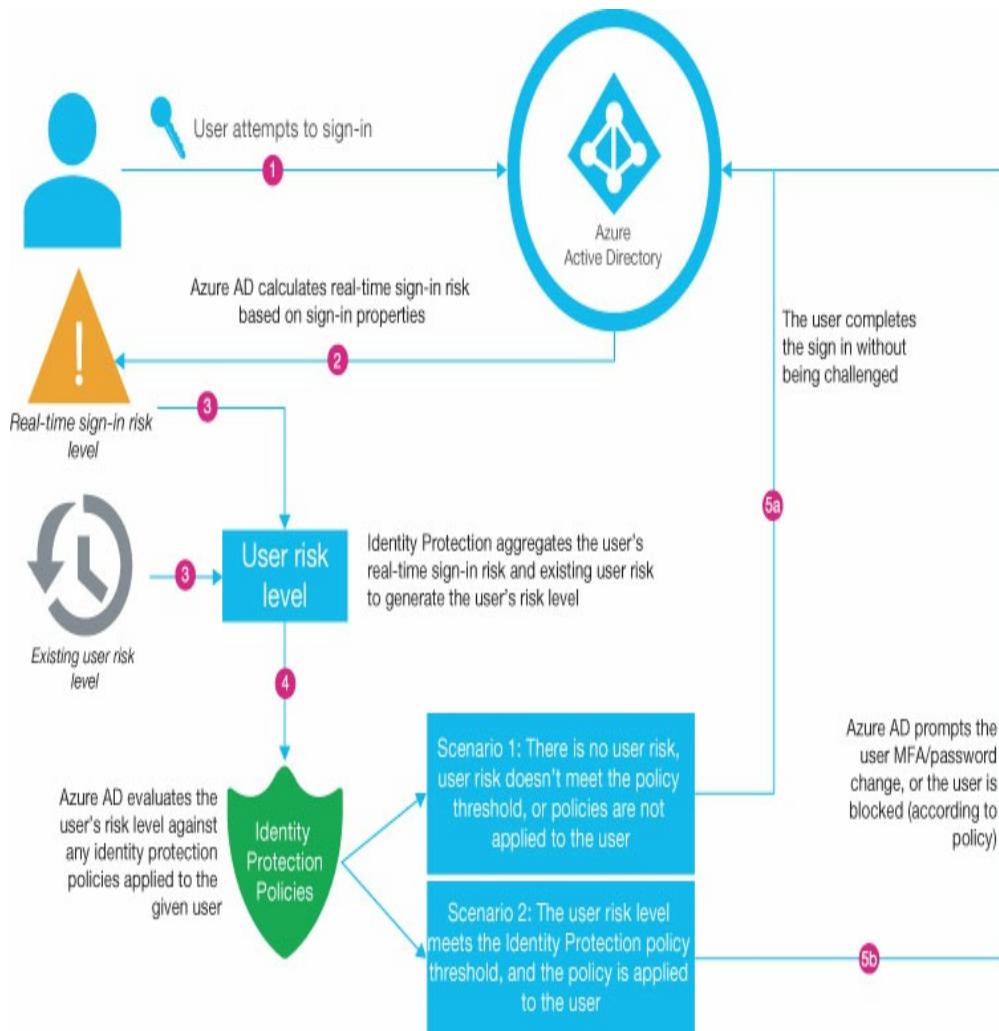
- **Viajes atípicos** El usuario inicia sesión desde una ubicación que no es típica para el usuario o que es geográficamente imposible, según los otros inicios de sesión recientes del usuario. Azure AD tiene en cuenta el tiempo de viaje entre las ubicaciones y gradualmente desarrolla su propio perfil de los hábitos del usuario, lo que ayuda a prevenir la aparición de falsos positivos.

(es decir, conclusiones de riesgo de los patrones de inicio de sesión que son comunes para ese usuario).

- **Dirección IP anónima** El usuario inicia sesión desde un navegador que suprime la dirección IP del usuario, como Tor o un cliente de red privada virtual (VPN). El usuario que inicia sesión puede o no ser el propietario de la identidad, pero Azure AD considera que el anonimato en sí mismo es sospechoso.
- **Propiedades de inicio de sesión desconocidas** El usuario inicia sesión desde un cliente que tiene propiedades desconocidas, como una nueva ubicación o una dirección IP inusual o un número de sistema autónomo (ASN), en función de las actividades anteriores del usuario. Para las nuevas identidades, hay un período de recopilación de información que dura al menos cinco días, durante el cual Azure AD no realiza evaluaciones de riesgos con este criterio.
- **Dirección IP vinculada a malware** Una identidad está asociada con una dirección IP que se ha utilizado previamente para contactar con un servidor bot conocido en Internet. Se supone que el sistema está infectado con malware y se considera un riesgo.
- **Credenciales filtradas** Se determina que una identidad usa credenciales que se sabe que han sido comprometidas. Microsoft recopila información sobre tales credenciales de numerosas fuentes, incluidas las agencias de aplicación de la ley, consultores de seguridad y sitios web ilícitos.

Cuando se producen estos eventos, Azure AD los evalúa y modifica el comportamiento del proceso de autenticación según los criterios establecidos por los administradores. Obviamente, hay muchas combinaciones posibles de comportamientos que Azure AD podría tener que tener en cuenta al evaluar los niveles de riesgo de una identidad. Por ejemplo, si los mismos eventos de riesgo ocurren repetidamente, los niveles de riesgo continuarán aumentando hasta que se requiera una reacción drástica, como bloquear todo acceso a la identidad.

El proceso básico de Azure AD Identity Protection se ilustra en Figura 3-24.



**FIGURA 3-24** El proceso de evaluación de riesgos de Azure AD Identity Protection

Como ejemplo, cuando un usuario intenta iniciar sesión con una contraseña simple de una dirección IP anónima, Azure AD determina que es un riesgo y le asigna un nivel de riesgo de inicio de sesión de medio. Este nivel de riesgo hace que Azure AD

Implemente una política de acceso condicional que imponga una acción específica, como solicitar la autenticación multifactor durante el proceso de inicio de sesión. Si el usuario completa con éxito la autenticación multifactor, el nivel de riesgo del usuario permanece sin cambios.

Sin embargo, si el usuario no puede completar la autenticación multifactor, Azure AD considera que esto es una posible indicación de que la identidad se ha visto comprometida y aumenta el nivel de riesgo del usuario. La próxima vez que el usuario intente iniciar sesión, el proceso podría continuar de manera completamente normal, sin que se detecte ningún riesgo de inicio de sesión; sin embargo, el nivel de riesgo del usuario asociado con la identidad persiste, y Azure AD podría configurarse para solicitar al usuario que cambie la contraseña como resultado.

Azure AD Identity Protection se incluye solo con el plan Azure Active Directory Premium P2, que se suministra con la edición Microsoft 365 Enterprise P2.



---

#### ***Consejo de examen***

**La seguridad adicional proporcionada por Azure AD Identity Protection es aplicable solo a las identidades basadas en la nube, no a las identidades locales en los Servicios de dominio de Active Directory. El mayor énfasis de Microsoft en soluciones basadas en la nube, como Office 365 y ahora Microsoft 365, significa que las últimas innovaciones en seguridad y otras áreas no se están transfiriendo a las versiones tradicionales locales. Es por esta razón que Microsoft es**

recomendar que las redes empresariales desplace más aplicaciones y servicios de los servidores locales a la nube. Al prepararse para el examen MS-900, los candidatos deben ser conscientes de este énfasis en la nube y tener cuidado de distinguir los productos basados en la nube de Microsoft de sus productos locales.

---

## Proteger documentos

El propósito fundamental de las identidades es proteger documentos y otros datos. Al proteger las identidades, la amenaza de penetración lateral obliga a los administradores a aplicar la misma protección a todos ellos, independientemente de sus privilegios. Sin embargo, al proteger documentos, la seguridad puede y debe ser más selectiva. Si bien una empresa puede tener cientos o miles de identidades para proteger, puede tener fácilmente cientos de miles o millones de documentos, y esto hace que no sea práctico aplicar la misma protección. Por lo tanto, es importante que los administradores identifiquen los documentos que contienen datos confidenciales, que requieren más protección.

Como se discutió anteriormente en este capítulo, Azure Information Protection (AIP) y Office 365 Data Loss Prevention (DLP) son herramientas que permiten a los administradores y usuarios aplicar etiquetas de clasificación a los documentos y especificar medidas de seguridad que se aplican a los documentos basados en esas etiquetas. Si bien estas herramientas pueden, en algunos casos, detectar datos confidenciales en documentos

según los criterios que especifican los administradores, hay muchos otros casos en los que corresponde a los usuarios aplicar las etiquetas correctamente a sus propios documentos.

**Nota:**

**Información**

**Protección y prevención de pérdida de datos**

Para obtener más información sobre Azure Information Protection y Office 365

**Data Loss Prevention, consulte " Documentos ", Anteriormente en este capítulo.**

Los aspectos tecnológicos de la implementación de herramientas como AIP y DLP son relativamente sencillos; sin embargo, los aspectos administrativos, culturales y educativos de la implementación pueden ser más problemáticos, especialmente en una gran empresa. Para que estas herramientas funcionen de manera efectiva, las etiquetas de clasificación que representan los diversos niveles de sensibilidad de datos deben ser entendidas por todos los involucrados y aplicadas consistentemente en toda la organización.

Cuando la intención es crear una taxonomía de etiqueta de clasificación única que utilizará toda la empresa, tiene sentido que los representantes de todas las áreas y todos los niveles de la empresa tengan voz en el diseño de esa taxonomía. A menos que los términos utilizados para las etiquetas signifiquen lo mismo para todos, existe la posibilidad de que los documentos se etiqueten incorrectamente o, peor aún, no se etiqueten en absoluto cuando deberían serlo.

Con la taxonomía de etiquetado acordada y establecida, el siguiente paso en la implementación, como con todos los programas nuevos, debería ser una implementación piloto. Con un pequeño grupo de usuarios representativos aplicando etiquetas a sus documentos, y con DLP configurado para clasificar un subconjunto de documentos de la compañía automáticamente, el monitoreo cuidadoso del proceso de etiquetado y la evaluación de los documentos clasificados casi con certeza revelará algún etiquetado incorrecto, que requiere modificaciones para las herramientas mismas o los procedimientos de los usuarios. Es probable que se necesiten sucesivas iteraciones de la taxonomía y los algoritmos DLP antes de que el sistema sea completamente confiable.

La fase final de la implementación, y posiblemente la más difícil, será educar a todos los usuarios de la organización sobre qué es el sistema de etiquetado, cómo funciona y por qué es necesario. Esto es particularmente cierto para los usuarios que no están involucrados en la tecnología detrás del sistema. La protección de documentos no es un problema que los administradores puedan resolver solo con tecnología; El factor humano también es una parte crítica.

### Comprobación rápida

- ¿Cuál de los siguientes elementos es responsable de crear identidades híbridas mediante la replicación de identidades locales en la nube?
  - Azure AD

- Azure AD Connect
- Contraseña hash sincronización AD DS
- 

#### Respuesta de verificación rápida

- Azure AD Connect es una herramienta de software que se ejecuta en la red local y replica las identidades de los Servicios de dominio de Active Directory en Azure Active Directory en la nube, creando identidades híbridas.

## HABILIDAD 3.3: ENTENDER LA NECESIDAD DE GESTIÓN DE ENDPOINT UNIFICADA, ESCENARIOS Y SERVICIOS DE USO DE SEGURIDAD

---

En un momento, la seguridad de la red empresarial consistía en computadoras propiedad de la compañía, implementadas y administradas internamente, y protegidas mediante políticas de contraseña, firewalls, software antivirus y, para algunos usuarios remotos, conexiones de acceso telefónico y redes privadas virtuales. Los administradores de red controlaron todo el equipo y una generación de *Herramientas de gestión de clientes (CMT)*

apareció, como el de Microsoft *Administrador de configuración de System Center (SCCM)*. SCCM proporciona una solución de gestión unificada que permite a los administradores hacer un inventario del hardware e implementar operaciones

sistemas y aplicaciones, actualice software, administre licencias y controle remotamente computadoras en toda la empresa.

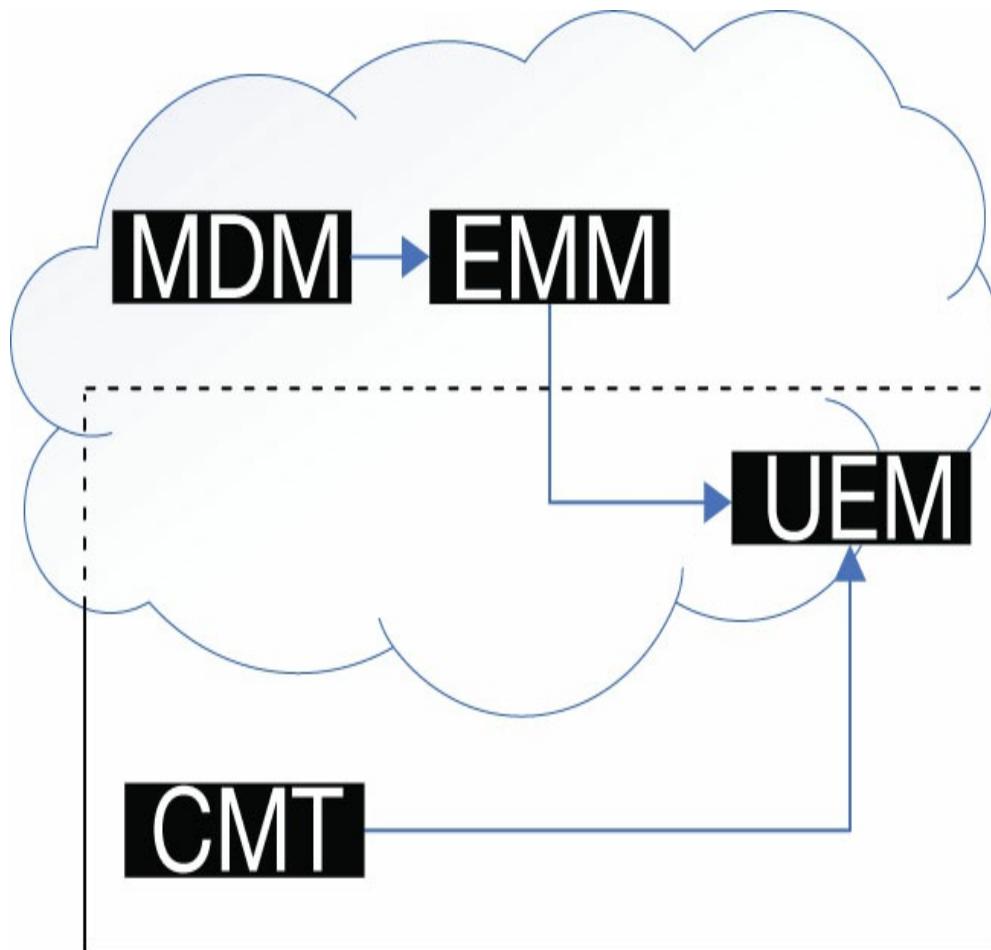
Desafortunadamente, las plataformas de administración como SCCM están diseñadas para usarse solo con computadoras locales y se comunican a través de redes de área local (LAN). A medida que los dispositivos informáticos móviles se hicieron cada vez más comunes, se necesitaba una nueva plataforma de gestión, una que pudiera funcionar a través de la nube. *Administración de dispositivos móviles (MDM)* fue la primera iteración de esa nueva plataforma. Los productos de MDM generalmente ejercen un control completo sobre los dispositivos móviles que administran y, como resultado, se hizo común que las organizaciones que usan los productos también sean propietarias de los dispositivos.

Sin embargo, los trabajadores a menudo tenían problemas con las restricciones de usabilidad impuestas por los dispositivos administrados por la empresa. Estos problemas solo se volvieron más severos cuando las personas comenzaron a comprar sus propios teléfonos inteligentes y les resulta más fácil trabajar con ellos que los dispositivos de su empresa administrados por MDM. Esto eventualmente resultó en el concepto BYOD (Trae tu propio dispositivo), que ciertamente complació a los usuarios pero dificultó la vida de los administradores.

Para proporcionar una seguridad adecuada en los dispositivos que la empresa no posee, se necesitaba un nuevo paso evolutivo en los productos de administración, y *gestión de movilidad empresarial (EMM)* herramientas, como Microsoft

Intune, fueron el resultado. Con Intune, los administradores pueden inscribir, configurar y administrar dispositivos móviles en varias plataformas de sistemas operativos diferentes, donde sea que estén los dispositivos. Los administradores pueden incluso intervenir cuando ocurre una amenaza a la seguridad, bloqueando el acceso de un dispositivo a la red de la empresa y borrando cualquier información confidencial almacenada en él.

Sin embargo, a pesar de los avances en la informática móvil y la gestión de dispositivos móviles, los dispositivos, las aplicaciones y los servicios locales no han desaparecido, y aún deben gestionarse. Las CMT y EMM son diferentes tipos de plataformas de gestión de muchas maneras fundamentales. Ambos requieren que los administradores tengan una cantidad significativa de capacitación y experiencia, pero los dos generalmente no se superponen. Surgió la necesidad de una plataforma de administración que pudiera funcionar con dispositivos locales y dispositivos basados en la nube, como se muestra en Dibujo 325 ; Esta plataforma de administración también debe ser extensible para incluir nuevas tecnologías a medida que se desarrollan, como los wearables y el Internet de las cosas (IoT).  
Esta nueva plataforma se conoce como *gestión unificada de puntos finales (UEM)*.



**FIGURA 3-25** Desarrollo de gestión unificada de puntos finales

El término *punto final* se ha utilizado para referirse a cualquier dispositivo de usuario, incluidas computadoras de escritorio, computadoras portátiles, impresoras, tabletas, teléfonos inteligentes, así como tecnologías más recientes, como dispositivos portátiles y dispositivos de Internet de las cosas. El objetivo de la gestión unificada de puntos finales es eliminar la necesidad de herramientas de gestión separadas para dispositivos locales y móviles. Una solución UEM ideal es una plataforma de administración de "panel único" que puede

administre las aplicaciones, identidades, recursos, actualizaciones, seguridad y cumplimiento de políticas para todos los puntos finales de la empresa, independientemente de sus ubicaciones, tipos de dispositivos o sistemas operativos.

**Nota:**

## Internet de las Cosas

A medida que la red móvil va más allá del ahora omnipresente teléfono inteligente, la próxima evolución parece ser el Internet de las cosas (IoT), en el que los dispositivos informáticos móviles están integrados en varios tipos de herramientas, dispositivos y sistemas. La automatización de viviendas y edificios es un mercado en crecimiento para dispositivos IoT, incluidos termostatos, interruptores de luz y refrigeradores, así como sistemas industriales y de servicios públicos a gran escala.

En la industria del cuidado de la salud, los dispositivos IoT pueden monitorear las condiciones de los pacientes tanto dentro como fuera de los hospitales, incluidos los monitores de frecuencia cardíaca, presión arterial y glucosa en sangre; Además, pueden controlar dispositivos implantados, como marcapasos y desfibriladores. Los automóviles y otros vehículos también son aplicaciones comunes para IoT, que pueden proporcionar servicios de monitoreo de ubicación, cobro de peajes y control de tráfico. Todos estos tipos de dispositivos requieren la administración por parte de los administradores de red y posiblemente podrían ser una amenaza de seguridad tan grande como cualquiera de los otros dispositivos informáticos móviles que se usan actualmente. Uno solo puede imaginar el caos que podría resultar si un atacante lograra penetrar la red de un hospital o la red eléctrica de una ciudad, por ejemplo.

En Microsoft 365, UEM se implementa en el producto Enterprise Mobility + Security (EMS), que incluye un conjunto de herramientas que pueden funcionar juntas para

Proporcionar una solución de gestión integral para puntos finales locales y basados en la nube. Las herramientas relevantes en EMS incluyen lo siguiente:

- **Azure Active Directory Premium** El servicio de directorio basado en la nube que administra identidades y proporciona autenticación y autorización para todas las aplicaciones y servicios de Microsoft 365, incluidas todas las herramientas de administración de EMS
- **Azure AD Connect** Una herramienta local que replica las identidades de los usuarios en los controladores de dominio de AD DS en las identidades de Azure AD almacenadas en la nube para que los usuarios puedan iniciar sesión a través de la nube y los administradores puedan aprovechar las características de seguridad de identidad de Azure AD
- **Microsoft Intune** Un servicio de gestión de movilidad empresarial (EMM) basado en la nube que permite a los administradores inscribir dispositivos móviles, implementar aplicaciones y aplicar políticas de seguridad
- **Administrador de configuración de System Center (SCCM)** Una CMT local que los administradores pueden usar para hacer un inventario del hardware de la computadora, implementar imágenes del sistema operativo en estaciones de trabajo internas, administrar aplicaciones, aplicar actualizaciones de software y aplicar políticas de cumplimiento de dispositivos
- **Protección de la información de Azure (AIP)** Una herramienta basada en la nube que permite a los usuarios y administradores aplicar etiquetas de clasificación a los documentos e implementar varios tipos de protección basados en las etiquetas, como restricciones de acceso y cifrado de datos.
- **Microsoft Advanced Threat Analytics (ATA)** Una plataforma local que captura el tráfico de red y registra la información y la analiza para identificar comportamientos sospechosos relacionados con múltiples fases del proceso de ataque.
- **Seguridad de aplicaciones en la nube** Un servicio basado en la nube que analiza los registros de tráfico y las secuencias de comandos proxy para identificar las aplicaciones a las que acceden los usuarios, incluidas las aplicaciones no autorizadas, y permite a los administradores sancionar o desautorizar aplicaciones individuales y conectarse a las API suministradas por los proveedores de aplicaciones en la nube para realizar análisis de Cloud App Security

- **Protección contra amenazas avanzada de Azure** Un motor de prevención, detección y reparación de amenazas basado en la nube que utiliza inteligencia artificial busca amenazas de seguridad exclusivas del entorno Azure mediante el análisis del comportamiento del usuario y su comparación con los patrones de ataque conocidos.

*Nota:*

### Microsoft ATA

Para obtener más información sobre Microsoft Advanced Threat Analytics, consulte " Describir las capacidades analíticas en Microsoft 365. "Sección en Capítulo 2 , " Comprender los servicios y conceptos básicos de Microsoft 365 . "

## Microsoft 365 y servicios de directorio

Un servicio de directorio es un producto de software que almacena información sobre recursos de red con el fin de unificarlos en una entidad única y manejable. Por ejemplo, el Sistema de nombres de dominio (DNS) es un servicio de directorio que asocia los nombres de los recursos de red con sus direcciones de red correspondientes.

Como se señaló en la sección "Identidad", anteriormente en este capítulo, Azure Active Directory (Azure AD) y Active Directory Domain Services (AD DS) son los servicios de directorio que almacenan y administran las identidades de los usuarios para los diversos componentes de Microsoft 365. Azure AD almacena la información de su directorio en la nube de Microsoft Azure, y AD DS se almacena en equipos que ejecutan Windows Server que se han configurado para funcionar como controladores de dominio.

## Azure Active Directory

Azure AD está disponible en tres planes, como se muestra en Tabla 3-3.

Todos los productos de Microsoft 365 incluyen el plan Premium P1 o Premium P2.

**CUADRO 3-3** Licencias de Azure Active Directory

LICENCIA DE DIRECTORIO ACTIVO AZURE	INCLUIDO CON
Azure Active Directory gratuito	Suscripciones de Office 365 o Microsoft Azure
Azure Active Directory Premium P1	Microsoft 365 Enterprise E3 y Microsoft 365 Business
Azure Active Directory Premium P2	Microsoft 365 Enterprise E5

El plan Azure Active Directory Premium P1 admite las siguientes características y servicios:

- **Ilimitados objetos de directorio** Permite a los administradores crear identidades en la nube para un número ilimitado de usuarios.
- **Gestión de usuarios y grupos.** Permite a los administradores crear y administrar identidades de usuarios y grupos utilizando herramientas basadas en la nube, como el centro de administración de Azure AD y el Centro de administración de Microsoft 365.
- **Autenticación en la nube** Permite a los usuarios iniciar sesión en la red utilizando identidades híbridas almacenadas en la nube y con sincronización de hash de contraseña o autenticación de paso.
- **Sincronización con AD DS mediante Azure AD Connect** Despues de instalar la herramienta Azure AD Connect en un controlador de dominio AD DS

o servidor local, las identidades locales se pueden replicar en el directorio de Azure AD en la nube. Esto crea identidades híbridas que permiten a los usuarios acceder a recursos locales y basados en la nube con un inicio de sesión único.

- **Inicio de sesión único sin interrupciones** Permite a los usuarios con identidades híbridas que están conectadas a la red local iniciar sesión sin un procedimiento de autenticación interactivo.
- **Soporte para autenticación federada** Permite a los administradores descargar el proceso de autenticación de Azure AD en un servicio federado, como los Servicios de federación de Active Directory.
- **Autenticación multifactorial mediante teléfono, SMS o aplicación** Permite a los administradores exigir que los usuarios proporcionen dos o más formas de identificación al iniciar sesión con una identidad de Azure AD, como una contraseña más un escaneo biométrico o un código único enviado al teléfono inteligente del usuario.
- **Soporte para acceso de usuario híbrido a recursos en la nube y locales** Permite a los usuarios con identidades híbridas acceder a recursos locales y basados en la nube después de una única autenticación de Azure AD.
- **Autoservicio de restablecimiento de contraseña** Permite a los usuarios con identidades basadas en la nube modificar sus contraseñas sin asistencia del administrador.
- **Reescritura de dispositivos de Azure AD a identidades de AD DS** Permite que los dispositivos registrados en Azure AD y las contraseñas de identidad en la nube modificadas se copien en un contenedor de AD DS. Normalmente, Azure AD Connect solo sincroniza datos de AD DS a Azure AD.
- **Proxy de aplicación** Permite a los usuarios remotos basados en la nube acceder a aplicaciones web internas al reenviar sus solicitudes a un conector que se ejecuta en un servidor local.
- **Grupos dinámicos** Permite a los administradores crear reglas que especifiquen los atributos que debe poseer una cuenta de usuario para agregarse automáticamente a un grupo.
- **Políticas de nomenclatura grupal** Permite a los administradores crear políticas

que especifican un formato para los nombres de los grupos. Por ejemplo, se pueden requerir nombres de grupos para especificar una función, un departamento o una ubicación geográfica.

- **Acceso condicional** Permite a los administradores especificar las condiciones que los dispositivos móviles deben cumplir antes de que se les otorgue acceso a los recursos basados en la nube, como el riesgo de inicio de sesión, la aplicación del cliente en uso, el estado del dispositivo móvil y la ubicación del dispositivo.
- **Administrador de identidad de Microsoft** Proporciona administración de identidad y acceso, incluida la sincronización de usuarios, grupos y otros objetos para AD DS y Azure AD, así como servicios de directorio de terceros.
- **Azure Information Protection Premium P1** Permite a los usuarios y administradores clasificar y etiquetar documentos en función de la sensibilidad de los datos que contienen.
- **Informes de seguridad y actividad.** Proporciona a los administradores informes que enumeran amenazas potenciales, incluidos inicios de sesión riesgosos y registros de auditoría que documentan las actividades de los usuarios.

Con estas características y servicios, el plan Azure Active Directory Premium P1 permite a los administradores administrar los recursos basados en la nube de una organización, así como también identificar, predecir, detectar y remediar una amplia variedad de amenazas de seguridad. Sin embargo, el plan Azure Active Directory Premium P2 admite todo lo incluido en el plan P1 y también proporciona las siguientes características de seguridad adicionales:

- **Protección de identidad de Azure AD** Evalúa las actividades de inicio de sesión de los usuarios, cuantifica sus niveles de riesgo y toma medidas en función de esos niveles.
- **Gestión de identidad privilegiada** Permite a los administradores regular el acceso a recursos confidenciales al otorgar privilegios temporales a usuarios específicos, que requieren medidas de seguridad adicionales y recibir

notificaciones cuando se accede a los recursos. El objetivo es evitar que los usuarios con privilegios administrativos los usen innecesariamente.

- **Seguridad de aplicaciones en la nube** Un servicio basado en la nube que analiza los registros de tráfico y los scripts proxy para identificar y monitorear las aplicaciones a las que acceden los usuarios.
- **Azure Information Protection Premium P2** Expande las capacidades del plan Premium P1 al automatizar el proceso de identificación, clasificación y etiquetado de documentos.

Azure Information Protection está incluido en todos los planes de Microsoft 365, pero también está disponible con otros productos de Microsoft en una versión gratuita con funcionalidad limitada y como una suscripción separada en dos planes propios, llamados Premium P1 y Premium P2. Cada nivel de suscripción agrega funciones, como se muestra en **Tabla 3-4** e incluye todas las características de los niveles de suscripción inferiores.

#### **CUADRO 3-4 Suscripciones de Azure Information Protection**

PLAN	INCLUIDO CON	DESCRIPCIÓN
Gratis	No se requiere compra	Permite el consumo de contenido protegido por AIP por parte de usuarios con cuentas que no están asociadas con identidades de Azure
Información de Azure	Office 365 Enterprise E3 y superior	Brinda protección para los servicios de Office 365 mediante plantillas personalizadas y admite el cifrado de mensajes de Office 365

Protección para Office 365		
Información de Azure	Microsoft 365 Business	Proporciona la capacidad de usar conectores locales, rastrear y revocar documentos, y clasificar y etiquetar documentos manualmente
Protección	Microsoft 365 Enterprise E3	
Premium P1	Microsoft Enterprise Mobility + Security E3	
Información de Azure	Microsoft 365 Enterprise E5	Proporciona soporte para reglas basadas en políticas y clasificación automatizada, etiquetado y protección de documentos.
Protección Premium P2	Microsoft Enterprise Mobility + Security E5	

## Servicios de dominio de Active Directory

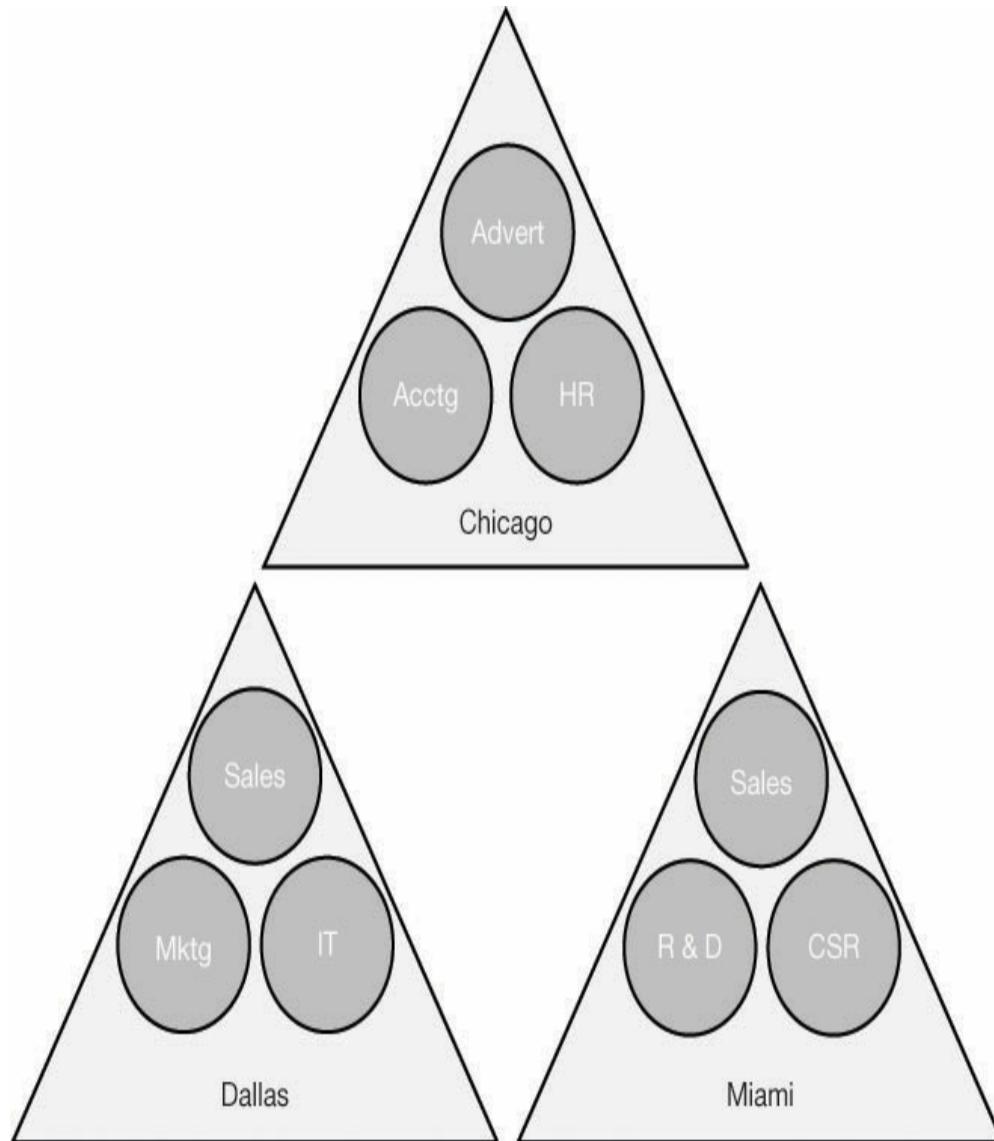
Active Directory Domain Services (AD DS) es un servicio de directorio jerárquico orientado a objetos que funciona como un proveedor interno de autenticación y autorización para redes Windows. Debido a que no se encuentra en la nube como Azure AD, la fuente principal de protección

para AD DS es el firewall y otra protección perimetral que rodea la red local. Los controladores de dominio AD DS son servidores de Windows que se encuentran dentro del perímetro de la red; no deben implementarse en una DMZ ni de ninguna otra manera que los deje abiertos para acceder desde Internet.

Además, a diferencia de Azure AD, los administradores de red deben diseñar, implementar y mantener un directorio de AD DS. El servicio se proporciona como una función en el sistema operativo Windows Server, que los administradores deben agregar después de la instalación del propio sistema operativo. Un directorio AD DS no incluye ninguno de los mantenimientos integrados y la tolerancia a fallas que se encuentran en los servicios en la nube de Microsoft.

Por lo general, los controladores de dominio AD DS no realizan otra función que no sea actuar como servidores DNS. Por ejemplo, no se considera seguro usar controladores de dominio como servidores de aplicaciones o archivos. Para garantizar la tolerancia a fallas y la alta disponibilidad, los administradores deben instalar múltiples controladores de dominio, preferiblemente en diferentes sitios. Los controladores de dominio replican los contenidos del directorio entre sí de manera regular.

A diferencia de Azure AD, AD DS es un servicio de directorio jerárquico que permite a los administradores crear un directorio que emule la infraestructura departamental o geográfica de su empresa, como se muestra en **Figura 3-26**.



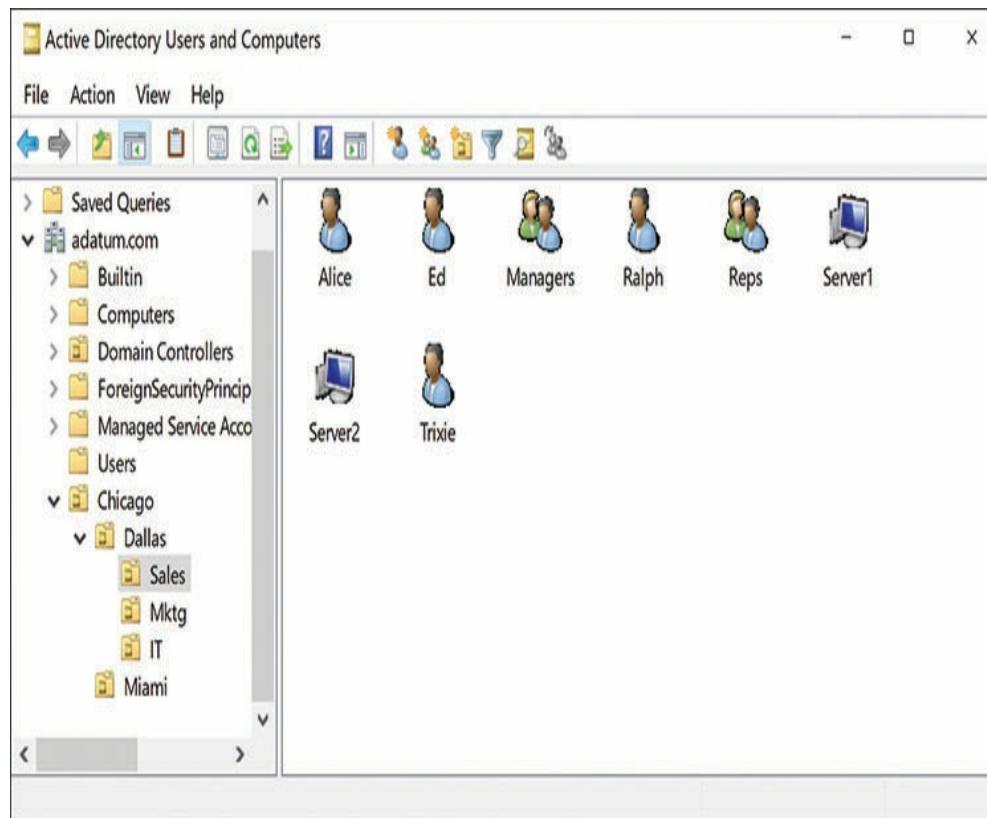
**FIGURA 3-26** Una jerarquía de contenedor de Servicios de dominio de Active

Directory

Los bosques, los árboles, los dominios y las unidades organizativas son todos los tipos de objetos de AD DS que contienen otros objetos, como usuarios, grupos y computadoras, como se muestra en

Figura 3-27. . Al igual que con un sistema de archivos, los permisos fluyen

hacia abajo a través de la jerarquía. Los permisos otorgados a un objeto contenedor son heredados por todos los objetos en ese contenedor y por todos los contenidos subordinados debajo de él. Los administradores pueden diseñar la jerarquía de AD DS como lo deseen.



**FIGURA 3-27 AD DS objetos en una unidad organizativa**

En la administración de AD DS, queda mucho más trabajo para el administrador de la red que en Azure AD. En Azure AD, se puede comenzar a crear usuarios y grupos inmediatamente después de establecer un arrendamiento, sin necesidad de instalar y mantener controladores de dominio o diseñar una infraestructura. Tampoco hay preocupaciones sobre

seguridad física con Azure AD, porque Microsoft es responsable de sus centros de datos y del mantenimiento de las computadoras que brindan los servicios. El gasto de costo inicial para un directorio de Azure AD también es mínimo. AD DS requiere la compra de computadoras servidor y el sistema operativo Windows Server, pero no hay tarifas de suscripción continuas.

Aunque AD DS usa una infraestructura que es sustancialmente diferente de Azure AD, realiza los mismos servicios básicos al autenticar a los usuarios y autorizar su acceso a los recursos de la red. Sin embargo, AD DS no admite muchas de las características de seguridad avanzadas que se encuentran en Azure AD. Por ejemplo, no tiene soporte interno para la autenticación multifactor, aunque es posible usar un servicio de autenticación externo para algunos factores de autenticación adicionales. AD DS tampoco incluye Azure AD Identity Protection, Conditional Access y Azure Information Protection.

Debido a que los controladores de dominio a menudo están conectados a la misma red que las estaciones de trabajo y otros sistemas menos sensibles, pueden ser vulnerables a un ataque lateral de un intruso que ha obtenido acceso a otro sistema en la red. Como resultado, a pesar de que los controladores de dominio podrían estar protegidos, cualquiera de los vectores de ataque típicos a los que las computadoras locales son susceptibles puede representar una amenaza para la implementación de AD DS. Por ejemplo, cualquier computadora en el

La red que no está actualizada en su sistema operativo y las actualizaciones de aplicaciones o que carece de protección contra virus o malware puede ser un objetivo para el ataque y un punto de lanzamiento para una mayor invasión del directorio AD DS.

AD DS también es más vulnerable al robo de credenciales que Azure AD debido al uso inseguro de credenciales privilegiadas. Los administradores de una red local a veces pueden ser descuidados al usar sus identidades privilegiadas para realizar tareas cotidianas, como navegar por Internet o iniciar sesión en computadoras que no están completamente protegidas. En Azure Active Directory Premium P1, estas son prácticas que pueden abordarse con la característica de Administración de identidad privilegiada, pero Microsoft no ha integrado las herramientas de seguridad de Azure AD en AD DS.



---

#### ***Consejo de examen***

Para los candidatos al examen MS-900 que son nuevos en estas tecnologías, puede ser fácil confundir las capacidades de Azure Active Directory (Azure AD) basado en la nube y los Servicios de dominio de Active Directory (AD DS) locales. Es importante saber que AD DS es un servicio de directorio jerárquico, provisto con el sistema operativo Windows Server, que requiere un proceso de diseño e implementación bastante extenso. Azure AD, por el contrario, está basado en suscripción, no es jerárquico y prácticamente no requiere configuración. Los candidatos también deben ser conscientes de las características que se proporcionan en Azure Active Directory Premium P1

y los planes Azure Active Directory Premium P2, y con las diferentes funcionalidades de los planes Azure Information Protection Premium P1 y Azure Information Protection Premium P2.

---

## Cogestión de SCCM e Intune

System Center Configuration Manager (SCCM) es la herramienta de administración de clientes de Microsoft para redes locales. El producto, lanzado por primera vez en 1994 (bajo el nombre de Systems Management Server), proporciona una solución de administración integral para sistemas locales al proporcionar las siguientes características:

- **Despliegue del sistema operativo** Implementa imágenes del sistema operativo en las estaciones de trabajo del cliente a través de la red utilizando una variedad de escenarios, tanto automatizados como interactivos.
- **Gestión de actualizaciones de software** Implementa actualizaciones de sistemas operativos, aplicaciones, controladores de dispositivos y firmware del BIOS del sistema en flotas completas de dispositivos.
- **Inventario de hardware y software.** Realiza inventarios completos del hardware y el software instalado en las computadoras cliente.
- **Despliegue de aplicaciones** Proporciona la implementación de aplicaciones basadas en el usuario en múltiples tipos de dispositivos utilizando diversos mecanismos de entrega, incluidas las instalaciones locales, App-V y RemoteApp.
- **Protección de punto final** Para Windows 8.1 y versiones anteriores, proporciona un cliente antimalware System Center Endpoint Protection; para ventanas 10, proporciona un cliente de administración para el motor antimalware integrado de Windows Defender.
- **Monitoreo de salud del cliente** Proporciona monitoreo centralizado e informes sobre la salud y las actividades del cliente, con la capacidad de generar

alertas y realizar remediaciones.

- **Gestión de cumplimiento** Permite a los administradores crear una línea base de estado de configuración para los clientes, evaluar su cumplimiento y generar alertas o realizar correcciones.

SCCM es una excelente solución CMT para sistemas locales, pero no admite la administración de dispositivos móviles basados en la nube por sí mismo. Por lo tanto, para lograr una verdadera solución Unified Endpoint Management con productos de Microsoft, se necesita una combinación de SCCM y Microsoft Intune, en un acuerdo llamado

### *cogestión*

Una implementación de SCCM consta de al menos un servidor en la red, una consola de Configuration Manager y la instalación de un agente de software en cada cliente que se administrará. El proceso de implementación de SCCM en una red local no es simple, ya que requiere modificaciones del esquema de los Servicios de dominio de Active Directory y una instalación de Microsoft SQL Server, así como la instalación del servidor SCCM y los clientes individuales.

El escenario típico previsto para la cogestión es una empresa que ya ha realizado una inversión significativa en una infraestructura SCCM y planea agregar Microsoft 365. Microsoft Intune, la herramienta de gestión de movilidad empresarial que se incluye en el componente Enterprise Mobility + Security, proporciona capacidades de gestión avanzadas que los administradores

a menudo quieren usarlo para sus sistemas locales, así como para sus dispositivos móviles basados en la nube.

La administración conjunta es una característica de SCCM que vincula los sistemas locales a Microsoft Intune en la nube y permite a los administradores administrar sus computadoras locales con las consolas SCCM e Intune. Al agregar capacidades de administración conjunta a su infraestructura interna, los administradores pueden aprovechar las siguientes características de Microsoft 365:

- **Azure AD híbrido** Al crear identidades híbridas para usuarios locales, pueden acceder a los recursos locales y basados en la nube con un inicio de sesión único, así como utilizar las funciones de Microsoft 365 como Windows Hello para empresas y restablecimiento de contraseña de autoservicio. Los administradores pueden aprovechar el acceso condicional basado en dispositivos de Intune y las licencias automáticas de dispositivos.
- **Acceso condicional** La capacidad de acceso condicional en Intune va más allá de las capacidades de gestión de cumplimiento en SCCM al proporcionar una evaluación más completa del dispositivo, así como la detección y reparación de amenazas de seguridad.
- **Acciones remotas** Microsoft Intune permite a los administradores administrar dispositivos conectados a la red, donde sea que se encuentren, utilizando controles basados en la nube que pueden inventariar, reiniciar o restablecer un dispositivo, eliminar datos de la compañía o tomar el control remoto.
- **Salud del cliente** La supervisión del estado del cliente en SCCM se limita a los dispositivos que están conectados activamente a la red interna. Con Intune, el estado del cliente se supervisa siempre que se pueda acceder al dispositivo desde la nube. Intune proporciona registros con marca de tiempo del estado de cada cliente y su disponibilidad para la instalación y actualización de aplicaciones.
- **Piloto automático de Windows** Los administradores pueden optar por implementar nuevos dispositivos utilizando el piloto automático de Windows en lugar del proceso de implementación de imágenes que utiliza SCCM. Esto puede eliminar la necesidad de

administradores para crear y mantener imágenes de arranque y del sistema para varias combinaciones de hardware.

Para que los dispositivos con Windows 10 se administren conjuntamente, deben tener instalado el software de agente de cliente SCCM y deben estar inscritos en Microsoft Intune. Para una instalación SCCM existente, el proceso de implementación de la gestión conjunta con Intune consta de los siguientes pasos básicos:

- Cree identidades híbridas para los usuarios del cliente SCCM instalando Azure AD Connect en la red interna y configurándolo para replicar los usuarios de AD DS en el inquilino de Azure AD.
- Asigne una licencia de Microsoft 365 (o licencias individuales Intune y Azure AD Premium) a los usuarios del cliente SCCM. En la consola de Configuration Manager en SCCM,
- habilite el  
**Registre automáticamente nuevos dispositivos unidos al dominio de Windows 10 con Azure Active Directory Client** ajuste. En Azure Portal, habilite **Inscripción automática MDM** para algunos o todos los dispositivos con Windows 10 en la red. En la consola de Configuration Manager, ejecute el **Asistente de configuración de gestión conjunta** y habilitar el **Inscripción automática en Intune** ajuste

**Nota:**

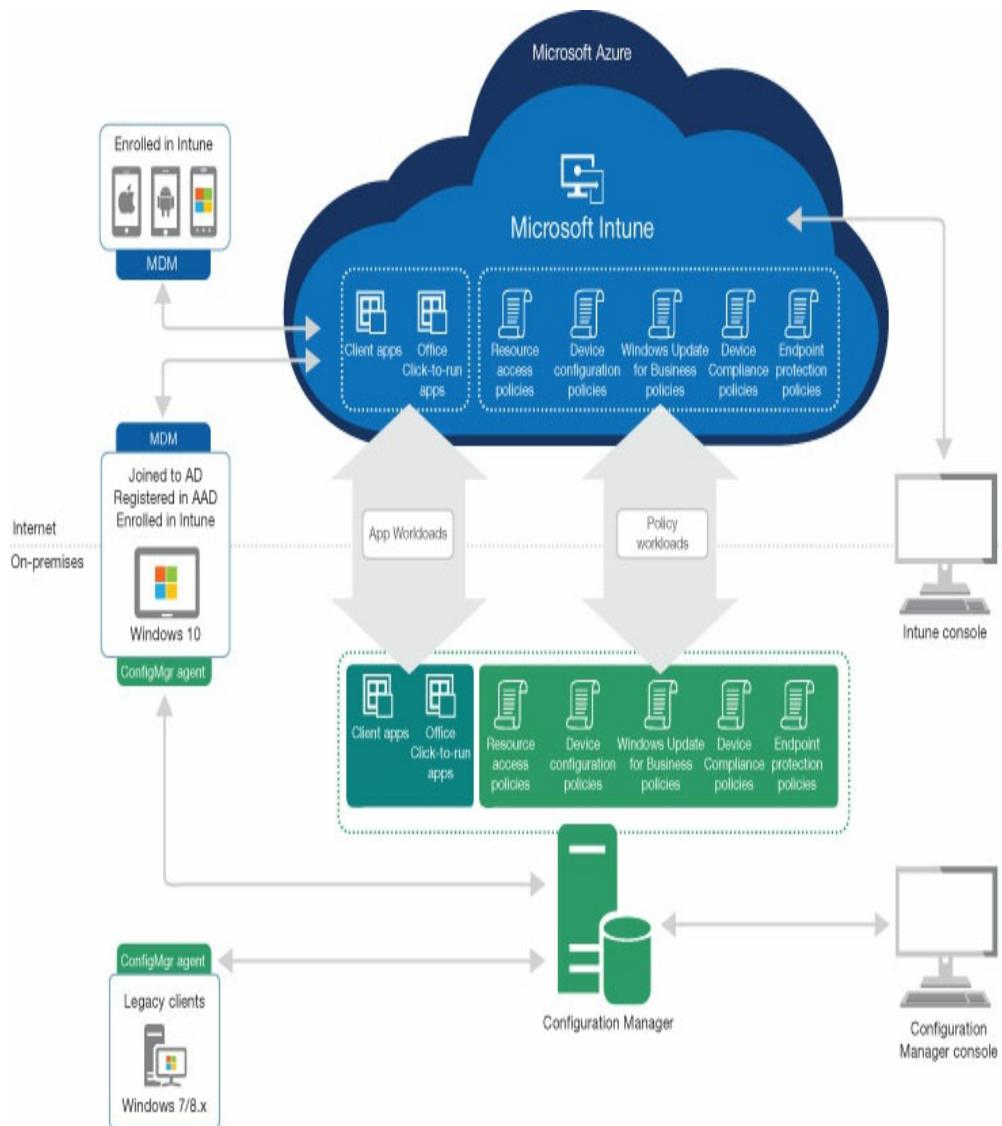
**Implementaciones piloto**

Al igual que con todas las implementaciones de nuevas tecnologías, Microsoft recomienda una pequeña implementación piloto para fines de evaluación antes de implementar cualquier producto en toda una empresa.

La implementación de la cogestión

la infraestructura es algo diferente para una empresa que busca administrar conjuntamente nuevas estaciones de trabajo con Windows 10 implementadas por un OEM o mediante el piloto automático de Windows, pero no proporciona a los usuarios identidades híbridas de AD DS / Azure AD. Los administradores deben implementar una puerta de enlace de administración en la nube en la red interna y obtener un certificado SSL público para ella, configurar Intune para instalar el agente de cliente SCCM en las nuevas computadoras y configurar a los clientes para usar la puerta de enlace.

Una vez que se completa la configuración de administración conjunta, SCCM y Microsoft Intune trabajan juntos con AD DS y Azure AD, como se muestra en Figura 3-28. .

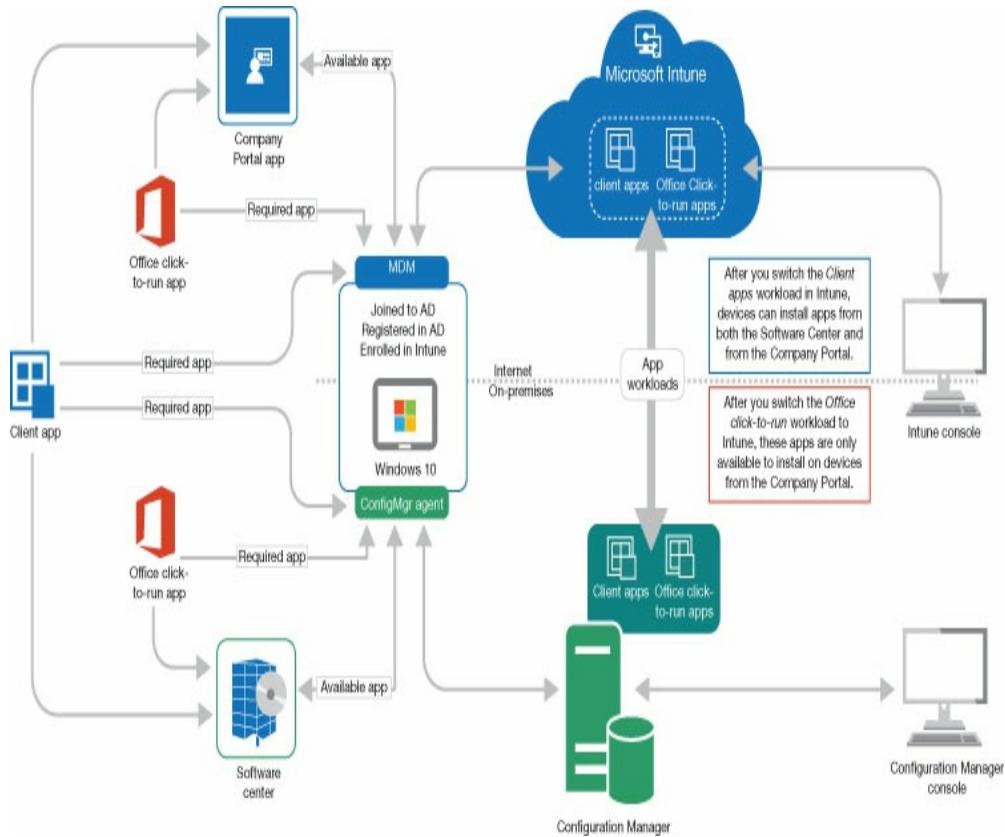


**FIGURA 3-28** System Center Configuration Manager y Microsoft Intune cogestión

En el Asistente de configuración de administración conjunta, también es posible seleccionar las cargas de trabajo que Microsoft Intune administrará, aunque los administradores también pueden hacerlo en cualquier momento después de implementar la administración conjunta. SCCM administra todas las cargas de trabajo hasta que

se desplazan explícitamente a Intune en su lugar. La función de administración de SCCM admite la transferencia de las siguientes cargas de trabajo a Intune:

- **Políticas de cumplimiento** Especifique las configuraciones y políticas de configuración que el dispositivo debe observar antes de que se le otorgue acceso condicional a los recursos de la red.
- **Políticas de actualización de Windows** Permita a los administradores definir políticas para la implementación de actualizaciones de calidad y características de Windows 10 en dispositivos que usan Windows Update para empresas.
- **Políticas de acceso a recursos** Proporcione la gestión de los dispositivos WiFi, la red privada virtual (VPN), el correo electrónico y la configuración de certificados.
- **Protección de punto final** Proporcione administración sobre todas las características antimalware de Windows Defender en dispositivos con Windows 10.
- **Configuración del dispositivo** Proporciona autoridad de administración para la configuración de administración de dispositivos, incluidos los incluidos en las políticas de acceso a recursos y las cargas de trabajo de protección de Endpoint. A pesar de transferir esta carga de trabajo a Intune, aún es posible configurar los ajustes del dispositivo en Configuration Manager, como los ajustes en SCCM que aún no se han implementado en Intune.
- **Aplicaciones de clic para ejecutar de Office** Proporcione autoridad de administración para todas las aplicaciones de Office 365.
- **Aplicaciones cliente** Proporcionar capacidad de implementación de aplicaciones. La transferencia de esta carga de trabajo a Intune permite que los dispositivos instalen aplicaciones desde Intune, usando el portal de la compañía, o desde SCCM, usando el Centro de software, como se muestra en Figura 3-29. .



**FIGURA 3-29** La carga de trabajo de la aplicación del cliente en un entorno comanaged

## Escenarios de uso de seguridad

La administración de los diversos tipos de puntos finales presenta a los administradores una variedad de problemas que deben abordar, incluidos los siguientes:

- **Dispositivos propiedad del usuario** Cuando los trabajadores usan sus propios dispositivos, los administradores deben definir una política que especifique qué grado de control tendrá la organización sobre los dispositivos y a qué recursos de la compañía se les permitirá acceder. Esta puede ser una tarea difícil porque, si bien la organización debe proteger sus recursos, los usuarios a menudo no están dispuestos a entregar el control total de su propiedad a

empresa. Windows Intune proporciona a los administradores capacidades de Administración de dispositivos móviles (MDM) y Administración de administración móvil (MAM), que proporcionan diferentes niveles de control de administración para satisfacer las necesidades de la organización y los usuarios.

- **Redes de dispositivos móviles** Los usuarios móviles a menudo se conectan a redes inalámbricas externas, como las de cafeterías y otras empresas, que no están aseguradas por la empresa. Esto deja a los dispositivos abiertos a la posibilidad de intrusión por parte de personas externas, exponiéndolos a amenazas potenciales que pueden poner en peligro el dispositivo, los datos almacenados en él y la red empresarial. Los administradores pueden usar Microsoft Intune u otras herramientas para crear y aplicar políticas de dispositivos móviles que requieren que los dispositivos tengan herramientas de prevención de malware, actualizaciones de software y otras formas de protección necesarias para repeler las amenazas.
  
- **Pérdida o robo del dispositivo.** Cualquier dispositivo móvil puede perderse o ser robado, con el peligro adicional de que cualquier información confidencial almacenada en el dispositivo pueda verse comprometida. También puede haber usuarios que abandonen la empresa en circunstancias poco amigables, llevándose consigo sus dispositivos personales. En algunos casos, el costo de reemplazar el hardware del dispositivo puede ser menor que el de identificar los datos que se han perdido y volver a crearlos. Los administradores deben prepararse para estas situaciones al diseñar una política de Microsoft Intune que pueda ejercer protección remota de los recursos de la organización, incluso cuando el dispositivo móvil está en manos hostiles.
  
- **Dispositivos infectados** Los dispositivos móviles que se infectan con malware mientras están conectados a redes externas pueden llevar esa infección a la empresa, dañar documentos y transmitir la infección a otros sistemas. Los administradores deben clasificar todos los dispositivos móviles que se conectan a la red empresarial como amenazas potenciales y protegerlos con herramientas como Windows Defender y System Center Endpoint Protection.
  
- **Sincronización de datos del dispositivo** Si bien los datos almacenados en la nube de Microsoft se replican en múltiples centros de datos para su protección, los dispositivos móviles que funcionan fuera de las instalaciones de la compañía no siempre están conectados a la nube. Por lo tanto, cuando los usuarios trabajan con la empresa.

documentos sin conexión, las revisiones que realicen a los documentos no se guardarán en la nube ni se realizarán copias de seguridad hasta que se conecten a la red. Por lo tanto, estos datos revisados se pueden perder si el dispositivo se daña, se pierde o se lo roban antes de que se conecte a la nube.

- **Cambios de contraseña** Una de las tareas más comunes para el personal y los administradores de la mesa de ayuda es la necesidad de cambiar las contraseñas de los usuarios. Esta tarea es aún más común cuando Azure AD Identity Protection está configurada para requerir un cambio de contraseña cuando sus niveles de riesgo basados en autenticación alcanzan un cierto valor. El restablecimiento de contraseña de autoservicio (SSPR) permite a los usuarios autenticados con éxito cambiar sus propias contraseñas, en lugar de requerir la intervención de un administrador.

## Abordar amenazas comunes

La gestión de riesgos es una empresa altamente especializada que depende en gran medida del tipo y la sensibilidad de la información a proteger y la naturaleza de las amenazas a las que la red es más vulnerable. Por ejemplo, una organización que consiste principalmente en profesionales de TI no será demasiado susceptible a los ataques de phishing porque tienen más conocimiento de ellos y experiencia con ellos. Por otro lado, una organización de usuarios con poca o ninguna experiencia en TI será mucho más vulnerable a esta amenaza particular y tendrá que hacer un mayor esfuerzo para tratar de prevenir este tipo de ataque.

Microsoft 365 incluye una amplia variedad de herramientas de seguridad que permiten predecir, prevenir y reaccionar a muchos tipos diferentes de amenazas. Muchas de estas herramientas son

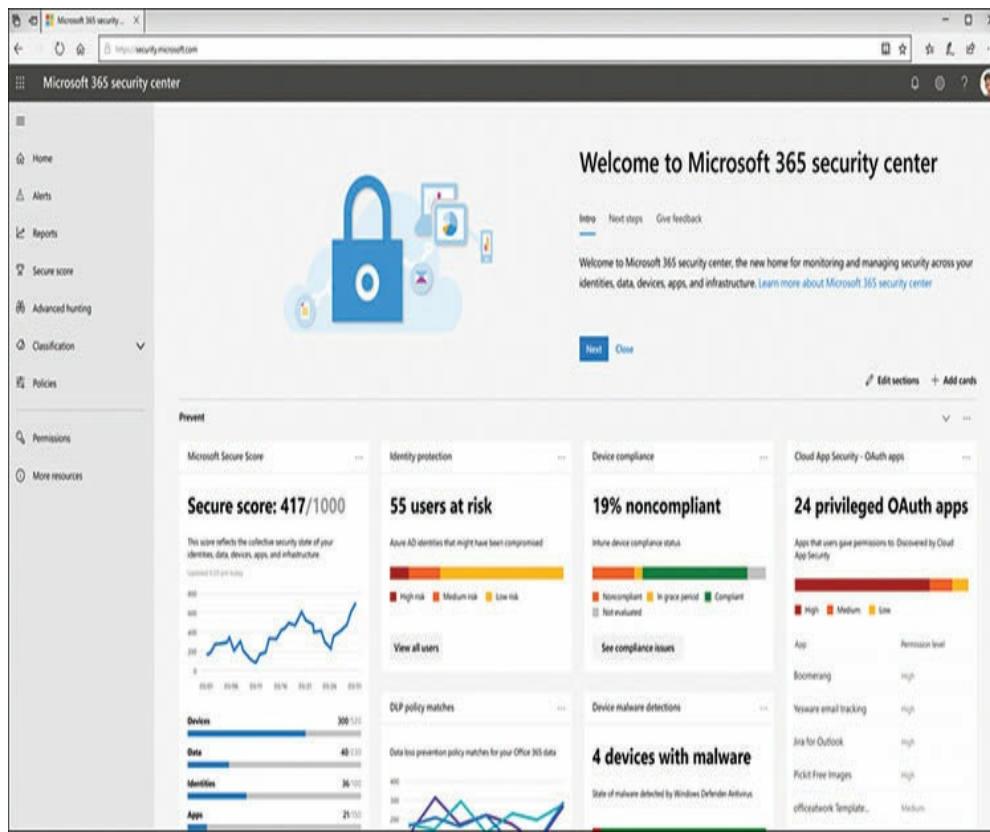
discutido individualmente, tanto en este capítulo como en otras partes de este libro. La naturaleza de la función de cada herramienta se explica en relación con los tipos de amenazas que aborda. Sin embargo, Microsoft anunció recientemente un esfuerzo para organizar los componentes de seguridad de Microsoft 365 con el nombre único *Protección contra amenazas de Microsoft*,

que ubica las herramientas en las siguientes cinco categorías:

- **Identidades** Herramientas que autentican, autorizan y protegen las cuentas de usuarios estándar y administradores privilegiados, como Windows Hello, Azure Active Directory Identity Protection, Privileged Identity Management, Azure Advanced Threat Protection y Microsoft Cloud App Security
- **Puntos finales** Herramientas que protegen los dispositivos y sensores del usuario de los efectos de pérdida, robo y ataque, como Microsoft Intune, System Center Configuration Manager, Windows 10, Microsoft Advanced Threat Analytics y Windows Defender Advanced Threat Protection
- **Datos del usuario** Herramientas que analizan documentos y mensajes en busca de contenido confidencial o malicioso, como Exchange Online Protection, Azure Information Protection, Data Loss Prevention, Windows Defender Advanced Threat Protection, Office 365 Advanced Threat Protection, Office 365 Threat Intelligence y Microsoft Cloud App Security
- **Aplicaciones en la nube** Herramientas que protegen aplicaciones de software como servicio (SaaS) como Office 365 y sus datos, como Exchange Online Protection, Office 365 Advanced Threat Protection y Microsoft Cloud App Security
- **Infraestructura** Herramientas que brindan protección a los servidores, tanto físicos como virtuales; bases de datos; y red, como Azure Security Center, Microsoft Advanced Threat Analytics y SQL Server

Sin embargo, Microsoft Threat Protection está destinado a ser más que una simple lista de herramientas individuales. Microsoft 365

también recopila información de todos estos componentes de seguridad y los acumula en un solo centro de seguridad de Microsoft 365, como se muestra en Figura 3-30 .



**FIGURA 3-30** Centro de seguridad de Microsoft 365

Las páginas del centro de seguridad de Microsoft 365, accesibles desde el panel de navegación de la izquierda, proporcionan lo siguiente:

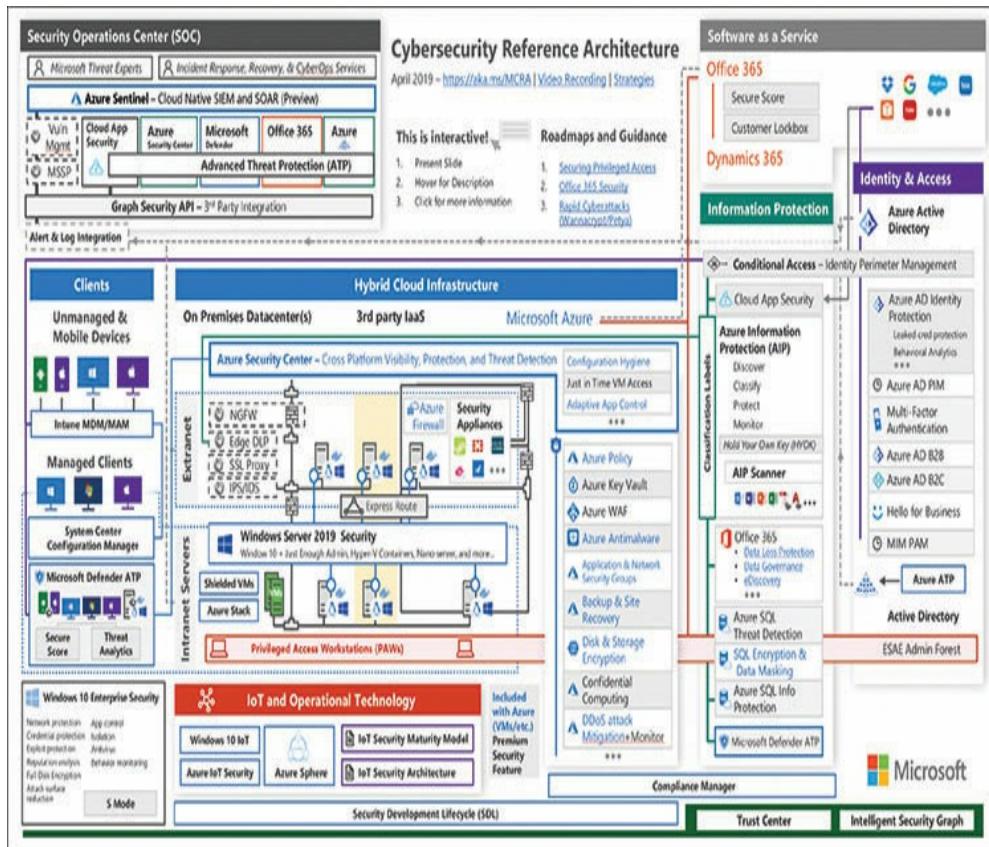
- **Hogar** Muestra un panel de control con mosaicos configurables que contienen indicadores de estado para los problemas de seguridad más importantes para un administrador u organización en particular.
- **Alertas** Muestra notificaciones generadas por otras herramientas de seguridad de Microsoft 365, incluidas Microsoft Cloud App Security, Office 365

Protección contra amenazas avanzada, Azure Active Directory y Protección contra amenazas avanzada de Microsoft Defender

- **Informes** Proporciona información detallada sobre el estado de seguridad de las identidades, dispositivos, datos, aplicaciones e infraestructura de la red.
- **Puntaje seguro** Proporciona una evaluación integral del estado actual de seguridad de la empresa en una puntuación numérica de 1,000
- **Caza avanzada** Proporciona acceso a las herramientas analíticas que pueden identificar de manera proactiva amenazas potenciales a las identidades, mensajes, datos y dispositivos de la red, como las herramientas de Protección contra amenazas avanzadas para Azure, Office 365 y Microsoft Defender
- **Clasificación** Proporciona acceso a herramientas para crear etiquetas de clasificación para las herramientas de protección de información de Microsoft 365
- **Políticas** Brinda la capacidad de crear políticas para una variedad de herramientas y propósitos de Microsoft 365, que incluyen Protección contra amenazas avanzada, alertas de Office 365 y Seguridad de aplicaciones en la nube

Microsoft 365 también va más allá del enfoque reactivo de la seguridad y proporciona herramientas que pueden ser proactivas al detectar ataques y otros problemas de seguridad antes de que ocurran, o cuando apenas han comenzado.

Las herramientas de Protección contra amenazas avanzadas para Azure, Office 365 y Microsoft Defender están diseñadas para monitorear el comportamiento de los usuarios, dispositivos y otros recursos de red y analizar la información que recopilan para detectar y anticipar comportamientos sospechosos. La inteligencia que las herramientas aplican a la tarea se basa en el Microsoft Intelligent Security Graph, una red de relaciones de seguridad que abarca toda la red. Arquitectura de referencia de seguridad cibernética de Microsoft, que se muestra en Figura 3-31 , ilustra estas relaciones.



**FIGURA 3-31 Arquitectura de referencia de seguridad cibernética de Microsoft**

*¿Necesita más revisión ?:*

## Arquitectura de referencia de seguridad cibernética de Microsoft

Para una versión interactiva de PowerPoint de la arquitectura que se muestra en Figura

3-31 , ver

<https://gallery.technet.microsoft.com/CybersecurityReference-883fb54c> .

### **Comprobación rápida**

- Microsoft Intune, que funciona por sí solo, se clasifica como ¿cuál de los siguientes tipos de herramientas de administración?
  - CMT
  - EMM
  - UEM
  - MDM

### **Respuesta de verificación rápida**

- Microsoft Intune se considera una herramienta de administración de movilidad empresarial (EMM) porque amplía las capacidades de administración de dispositivos móviles (MDM). Sin embargo, Intune está basado en la nube y no puede administrar clientes locales por sí mismo, por lo que no puede llamarse una herramienta de administración de clientes (CMT) o una herramienta unificada de administración de puntos finales (UEM).

## **HABILIDAD 3.4: ENTENDER EL PORTAL DE CONFIANZA DE SERVICIO Y EL GERENTE DE CUMPLIMIENTO**

---

Para muchos profesionales de TI, la perspectiva de implementar servicios vitales y almacenar información importante de la compañía en la nube se encuentra con una gran cantidad de temor. Pueden tener una reuencia instintiva a confiar en una infraestructura de TI que no está implementada en las computadoras que posee la compañía

y alojados en sus propios centros de datos. También pueden dudar en renunciar a su control personal sobre esas computadoras y sus recursos. Además, puede haber estatutos y estándares que la infraestructura de TI debe cumplir, ya sea por los términos contratados, las políticas de la empresa o los requisitos gubernamentales.

## Portal de confianza de servicio

Microsoft conoce estos problemas de confianza y ha creado un almacén central de información sobre ellos, denominado *Service Trust Portal (STP)*. STP es un sitio web que está disponible para todos en <http://aka.ms/stp>, aunque algunas partes del sitio están restringidas a usuarios registrados de Microsoft 365 y otros productos. Entre los muchos recursos en el sitio se encuentran enlaces a documentos en las siguientes categorías:

- **Informes de auditoría** Proporcione informes de auditoría y evaluación independientes de los servicios en la nube de Microsoft, evaluando su cumplimiento con estándares como los publicados por la Organización Internacional de Normalización (ISO), Controles de Organización de Servicios (SOC), Instituto Nacional de Estándares y Tecnología (NIST), Riesgo Federal y Autorización Programa de gestión (FedRAMP) y Reglamento general de protección de datos (GDPR)
- **Documentos y recursos** Consiste en una gran biblioteca de documentos, que incluye documentos técnicos, preguntas frecuentes, guías de cumplimiento, informes de pruebas de penetración, planos de seguridad y cumplimiento de Azure, y otros recursos de protección de datos
- **Gerente de Cumplimiento** Evalúa y califica el cumplimiento normativo de una organización, basado en múltiples estándares publicados

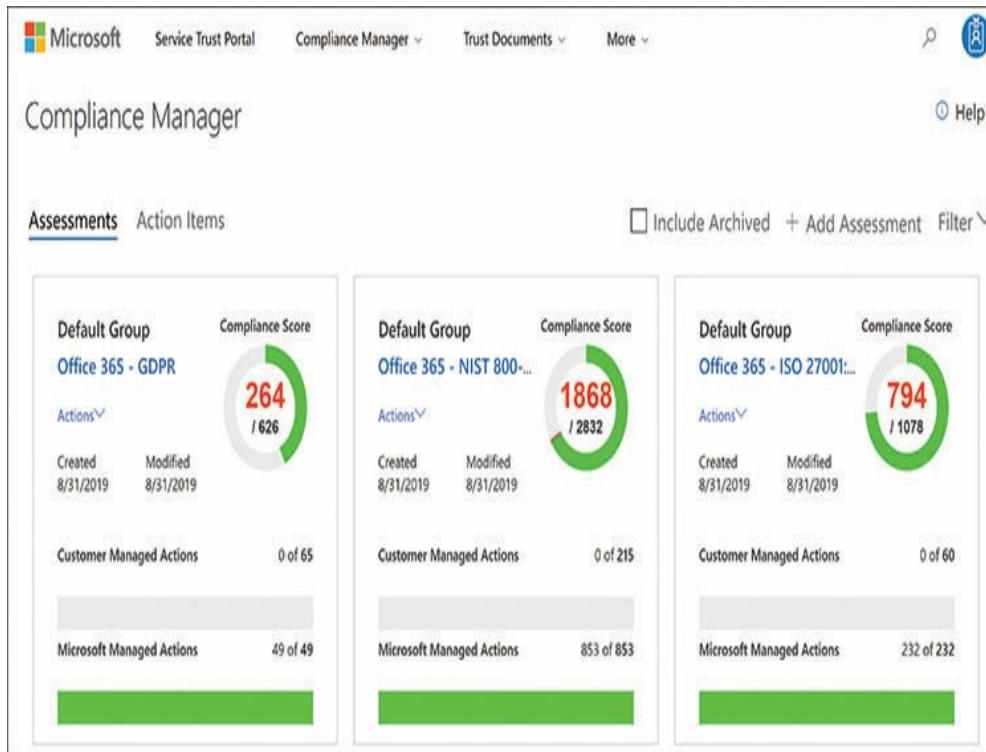
- **Industrias y Regiones** Proporcionar documentos que contengan información de cumplimiento para industrias específicas, como educación, servicios financieros, gobierno, atención médica, manufactura y venta minorista; y países específicos, incluidos Australia, República Checa, Alemania, Polonia, Rumania, España y Reino Unido
- **Centro de confianza** Enlaces al sitio del Centro de confianza, que proporciona documentación sobre los medios por los cuales Microsoft respalda la seguridad, la privacidad, el cumplimiento y la transparencia en sus servicios en la nube
- **Recursos** Proporcione información sobre los centros de datos globales de Microsoft, información de seguridad y cumplimiento para Office 365 y una lista de preguntas frecuentes para el Portal de confianza de servicio
- **Mi biblioteca** Permite a los usuarios anclar documentos del sitio en una página de usuario separada para una referencia rápida más adelante

## Gerente de Cumplimiento

Compliance Manager es una herramienta de evaluación de riesgos que permite a una organización rastrear y registrar las actividades que realizan para lograr el cumplimiento de estándares de certificación específicos. Una evaluación de la postura de cumplimiento de una organización se basa en las capacidades de los servicios en la nube de Microsoft 365 y en las formas en que la organización los utiliza, en comparación con un estándar, regulación o ley existente.

La página de inicio de la herramienta Administrador de cumplimiento contiene un panel que muestra mosaicos que representan las evaluaciones de los componentes de Office 365 y Azure con respecto a tres estándares diferentes, como se muestra Dibujo 332 . Cada mosaico especifica un servicio en la nube y el estándar con el que se compara. Los resultados de la

La comparación se establece como una puntuación numérica.



**FIGURA 3-32** El panel de evaluaciones de Compliance Manager

Al seleccionar un mosaico, se muestra una lista detallada de los controles probados para la evaluación, junto con los resultados de cada control individual, como se muestra en Figura 3-33. Los controles se dividen en aquellos de los cuales Microsoft es responsable y aquellos de los cuales el cliente es responsable. Cada entrada de control contiene una referencia a una sección o artículo en el estándar que corresponde al control; información sobre quién probó el control y cuándo; y los resultados de la prueba, que se expresa como un valor de puntaje de cumplimiento individual.

Microsoft Managed Controls					
Conditions for collection and processing					
Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: 8.2.1 Control Title: Cooperation agreement	8	Implemented	10/19/2016	Third-party independent auditor	✓
<p>Supported GDPR Article(s): Article (28)(3)(e), Article (28)(3)(f), Article (28)(9), Article (35)(1)</p> <p>Description: Article (28)(3): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:</p> <ul style="list-style-type: none"> <li>(e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III</li> <li>(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing</li> </ul>					

**FIGURA 3-33 Un control administrado de Microsoft en Compliance Manager**

En la vista predeterminada de una evaluación de Compliance Manager, los controles administrados por Microsoft están completos con resultados y puntajes de cumplimiento, pero los controles administrados por el cliente no. Depende del suscriptor completar estos controles y usar la guía y las recomendaciones de cada uno para finalizar la evaluación y generar una puntuación general que refleje el cumplimiento de Microsoft y la organización con el estándar seleccionado.

## La adopción de la nube muestra

Para cualquier organización que contemple o anticipa un movimiento hacia la nube, hay problemas que deben contemplar antes de tomar una decisión final. En algunos casos, los responsables de la toma de decisiones de la empresa pueden no estar seguros de si los proveedores basados en la nube pueden ofrecer los servicios que necesita la organización. En otros casos, no cabe duda de que la nube puede proporcionar los servicios necesarios, pero existe una indecisión sobre cómo implementar realmente una transición de los servicios locales a los servicios basados en la nube.

Ambos tipos de problemas a veces pueden ser "showstoppers" que evitan que ocurra una implementación en la nube. Microsoft ha considerado muchos de estos problemas críticos de adopción, como se muestra anteriormente en la extensa documentación proporcionada en el Portal de confianza de servicio y las herramientas del Administrador de la compañía. Sin embargo, a veces las consideraciones involucradas en una situación de transición a la nube son exclusivas de una industria o una compañía individual, o son más legales o financieras que técnicas, y las soluciones deben generarse internamente en lugar de ser provistas por un producto o servicio como Microsoft 365

Las siguientes secciones abordan algunos de los mejores ejemplos de adopción de la nube más comunes y brindan enfoques que las empresas pueden adoptar para abordarlos.

## Anticipando latencia de rendimiento

¿Pueden los servicios basados en la nube proporcionar los niveles de rendimiento?

que la organización está acostumbrada a lograr con recursos locales? Los profesionales de TI familiarizados con los problemas de servicio a los que pueden estar sujetos los proveedores de servicios de Internet e Internet en sí mismos podrían preguntarse si es posible un alto nivel de rendimiento consistentemente con servicios basados en la nube. El rendimiento consistentemente cómodo de una planta de cable interno, sobre el cual la compañía tiene control total, es algo difícil de perder. Puede haber dudas sobre si pueden ocurrir interrupciones del servicio o períodos de mayor latencia que pueden afectar la productividad y dañar la reputación de la empresa con sus socios y clientes.

Al considerar cualquier proveedor de servicios en la nube, el suscriptor potencial debe investigar el registro de rendimiento del servicio del proveedor, tanto examinando los datos que proporcionan como contactando a sus otros clientes. La mayoría de los proveedores incluyen un Acuerdo de Nivel de Servicio (SLA) en sus contratos que explica la disponibilidad del servicio, pero los subscriptores potenciales también deben preguntar sobre la posibilidad de un SLA de nivel de rendimiento.

También se recomienda un examen de la infraestructura de hardware del proveedor, para determinar dónde están ubicados sus centros de datos cerca de los sitios de la compañía. Microsoft ha abordado este problema al construir una red global de centros de datos y al recomendar que los subscriptores de Microsoft 365 realicen un examen detallado de su propia red

infraestructura. Esto es para garantizar que cada ubicación de la empresa acceda a los servicios en la nube de Microsoft a través del punto final de la Red Global de Microsoft más cercano a su ubicación física.

*Readeraid:*

## Redes

### Infraestructura y Microsoft 365

Para obtener más información sobre el examen de infraestructura de red recomendado como parte de la implementación de Microsoft 365, consulte "Fase 1: Redes" Sección en Capítulo 2, "Comprender los servicios y conceptos básicos de Microsoft 365".

### Seleccionar proveedores de servicios

El proceso de elegir proveedores de servicios es, por supuesto, crítico para cualquier implementación en la nube. Una de las primeras preguntas a considerar es si se debe usar un solo proveedor para todos los servicios que la organización requiere o evaluar a varios proveedores para servicios individuales. Elegir un proveedor para todo minimiza la posibilidad de brechas en el servicio, pero también crea un único punto de falla. Es posible que el proveedor seleccionado tampoco proporcione el mejor precio para cada uno de los servicios necesarios.

Para los suscriptores de Microsoft 365, por supuesto, no hay elección de proveedores para los servicios incluidos en el producto, pero esto no significa que una organización deba usar Microsoft para toda su infraestructura en la nube.

El uso de múltiples proveedores para diversos servicios podría permitir a la empresa negociar los mejores términos para cada uno, y también le permite a la empresa mantener relaciones con más de un proveedor, de modo que los servicios se puedan trasladar a otro proveedor si las circunstancias lo requieren. Sin embargo, tratar con múltiples proveedores de servicios en la nube requiere una planificación meticulosa para garantizar que la empresa reciba todos los servicios que necesita.

La organización debe tener un diseño completo de infraestructura de red antes de contratar a cualquier proveedor, y es necesaria una comparación cuidadosa de los contratos para los proveedores para asegurarse de que todos los servicios solicitados en el plan estén disponibles y contabilizados. Al agregar un nuevo servicio a una infraestructura existente basada en la nube, los administradores deben comparar los nuevos contratos de posibles proveedores con todos los contratos existentes que estén vigentes.

El peor de los casos, en este caso, sería la comprensión tardía de que ninguno de los proveedores de servicios comprometidos está suministrando un componente de infraestructura vital y que ninguno de los proveedores puede suministrarlo. Estas brechas de servicio pueden ser costosas y embarazosas para las personas responsables.

### **Evitar el bloqueo del proveedor**

Estar encerrado en un solo proveedor es una de las preocupaciones

de muchas organizaciones que consideran una infraestructura basada en la nube. Los precios y otras estipulaciones del contrato pueden cambiar con el tiempo, y podría ser necesario cambiar de proveedor cuando varios proveedores brinden los mismos servicios en el futuro. Para prepararse para esta eventualidad, los contratos con proveedores de servicios en la nube siempre deben incluir una estrategia de salida y un lenguaje con respecto a la novación del contrato, ya sea temprano o no.

Una preocupación particularmente importante debería ser el tema de la recuperación de datos. Una gran red empresarial basada en la nube puede generar enormes cantidades de datos en el transcurso de varios años. En el caso de un cambio de proveedor, el proceso de reclamar esos datos del servicio en la nube de un proveedor y pasarlo al de otro puede ser extremadamente largo. El plan de infraestructura en la nube de la organización debe tener en cuenta esta eventualidad, al igual que los contratos con los proveedores antiguos y los nuevos.

### Evaluación de la solidez del proveedor

Al momento de escribir este artículo, el negocio de proporcionar servicios de redes en la nube está dominado por tres compañías muy grandes, ninguna de las cuales parece estar en peligro de fallar en el corto plazo. Sin embargo, existen otros proveedores más pequeños y pueden ofrecer términos tentadores para sus servicios. Al considerar proveedores más pequeños, los posibles suscriptores deben investigar el estado de

sus negocios a fondo. Los responsables de la toma de decisiones deben sopesar el riesgo de contratar a un pequeño proveedor, que posiblemente podría fallar en algún momento en el futuro, con las consecuencias comerciales de tal falla, como el posible tiempo de inactividad de la red e incluso la pérdida de datos.

### **Comparación de modelos de costos**

Comparar el costo financiero de una infraestructura basada en la nube con una infraestructura local es difícil porque utilizan modelos completamente diferentes. Una red local requiere un gran desembolso por hardware y gastos de implementación, pero una vez que ese costo se ha amortizado, la red es propiedad de la empresa y el gasto continuo se reduce sustancialmente. Una infraestructura basada en la nube requiere un desembolso inicial mucho menor, pero las tarifas de los suscriptores pueden ser sustanciales y persistentes mientras la empresa utilice el servicio.

También hay otros factores de costo a considerar. En el modelo local, la empresa debe planificar el crecimiento futuro y ajustar todo el proceso de implementación para tener en cuenta los recursos que podrían no ser necesarios durante años. Con una infraestructura basada en la nube, el suscriptor puede contratar los servicios que necesita en este momento y agregar más (o eliminar) la funcionalidad más adelante, cuando sea necesario.

Para anticipar el TCO (costo total de propiedad) para una red basada en la nube versus una red local

infraestructura, una práctica recomendada sería totalizar todos los gastos necesarios para cada modelo durante un período de dos a tres años. Sin embargo, el TCO no necesariamente proporciona la imagen completa. La solución en la nube puede proporcionar otros beneficios que son más difíciles de cuantificar financieramente. Por ejemplo, los servicios suscritos a la nube pueden ampliarse o reducirse con efecto inmediato. Por lo general, los proveedores de la nube pueden implementar nuevos servidores virtuales, agregar recursos a los existentes o incluso proporcionar servicios completamente nuevos casi de inmediato. En una red local, una expansión puede requerir la compra, instalación e implementación de nuevo hardware, lo que puede llevar semanas o meses. La escalabilidad puede ser un factor importante para una empresa que experimenta fluctuaciones estacionales significativas en los negocios.

### **Asegurar los datos de la compañía**

Podría decirse que la mayor preocupación para muchos profesionales de TI que consideran una infraestructura de red basada en la nube es el riesgo de que sus datos se pierdan o se vean comprometidos. Microsoft, y presumiblemente otros proveedores de servicios en la nube de buena reputación.

- tenga en cuenta en sus descripciones de servicio los mecanismos que utilizan para proteger los datos de los suscriptores, como el almacenamiento replicado en múltiples centros de datos. Los contratos también incluyen habitualmente un SLA que especifica un porcentaje de tiempo de actividad garantizado (99.9 por ciento, en el caso de Microsoft),

que casi asegura la disponibilidad de los datos. Sin embargo, si bien el contrato podría imponer una multa al proveedor si no cumple con los términos del SLA, es casi seguro que no será financieramente responsable de las pérdidas en que incurra el suscriptor debido al tiempo de inactividad.

No hay forma de evitar el hecho de que los datos almacenados en la nube pública tienen un mayor riesgo de verse comprometidos que los datos almacenados en los servidores locales del suscriptor. Para abordar este riesgo, Microsoft 365 incluye herramientas de seguridad que, cuando se usan correctamente, pueden ayudar a mitigar el riesgo de penetración de identidades y acceso a datos por parte de personas no autorizadas. Sin embargo, la carga de aplicar esta protección y de exponer datos confidenciales al riesgo recae en primer lugar en el suscriptor.

Depende de los administradores de la red evaluar la sensibilidad de los datos de la compañía, clasificar los datos utilizando una taxonomía acordada de niveles de sensibilidad (como se discutió en la sección "Protección de documentos", anteriormente en este capítulo), y decidir qué medidas debe usar para proteger los datos en cada nivel. Por lo tanto, la organización sn que trabaja con datos extremadamente confidenciales podría optar por almacenarlos en las instalaciones, en lugar de permitirlos en la nube.

También debe depender del suscriptor asegurarse de que todos los datos, ya sean almacenados en la nube o en las instalaciones, se respalden regularmente, ya sea el proveedor de la nube

Incluye este servicio o no. Si las copias de seguridad también deben almacenarse en la nube, la mejor práctica sería utilizar un proveedor diferente para las copias de seguridad, de modo que los datos se almacenen en una red separada de centros de datos.

## **Ubicar datos de la compañía**

Para las organizaciones que están sujetas a restricciones de almacenamiento de datos impuestas por sus clientes o por entidades gubernamentales, las ubicaciones exactas de los centros de datos de un proveedor de servicios en la nube pueden ser significativas. La red de Microsoft Azure se divide en 54 regiones (que se muestran en Dibujo 334 ) y 18 geografías que permiten a los suscriptores mantener sus datos en lugares que pueden cumplir con los requisitos específicos de residencia, soberanía, cumplimiento o resistencia que podrían verse obligados a observar. Sin embargo, esto no es necesariamente cierto para todos los proveedores de nube pública, y los suscriptores potenciales sujetos a tales restricciones deben exigir a los proveedores que incluyan un lenguaje de contrato que especifique dónde se almacenarán sus datos.

**54** regions worldwide    **140** available in  
140 countries



**FIGURA 3-34** Mapa de regiones de Microsoft Azure

*Nota:*

## Microsoft Azure

### Gobierno

Microsoft mantiene una nube dedicada para las agencias gubernamentales federales, estatales y locales de los Estados Unidos y sus socios, que cumple con una gran cantidad de estándares gubernamentales, incluidos FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4 y CJIS. Los centros de datos para esta nube del gobierno están ubicados dentro de los Estados Unidos y están físicamente aislados, al igual que las redes dentro de ellos. Además de los cuatro gobiernos estadounidenses dedicados

**En las regiones de Iowa, Texas, Arizona y Virginia que se muestran en el mapa, hay otras dos regiones secretas del gobierno de EE. UU. en ubicaciones no reveladas.**

## Obteniendo personal calificado

Debido a que los servicios basados en la nube son una tecnología relativamente nueva, no hay tantos administradores calificados y personas de soporte para ellos como las que existen para las tecnologías de redes locales tradicionales. Esto puede significar una empresa que tiene una infraestructura de red local establecida pero que está considerando agregar o migrar a los servicios en la nube, el personal de TI existente podría carecer de la experiencia necesaria para soportar adecuadamente las tecnologías en la nube.

Una forma efectiva de abordar este problema sin reemplazar a todo o parte del personal de TI es capacitar o reclutar primero un equipo de diseño y planificación de infraestructura de red de nube central. Entonces, ese equipo puede funcionar como mentores para el personal de TI que requieren una reorientación a las metodologías en la nube.

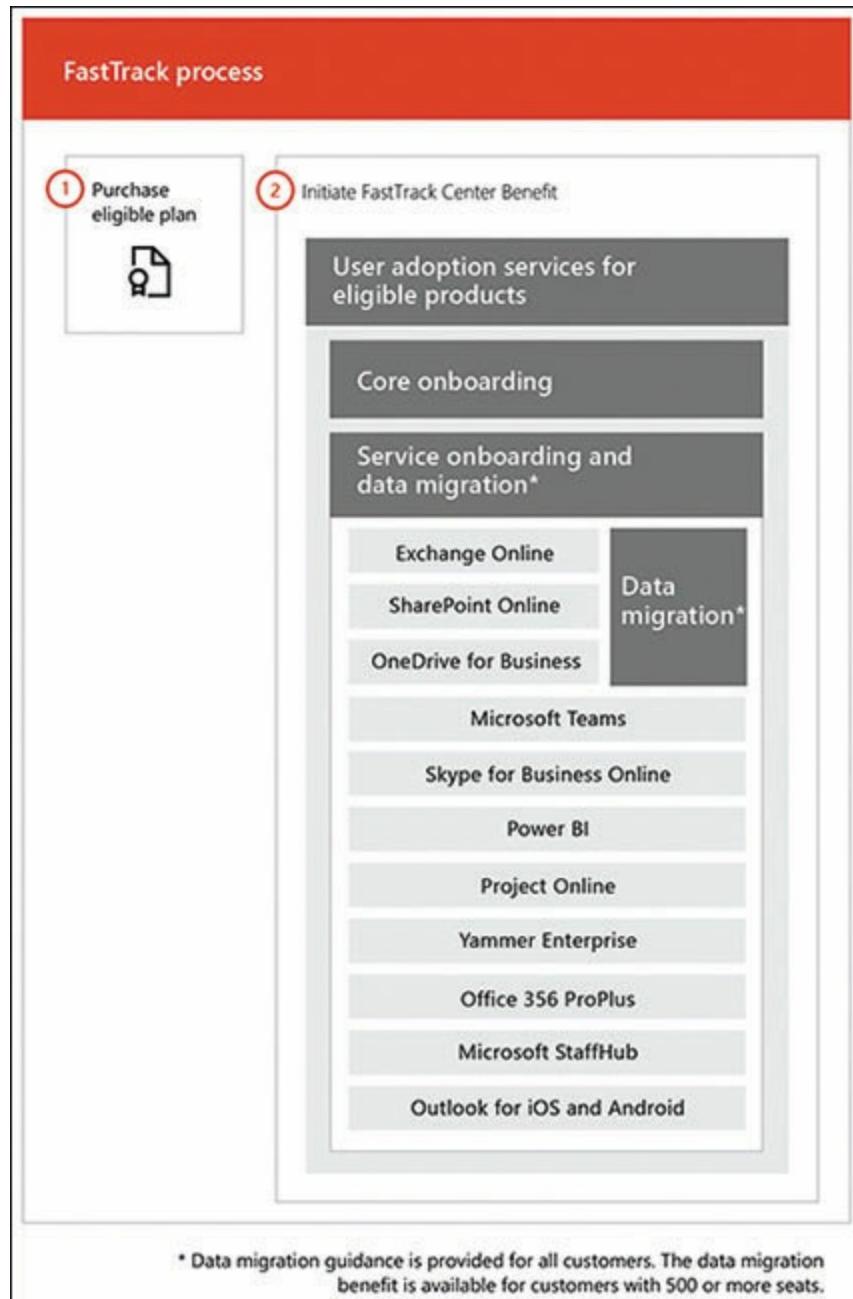
## Transición a la nube

Para los administradores de red locales tradicionales y el personal de soporte, una transición a los servicios basados en la nube puede ser un replanteamiento importante de cómo hacen casi todo, y muchas organizaciones son reticentes a realizar el cambio por ese motivo. Los proveedores de servicios en la nube tienen

Sin embargo, reconoció esto y podría proporcionar ayuda para los suscriptores que se mudan a la nube por primera vez.

El programa FastTrack de Microsoft está diseñado para este propósito exacto, brindando a las organizaciones un número específico de suscriptores de Microsoft 365 con una ruta claramente definida en la nube y ayuda de incorporación, sin costo adicional. Microsoft mantiene su propio equipo FastTrack, así como una red de socios que pueden proporcionar asistencia de transición al dividir el proceso en las siguientes tres etapas:

- **Imaginando** Proporciona al suscriptor información sobre los recursos disponibles e identifica escenarios específicos del negocio para ayudar en la creación de un plan general de implementación y migración en la nube atendiendo a las necesidades de la organización
- **Inducción** Se da cuenta del plan creado durante la fase de visualización mediante la configuración de los servicios en la nube; migrar archivos, tiendas de correo electrónico y contenido web; y creando usuarios y grupos, como se muestra en Figura 3-35
- **Valor de conducción** Ayuda al suscriptor a desarrollar prácticas de administración y mantenimiento eficientes y brinda ayuda continua al personal para trabajar con las tecnologías de Microsoft 365 y adaptarlas al modelo de negocio de la organización



**FIGURA 3-35 El proceso de incorporación de Microsoft 365**

FastTrack

No todos los proveedores de servicios en la nube tienen un programa como

esto, pero algunos proporcionarán asistencia; Además, hay consultores externos que pueden ayudar a una organización a lidiar con los problemas que surgen durante la transición a una infraestructura basada en la nube. Los profesionales de TI que dudan en adoptar tecnologías en la nube, incluso después de darse cuenta de las ventajas que brindan, tienen muchos recursos disponibles para recibir asistencia.

## RESUMEN

---

- El proceso de crear un plan de seguridad para una empresa se conoce como *gestión de riesgos*.
- Microsoft 365 incluye tecnologías de seguridad que se dividen en cuatro áreas: administración de seguridad, protección basada en identidad, protección de información y protección contra amenazas
- Una implementación de seguridad integral debe distribuir la protección entre los cuatro pilares principales que respaldan la infraestructura empresarial: Identidad, Documentos, Red y Dispositivos. Una identidad es una representación lógica de un usuario en un entorno de red.
- Para los usuarios, una identidad es un nombre que escriben para iniciar sesión en la red. Para los administradores, una identidad es una colección de atributos asociados con un individuo en particular.
- Hay tres medios básicos para autenticar la identidad de un individuo. El individuo debe proporcionar uno o más de los siguientes: algo que sabe, algo que es o algo que tiene. La gestión unificada de puntos finales (UEM) es una plataforma de gestión que puede funcionar con dispositivos locales y basados en la nube, y se puede ampliar para incluir nuevas tecnologías a medida que se desarrollan, como Internet de las cosas (IoT).
- Para lograr una verdadera solución Unified Endpoint Management con

En los productos de Microsoft, se necesita una combinación de System Center Configuration Manager y Microsoft Intune, en un acuerdo denominado *cogestión*

- El Service Trust Portal (STP) es un almacén central de información sobre la confianza en la nube y los problemas de cumplimiento de estándares. Muchos responsables de la toma de decisiones de la empresa no están seguros de si los proveedores basados en la nube pueden ofrecer los servicios que la organización necesita o no tienen claro cómo implementar realmente una migración a la nube. En ocasiones, estos problemas pueden ser "showstoppers" que evitan que se produzca una implementación en la nube, a menos que las soluciones se consideren cuidadosamente.

## EXPERIMENTO MENTAL

---

En este experimento mental, demuestre sus habilidades y conocimiento de los temas tratados en este capítulo. Puede encontrar la respuesta a este experimento mental en la siguiente sección.

Ralph es el Director del centro de datos de Brooklyn en Contoso Corp. La compañía actualmente tiene tres edificios de oficinas en el área de Nueva York con un total de 600 usuarios. Hay centros de datos en los tres edificios, todos los cuales se basan en productos de servidor de Microsoft y se administran utilizando System Center Configuration Manager. Los tres centros de datos están repletos de equipos y no tienen espacio para una mayor expansión. Ralph está convencido de que sería mejor para la compañía expandirse a la nube y comprar suscripciones de Microsoft 365 para los 600 usuarios en lugar de comprar un

propiedad adicional y construir un cuarto centro de datos desde cero.

Dado que el costo de los bienes raíces y la construcción en Nueva York es lo que es, el aspecto financiero de una expansión en la nube es responsable para la empresa. Sin embargo, todavía hay una oposición significativa a la propuesta de Ralph por parte de los otros dos directores del centro de datos y del director de tecnología:

**1) Ninguno del personal de administración de TI, incluido Ralph, tiene mucho experiencia con tecnologías en la nube.**

**2) Se teme que el almacenamiento de datos de la empresa en la nube no será seguro.**

**3) Hay preocupaciones de que el desempeño del cliente de la compañía**

El portal, una base de datos de catálogo que requirió un gran esfuerzo de desarrollo, se verá afectado por el tiempo de inactividad del servicio en la nube y los problemas de latencia de Internet.

Ralph debe preparar una presentación que promueva su proyecto en la nube y aborde estas tres preocupaciones. Utilizando lo que ha aprendido sobre la confianza del servicio en la nube y los problemas de implementación, proponga una solución para cada una de las tres preocupaciones que Ralph debe abordar en su presentación.

## PENSAMIENTO RESPUESTA DEL EXPERIMENTO

---

Ralph puede abordar las preocupaciones de los otros directores y el CTO de las siguientes maneras:

**1) El programa FastTrack de Microsoft está diseñado para proporcionar soporte gratuito para**

nuevos suscriptores en la nube durante sus procesos de diseño e implementación de infraestructura, así como soporte continuo para el personal de administración.

- 2) Microsoft 365 incluye herramientas como Azure AD Identity Protection, Azure Information Protection y Office 365 Advanced Threat Protection que permiten a los administradores proteger las identidades de los usuarios y elevar la seguridad de los datos de la empresa almacenados en la nube en función de su sensibilidad.**

- 3) Los contratos de Microsoft incluyen un acuerdo de nivel de servicio que garantiza 99.9 por ciento de tiempo de actividad. El proceso de implementación de Microsoft 365 también incluye una fase de red en la que la compañía evalúa su infraestructura de acceso a Internet para garantizar que todos los clientes y administradores de Microsoft 365 tengan suficiente conectividad a Internet para acceder a los recursos en la nube que requieren de forma regular.**

# **Capítulo 4. Comprender los precios y el soporte de Microsoft 365**

Microsoft 365 está diseñado para ser una solución completa para organizaciones de varios tamaños que proporciona el sistema operativo, las aplicaciones de productividad y los servicios basados en la nube que la mayoría de los usuarios necesitan. Para muchas empresas, Microsoft 365 puede ser una solución completa; otros podrían tener que instalar aplicaciones adicionales también.

Los candidatos que se preparan para el examen MS-900 deben comprender los componentes incluidos en los paquetes de Microsoft 365 y las características y beneficios que proporcionan, como se discutió en los capítulos anteriores. Sin embargo, también deben conocer las diversas opciones de licencia disponibles para los suscriptores de Microsoft 365, cómo tienen un precio, qué opciones de soporte están disponibles y cuál es el ciclo de vida esperado del producto Microsoft 365. Esta información es necesaria para que los profesionales de TI tomen una decisión de compra informada para sus organizaciones.

## Habilidades en este capítulo:

- Comprenda las opciones de licencia disponibles en el plan Microsoft 365,
- prediga y compare precios
- Describir las ofertas de soporte para los servicios de Microsoft 365 Comprender
- el ciclo de vida del servicio en Microsoft 365

## HABILIDAD 4.1: ENTENDER LAS OPCIONES DE LICENCIA DISPONIBLES EN MICROSOFT 365

---

Microsoft 365 no es un producto de "talla única". Su objetivo es admitir una variedad de tamaños de organizaciones y también organizaciones con diferentes requisitos de seguridad y características. Para hacer esto, hay varias ediciones del producto que tienen diferentes conjuntos de características y, por supuesto, diferentes precios. Al igual que con Office 365, Microsoft 365 está disponible solo por suscripción, pero a diferencia de Office

365, no es necesario que los suscriptores compren un sistema operativo.

Todas las ediciones de Microsoft 365 incluyen los siguientes tres componentes básicos:

- Windows 10 Enterprise Office
- 365 Pro Plus
- Movilidad empresarial + seguridad

Sin embargo, todos estos componentes están disponibles en su

planes propios, y las ediciones de Microsoft 365 los incluyen en varias combinaciones.

## **Microsoft 365 suscripciones**

La mayoría de las organizaciones interesadas en Microsoft 365 como introducción a las redes basadas en la nube, ya sea como una nueva implementación o como una adición a una red local tradicional, optarán por Microsoft 365 Business o una de las opciones de suscripción de Microsoft 365 Enterprise que se describen a continuación. Además, hay versiones especializadas de Microsoft 365 diseñadas para entornos educativos y gubernamentales.

### **Microsoft 365 Business**

Destinada a pequeñas y medianas empresas con hasta 300 usuarios, la suscripción a Microsoft 365 Business incluye Windows 10 Pro, Office 365 Pro Plus y la mayoría (pero no todas) de las características incluidas en Enterprise Mobility + Security E3. La intención detrás del producto es crear un paquete integral para organizaciones que no mantienen un personal de TI a tiempo completo, como es el caso de muchas pequeñas empresas. El proceso de implementación de estaciones de trabajo de Microsoft 365 está en gran medida automatizado, y el paquete incluye el Centro de administración de Microsoft 365, que proporciona una interfaz unificada para la configuración y administración de identidades y dispositivos.

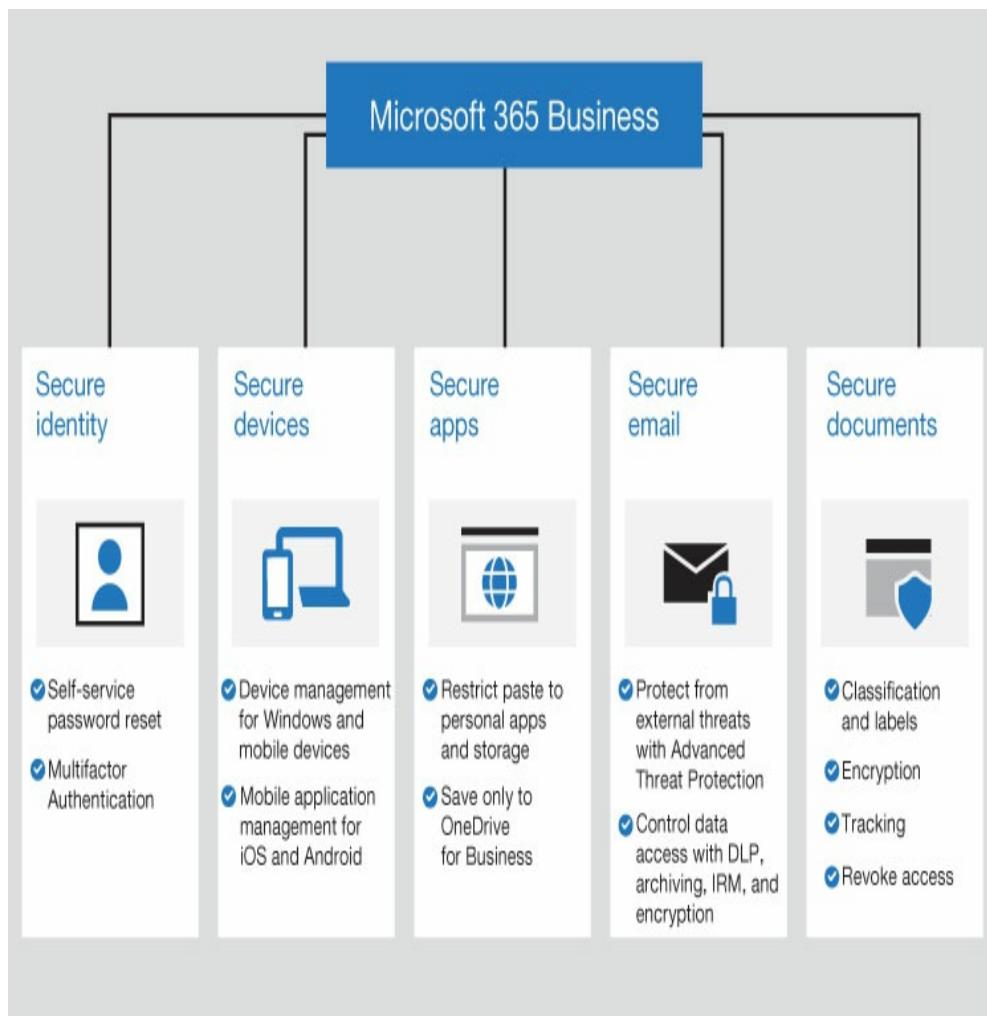
Microsoft 365 Business incluye Windows Autopilot, que simplifica el proceso de implementación de nuevas estaciones de trabajo de Windows o la actualización de las existentes. Para las computadoras que ya tienen instalado Windows 7, Windows 8 o Windows 8.1, Microsoft 365 proporciona una actualización a Windows 10 Pro. Además del piloto automático, Microsoft 365 incluye configuraciones de administración de dispositivos en Azure Active Directory que pueden aplicar automáticamente políticas a estaciones de trabajo recientemente implementadas, incluidas aquellas para funciones como las siguientes:

- Activación de la suscripción a Microsoft 365 Windows 10 y
- actualizaciones de Office 365
- Instalación automatizada de aplicaciones de Office 365 en Windows 10 Control de la pantalla del dispositivo cuando el sistema está inactivo Control de acceso a aplicaciones de Microsoft Store
- Control de acceso a Cortana
- 
- Control de acceso a consejos y anuncios de Windows de Microsoft

Otra prioridad de Microsoft 365 es proporcionar seguridad en áreas donde las pequeñas empresas a menudo se quedan cortas, como se muestra en Figura 4-1 .

El conjunto de funciones y servicios de seguridad incluidos en el producto proporciona protección para todas las áreas principales de una red empresarial: identidades, con autenticación multifactorial; dispositivos, con capacidades de gestión para dispositivos locales y móviles; aplicaciones, con restricciones de uso; correo electrónico, con detección de amenazas y prevención de pérdida de datos; y

documentos, con clasificación, encriptación y control de acceso.



**FIGURA 4-1** Funciones de seguridad en Microsoft 365 Business

Microsoft 365 Business permite hasta 300 suscripciones de usuarios en una tenencia, pero esto no significa que la red de una organización esté limitada a 300 usuarios. No es necesario que todos los usuarios de la red tengan un

Licencia de Microsoft 365 Business, aunque solo los titulares de licencias pueden utilizar los servicios en la nube incluidos con el producto. También es posible combinar tipos de licencia en un solo arrendamiento. Esto significa que si una organización que ejecuta Microsoft 365 Business se expande hasta el punto en que hay más de 300 usuarios, es posible agregar más usuarios con licencias de Microsoft 365 Enterprise sin tener que actualizar los 300 usuarios originales de Business.

## **Microsoft 365 Enterprise**

Para las organizaciones con más de 300 usuarios, hay dos opciones de suscripción, llamadas Microsoft 365 Enterprise E3 y Microsoft 365 Enterprise E5. Ambos incluyen Windows 10 Enterprise y Office 365 Pro Plus, así como Enterprise Mobility + Security, y ambos admiten un número ilimitado de usuarios. Las listas de características para las suscripciones E3 y E5 son en gran medida idénticas, con Microsoft 365 Enterprise E5 que incluye todas las características de E3 más herramientas de seguridad, protección contra amenazas y análisis más avanzadas.



---

### ***Consejo de examen***

**Los candidatos para el examen MS-900 deben entender que si bien Microsoft 365 Enterprise está dirigido a organizaciones más grandes, más**

No se requieren más de 300 usuarios. Las pequeñas y medianas empresas que requieren seguridad adicional y capacidades analíticas en el producto Enterprise E3 o E5 también pueden usarlo.

---

Varios de los elementos incluidos en Microsoft 365 también están disponibles como suscripciones individuales y están disponibles en dos planes, denominados Plan 1 (P1) y Plan 2 (P2), e incluyen lo siguiente:

- Azure Active Directory Premium Office 365 Protección
- avanzada contra amenazas Protección de información
- de Azure

En cada caso, el Plan 2 incluye todas las características del Plan 1, más algunas capacidades adicionales. Microsoft 365 Enterprise E5 incluye el Plan 2 para las tres características, mientras que el Plan 1 se incluye en una o más de las otras suscripciones, como se muestra más adelante en Tabla 4-1 .

---

**CUADRO 4-1** Características y beneficios en las suscripciones de Microsoft 365

CARACTERÍSTICAS INCLUIDAS	MICROS OFT 365 BUSINE SS	MICROSO FT 365 ENTERPRI SE E3	MICROSO FT 365 ENTERPRI SE E5	MICROSOFT 365 F1
Windows 10	Pro	Enterpri se	Enterpri se	Empresa
Oficina 365	Oficina 365	Office 365 Pro	Office 365 Pro	Office 365 F1 (Office para móviles)

	Pro Plus	Más	Más	aplicaciones y Office para la web)
Intercambio en línea	Sí, con 50 GB de correo	Sí, con buzón de 50 GB.	Sí, con buzón de 50 GB.	Sí, con buzón de 2 GB.
SharePoint en línea	sí	sí	sí	Sí (sin sitio personal, buzón de sitio o creación de formulario)
Equipo de Microsoft	sí	sí	sí	Sí (solo llamadas individuales, solo se unen las reuniones)
OneDrive	1 TB	5 TB (cinco o más usuarios)	5 TB (cinco o más usuarios)	2 GB (sin sincronización de escritorio)
		1 TB (menos de cinco usuarios)	1 TB (menos de cinco usuarios)	
OneDrive para hacer negocios	No	Ilimitado	Ilimitado	No
Microsoft Stream	sí	sí	sí	Sí (solo consumir)

Audio sistema de conferencia / Phone	No	No	si	No
Quejarse	si	si	si	si
Planificador	si	si	si	si
Fluir	si	si	si	Sí (solo consume, 750 ejecuciones por usuario por mes)
Influencia	si	si	si	si
Windows Hello	si	si	si	si
Azure Active Directory Premium	Plan 1	Plan 1	Plan 2	Plan 1
Administración de identidad privilegiada de Azure Active Directory	No	No	si	No
Centro de administración de Microsoft 365	si	si	si	si
Microsoft Intune	si	si	si	si

Administrador de configuración de System Center	No	si	si	si
Piloto automático de Windows	si	si	si	si
Análisis avanzado de amenazas de Microsoft	No	si	si	si
Protección avanzada contra amenazas de Microsoft Defender	No	No	si	No
Protección contra amenazas avanzadas de Office 365	Plan 1 No		Plan 2	No
Inteligencia de amenazas de Office 365	No	No	si	No
Protección contra amenazas avanzadas de Azure	No	No	si	No
Prevención de pérdida de datos de Office 365	si	si	si	No

Azur	Plan 1	Plan 1	Plan 2	Plan 1
Protección de la información				
Protección de información de Windows	sí	sí	sí	sí
Acceso privilegiado de Office 365 administración	No	No	sí	No
MyAnalytics	No	sí	sí	sí
Power BI Pro	No	No	sí	No
Seguridad de aplicaciones en la nube	No	No	sí	No
Centro de seguridad y cumplimiento de Microsoft	sí	sí	sí	sí

Para las organizaciones que se suscriben a Microsoft 365 Enterprise E3, también es posible agregar ciertas características avanzadas de E5 en dos paquetes de suscripción adicionales, de la siguiente manera:

- **Identidad y protección contra amenazas** Incluye Azure Advanced Threat Protection (ATP), Windows Defender Advanced Threat Protection,

y Office 365 Advanced Threat Protection, así como Microsoft Cloud App Security y Azure Active Directory Premium P2

- **Protección de información y cumplimiento** Incluye Office 365 Advanced Compliance y Azure Information Protection P2

## Microsoft 365 F1

Microsoft visualiza el producto Microsoft 365 como un paso crucial en la transición de una organización de la informática local tradicional a los servicios basados en la nube. Para que esa transición sea completa, consideran esencial que los trabajadores de todos los niveles del negocio participen. Microsoft 365 F1 está destinado a

*trabajadores de primera línea* —Es decir, el segmento de la fuerza laboral de una organización que proporciona el primer punto de contacto entre la organización y el mundo exterior. Esto se refiere específicamente a los trabajadores en el campo, en los centros de llamadas, en los talleres y en los roles de servicio al cliente.

La suscripción a Microsoft 365 F1 proporciona una versión simplificada de la misma funcionalidad básica que las otras suscripciones de Microsoft 365, incluidas herramientas similares de productividad, colaboración y seguridad, pero a un precio más bajo y con limitaciones adecuadas para las necesidades típicas de los trabajadores de primera línea. Los componentes de la suscripción a Microsoft 365 F1 son los siguientes:

- Windows 10 Enterprise
- Office 365 F1 (formalmente Office 365 Enterprise K1)

- Movilidad empresarial + seguridad

La principal diferencia en la suscripción F1, en comparación con las suscripciones Enterprise y Business, es que los usuarios reciben acceso a las aplicaciones de productividad de Office 365 solo en sus versiones web y móvil; Las aplicaciones instalables no están incluidas. El producto incluye acceso a los servicios basados en la nube de Office 365, incluidos Exchange Online, SharePoint Online, OneDrive, Microsoft Teams, Microsoft Intune, Stream, Yammer, Sway y Planner, pero con limitaciones que se adaptan a las tareas que normalmente realizan y los dispositivos que estos trabajadores emplean, incluidos los siguientes:

- Los buzones de Exchange Online están limitados a 2 GB. Se incluye el acceso a
- SharePoint Online, sin sitios personales, buzones de sitio o la capacidad de crear formularios.
- OneDrive está limitado a 2 GB de almacenamiento en la nube, sin sincronización de escritorio.
- Microsoft Teams se limita solo a llamadas uno a uno; los usuarios pueden unirse pero no crear reuniones.
- El flujo se limita solo al consumo; los usuarios no pueden crear o subir transmisiones de video.
- El flujo se limita solo al consumo, con un límite de 750 ejecuciones de flujo por usuario por mes.

Microsoft 365 F1 también incluye muchos de los mismos servicios de protección contra amenazas y administración de dispositivos que las suscripciones Microsoft 365 Business y Enterprise E3. El resultado final es un paquete que permite

Trabajadores de primera línea para participar plenamente en la cultura y la comunidad de la organización, con acceso a las mismas herramientas de productividad, colaboración y seguridad que los usuarios con suscripciones Microsoft 365 Enterprise o Business. Al mismo tiempo, los trabajadores de primera línea pueden adquirir habilidades y experiencia con herramientas que les permitan crecer y desarrollarse dentro de la fuerza laboral.

## **Comparación de características de Microsoft 365 Business y Enterprise**

Los componentes y características incluidos en las principales suscripciones de Microsoft 365 se muestran en **Tabla 4-1**.

**Nota:**

### **Microsoft 365**

#### **Usuarios internacionales**

**Las características exactas incluidas en las suscripciones de Microsoft 365, así como sus requisitos de precios y licencias, pueden variar según el país o la región geográfica en la que se compra la suscripción.**

## **Gobierno de Microsoft 365**

Además de las suscripciones principales de Microsoft 365 mencionadas anteriormente, Microsoft también ha creado paquetes especializados para organizaciones gubernamentales y educativas diseñadas para satisfacer sus necesidades específicas. Las suscripciones de Microsoft 365 Government G3 y G5 contienen las mismas herramientas y servicios encontrados

en sus equivalentes Enterprise E3 y E5, pero los paquetes están diseñados para cumplir con las regulaciones y requisitos de cumplimiento adicionales a los que las entidades gubernamentales de los Estados Unidos a menudo están sujetas.

Para todos los productos de Microsoft 365 Government, los datos se almacenan en condiciones especiales, que incluyen lo siguiente:

- Todo el contenido del usuario de Microsoft 365 Government, incluidos los buzones de Exchange Online, el contenido del sitio de SharePoint Online, las conversaciones de Skype for Business y las transcripciones de chat de Microsoft Teams, se almacenan en centros de datos ubicados en los Estados Unidos.
- El contenido del usuario generado por los suscriptores del gobierno de Microsoft 365 está segregado lógicamente del contenido comercial del usuario de Microsoft 365 dentro de los centros de datos de Microsoft.
- El acceso al contenido del usuario de Microsoft 365 Government dentro de los centros de datos de Microsoft está restringido a los empleados que se hayan sometido a controles de seguridad adicionales.

El acceso a los productos del gobierno de Microsoft 365 está restringido a las entidades gubernamentales federales, estatales, locales, tribales o territoriales de los Estados Unidos, así como a otras entidades que deben manejar los datos del gobierno de conformidad con las mismas regulaciones y requisitos que una entidad gubernamental. . La elegibilidad para comprar estos productos está sujeta a verificación por parte de Microsoft utilizando diversos recursos gubernamentales, incluidos los de las agencias de aplicación de la ley y el Departamento de Estado, así como los estándares gubernamentales, como el Reglamento Internacional de Tráfico de Armas (ITAR) y el FBI

Política de Servicios de Información de Justicia Criminal (CJIS).

Además de las suscripciones de Microsoft 365 Government G3 y G5, que definen los conjuntos de características de los productos, existen versiones de Microsoft 365 Government que definen varios niveles de seguridad y cumplimiento, que incluyen los siguientes:

- **Microsoft 365 Comunidad del Gobierno de EE. UU. (GCC)** Destinado a situaciones de impacto de riesgo moderado del Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP); también cumple con el estándar de Publicación 1075 del Servicio de Impuestos Internos, la Política de Seguridad de los Servicios de Información de Justicia Criminal de los Estados Unidos (CJIS) y el

Requisito de Nivel 2 de la Agencia de Sistemas de Información de Defensa (DISA) del Departamento de Defensa de los Estados Unidos (DoD) para información no clasificada no controlada.

- **Microsoft 365 Comunidad del Gobierno de EE. UU. (GCC) Alta** Destinado a situaciones de alto impacto de FedRAMP; cumple con el Reglamento Internacional de Tráfico de Armas (ITAR) y el Suplemento del Reglamento Federal de Adquisición de Defensa (DFARS).
- **Microsoft 365 DoD** Restringido al uso exclusivo de las agencias del Departamento de Defensa de los Estados Unidos; cumple con el requisito de Nivel 5 de la Agencia de Sistemas de Información de Defensa del Departamento de Defensa de los Estados Unidos (DISA) para la información no clasificada controlada y los sistemas de seguridad nacional no clasificados.

Además de las suscripciones de Microsoft 365 Government, Microsoft también mantiene un medio alternativo para acceder a los servicios en la nube de Office 365, llamado Azure Government ExpressRoute, que es una conexión de red privada y dedicada a los servicios en la nube de Microsoft para suscriptores elegibles que tienen requisitos reglamentarios que los impiden de usar el público

Internet.

## Microsoft 365 Education

Microsoft 365 Education es otra versión especializada de Microsoft 365 que incluye herramientas y servicios adicionales que están específicamente dirigidos a maestros y estudiantes. Hay dos niveles de suscripción, llamados Microsoft 365 Education A3 y Microsoft Education A5, que corresponden a las suscripciones Enterprise E3 y E5 en la mayoría de sus funciones y servicios. Las suscripciones incluyen versiones especializadas de los tres componentes principales, como sigue:

- Windows 10 Education Office
- 365 Educación Gestión y
- seguridad

Algunas de las herramientas incluidas en las suscripciones de Educación están especialmente modificadas para uso en el aula, y también se incluyen herramientas educativas adicionales.

*Nota:*

### Microsoft 365

#### Educación A1

Además de Microsoft Education A3 y A5, también hay un producto Microsoft Education A1, que es una licencia por dispositivo única que incluye Office 365 para las aplicaciones web y correo electrónico, equipos, videoconferencias y cumplimiento, y protección de la información

**herramientas; no incluye las aplicaciones instalables de Office 365 y también omite algunas de las herramientas educativas, de seguridad y analíticas que se encuentran en las suscripciones A3 y A5.**

Las modificaciones específicas de educación en las suscripciones de Microsoft 365 Education A3 y A5 incluyen lo siguiente:

- **Cuaderno de clase OneNote** Una implementación compartida de OneNote que incluye un espacio de colaboración para el trabajo en clase, una biblioteca de contenido para documentos y un espacio de cuaderno personal para cada alumno.
- **Académico Yammer** Una implementación del servicio privado de redes sociales Yammer que incluye la capacidad de marca de la escuela, capacidades de administración que proporcionan administración de contenido y control de acceso.
- **Minecraft Education Edition con Code Builder** Una adaptación educativa del juego Minecraft que permite a los estudiantes aprender a codificar software arrastrando y soltando bloques de código visual.
- **Haz una aplicación de prueba** Una aplicación que permite a los maestros implementar pruebas de alto o bajo riesgo para los estudiantes en un entorno libre de distracciones, como se muestra en Figura 4-2. Una vez que los estudiantes han comenzado a tomar una prueba, no pueden navegar por la web, imprimir o compartir la pantalla, abrir otras aplicaciones, usar el portapapeles de Windows o cambiar la configuración del sistema.

## Chapter 1 Quiz

\* Required

1. What is a variable in terms of coding? \*

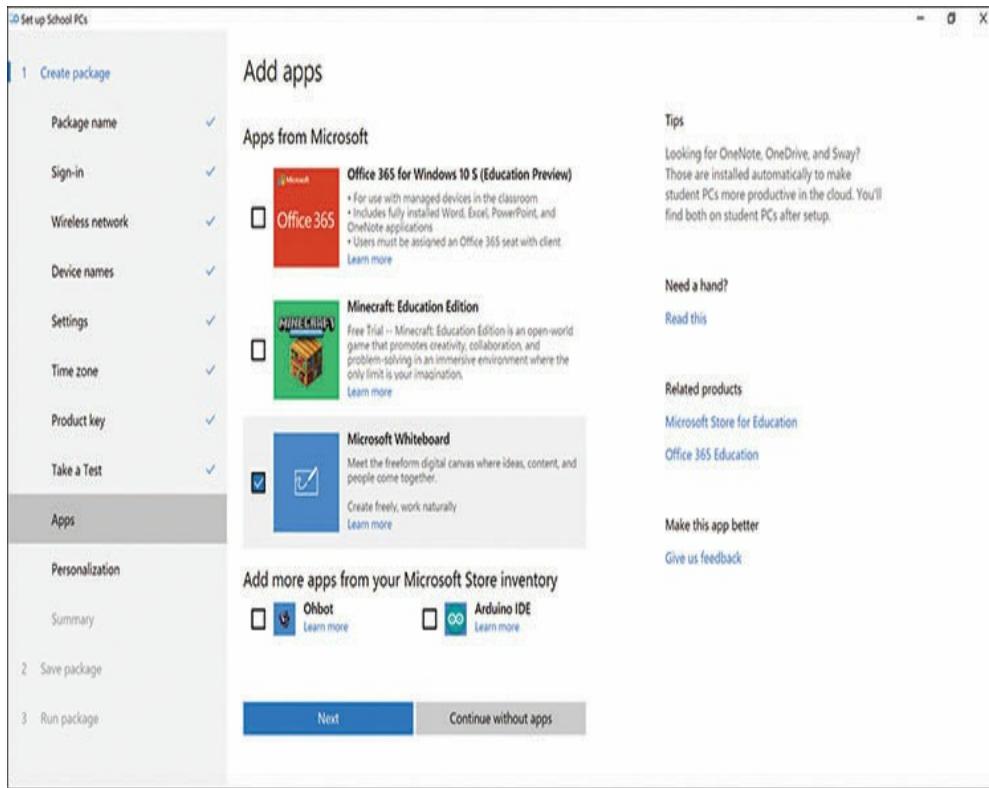
A number  
 A name that stores data  
 An unknown factor that could change  
 An alphabetic character that represents a number

2. What is myCat's value after the following code has been executed?

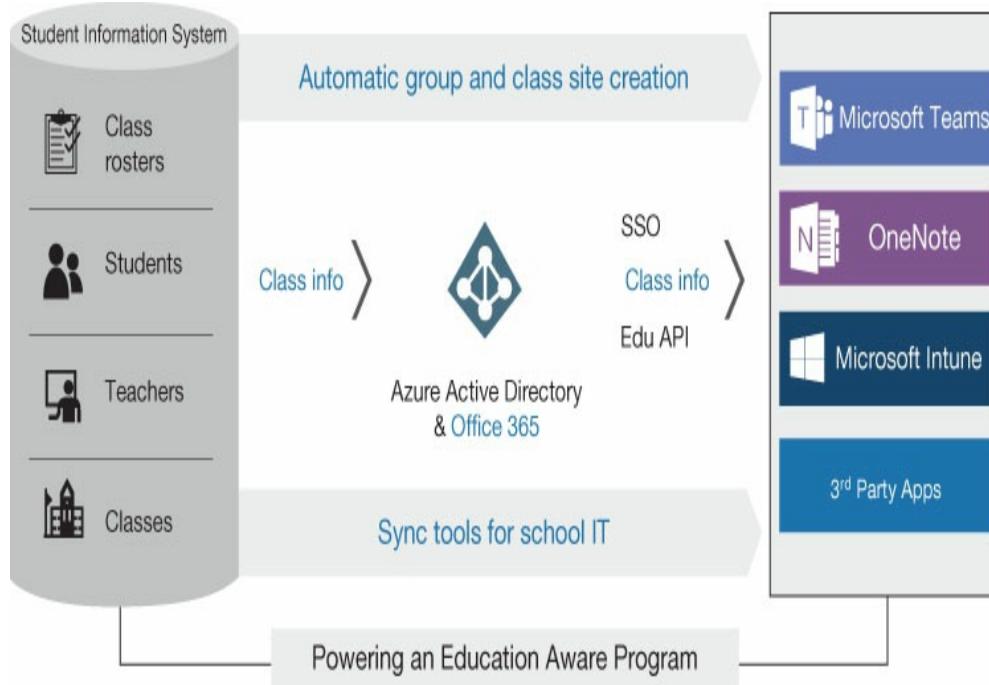
```
var myDog = 'dog'  
var myCat = 'cat'  
myDog = myCat  
myCat = myDog *
```

**FIGURA 4-2** Una pregunta de prueba en la aplicación Tomar una prueba

- **Configurar la aplicación de PC de la escuela** Una aplicación que permite a los administradores o maestros configurar fácilmente computadoras con Windows 10 al unirlas a un inquilino de Azure Active Directory e instalar aplicaciones aprobadas (como se muestra en Figura 4-3. ), eliminando aplicaciones no aprobadas, configurando Windows Update para instalar actualizaciones fuera del horario de clase y bloqueando el sistema para evitar su uso con fines que no sean educativos.
- **Sincronización de datos escolares (SDS)** Un servicio que utiliza datos sincronizados del Sistema de información estudiantil (SIS) de una escuela para crear grupos de Office 365 para Exchange Online y SharePoint Online, grupos de Microsoft Intune, equipos de clase para equipos de Microsoft y cuadernos de clase para OneNote, como se muestra en Figura 4-4. . Además, SDS puede llenar muchas otras aplicaciones de terceros con información del estudiante.

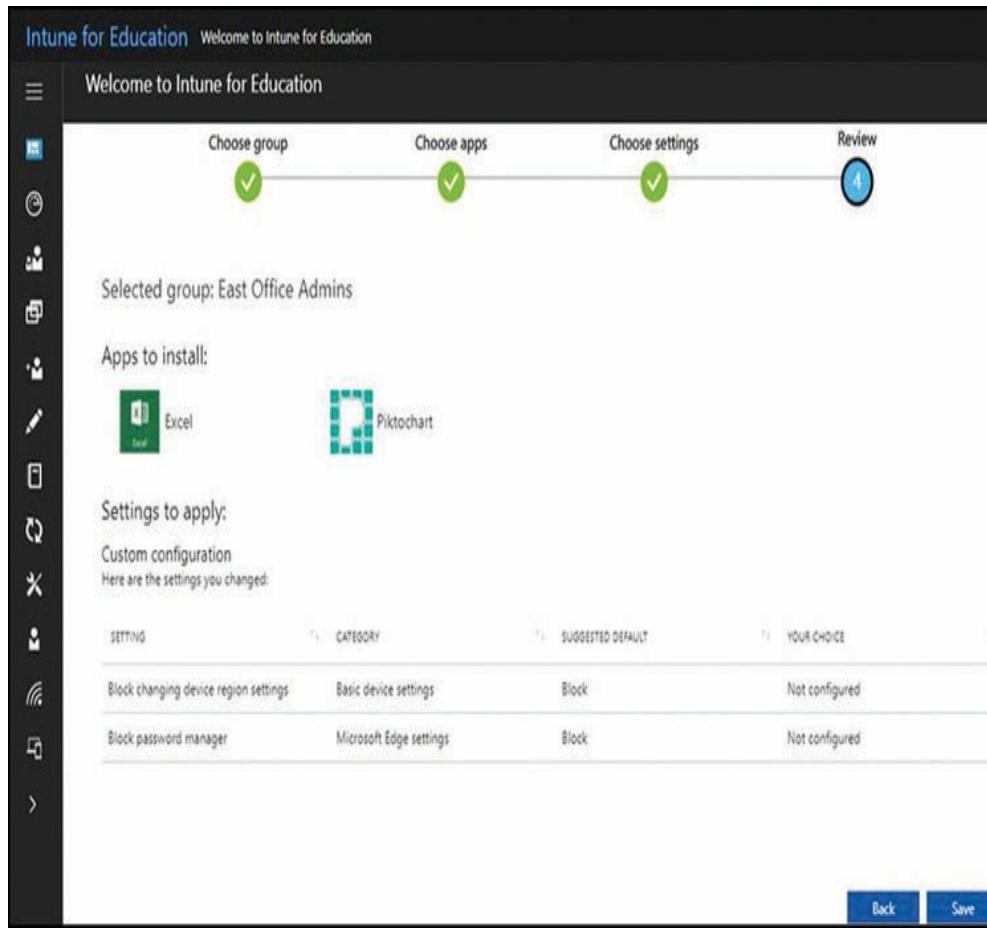


**FIGURA 4-3** Agregar aplicaciones en la aplicación Set Up School PCs



**FIGURA 4-4** Sincronización de datos del sistema de información escolar

- **Lente de la oficina** Una herramienta que utiliza la cámara de un teléfono inteligente o tableta para tomar fotos de páginas impresas o pizarras blancas. Esta herramienta los recorta, endereza y agudiza, y los convierte a archivos PDF, Word o PowerPoint y luego los guarda en un cuaderno OneNote, una carpeta OneDrive o una unidad local.
- **Intune para la educación** Una versión simplificada de Microsoft Intune que proporciona servicios de administración de dispositivos y despliegue de aplicaciones para dispositivos de maestros y estudiantes a través de un portal basado en la web, como se muestra en Figura 4-5 .



**FIGURA 4-5** Implementación de la aplicación Intune for Education

### Comprobación rápida

● ¿Cuál de las siguientes es una de las características incluidas en Microsoft 365 F1?

- 1) Instale Office 365 en hasta cinco dispositivos
- 2) 50 GB de buzones de Exchange Online
- 3) 2 GB de almacenamiento en la nube OneDrive
- 4) Sitios personales de SharePoint Online

### **Respuesta de verificación rápida**

- C. Microsoft 365 F1 no incluye las versiones instalables de las aplicaciones de Office 365, solo incluye buzones de Exchange Online de 2 GB y no incluye sitios personales de SharePoint Online.

## **Venta de Microsoft 365**

Como se señaló en otra parte de este libro, hay muchos profesionales de TI que dudan en aceptar la idea de los servicios basados en la nube, y la nube es la primera y más importante palabra de moda para el producto Microsoft 365. Como resultado, Microsoft ha dedicado una gran cantidad de tiempo, esfuerzo y gasto al desarrollo de un producto y una campaña que pueda convencer a personas como estas para que adopten, o al menos consideren, Microsoft 365 como una ruta viable para el desarrollo de su empresa. infraestructuras Las siguientes secciones analizan los puntos de venta clave para Microsoft 365 en cuatro áreas principales.

*¿Necesita más revisión ?:*

### **Puntos de venta clave de Microsoft 365**

Para obtener información adicional sobre los puntos de venta clave de Microsoft 365, consulte " La adopción de la nube muestra "Sección en Capítulo 3 , " Comprenda la seguridad, el cumplimiento, la privacidad y la confianza en Microsoft 365 . "

## **Productividad**

Pocos profesionales de TI deben venderse en las aplicaciones de productividad de Microsoft Office, como Word, Excel y PowerPoint; son estándares de la industria que prácticamente no tienen competencia. Sin embargo, hay quienes deben venderse en una implementación basada en la suscripción basada en la nube, como Office 365 ProPlus, a diferencia de las versiones locales como Office Professional Plus 2019. Los puntos de venta que hacen un caso efectivo para Office 365 incluyen el seguimiento:

- **Aplicaciones** Algunas personas podrían pensar que con Office 365, las aplicaciones de productividad son accesibles solo desde la nube y que se requiere una conexión a Internet para ejecutarlas. Si bien las aplicaciones de productividad son accesibles desde la nube con una suscripción a Office 365 ProPlus, como la que se incluye en Microsoft 365, el producto también incluye versiones completamente instalables de las aplicaciones de productividad, al igual que las de Office 2019.
- **Dispositivos** Una licencia de Office 2019 Professional Plus permite al usuario instalar las aplicaciones de productividad en una sola computadora; sin embargo, con una suscripción a Office 365 ProPlus, un usuario puede instalar las aplicaciones en hasta cinco PC, Mac o dispositivos móviles e iniciar sesión en cualquiera de ellos al mismo tiempo. Esto significa que los usuarios pueden ejecutar las aplicaciones de Office 365 en una computadora de oficina, una computadora doméstica y un teléfono inteligente, además de otros dos dispositivos, con una sola licencia, mientras que un usuario de Office 2019 necesitaría una licencia separada para cada dispositivo.
- **Instalación** Una licencia de Office 365 ProPlus incluye acceso a un portal basado en la nube, con el cual los usuarios pueden instalar las aplicaciones de productividad ellos mismos en cualquier computadora. Office 2019 y otras versiones locales no incluyen acceso al portal de autoservicio y requieren que los administradores instalen las aplicaciones en cada dispositivo.
- **Activación** Cuando los usuarios instalan las aplicaciones de productividad de Office 365 desde el portal de autoservicio, son automáticamente

activado. Permanecen activados mientras las computadoras se conectan al Servicio de licencias de Office en la nube al menos una vez cada 30 días. Si un dispositivo excede el requisito de 30 días, Office 365 entra en modo de funcionalidad reducida, lo que limita al usuario a ver e imprimir documentos existentes. Office 2019 y otras versiones locales en un entorno empresarial requieren que los administradores realicen un seguimiento de la clave del producto para cada licencia individual o utilicen un método de activación basado en la red, como el Servicio de administración de claves (KMS) o la Clave de activación múltiple (MAK). Una vez activadas, las instalaciones de Office 2019 no requieren una reactivación periódica.

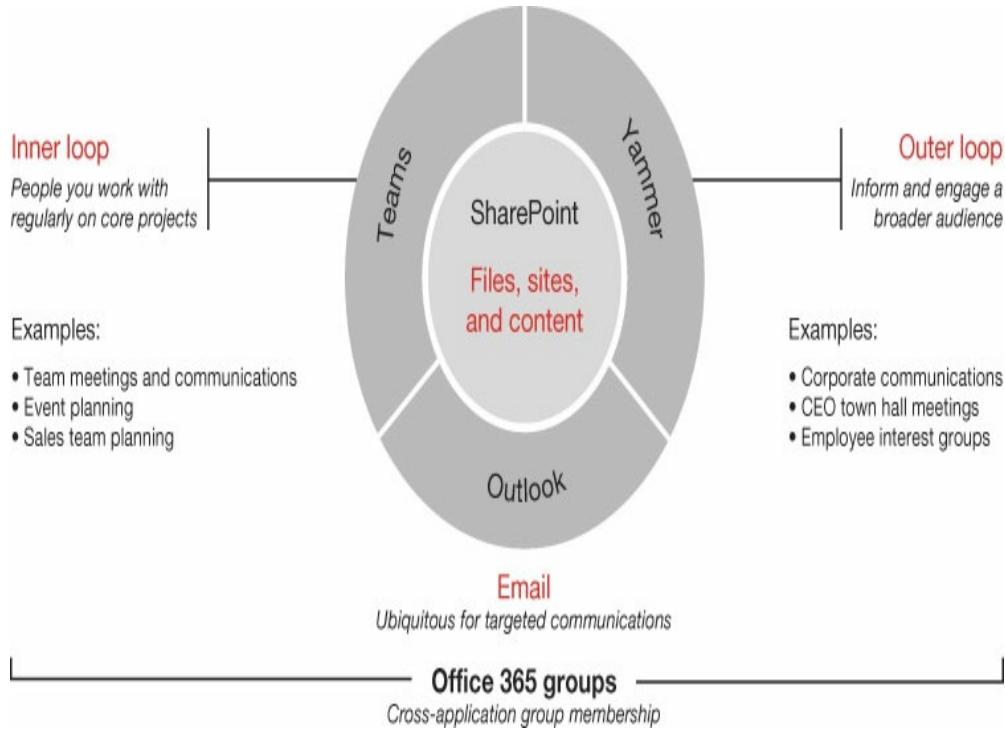
- **Actualizaciones** Las instalaciones de Office 365 se actualizan automáticamente ya sea mensual o semestralmente con las últimas actualizaciones de seguridad, calidad y características. Office 2019 y otras versiones locales reciben actualizaciones de seguridad pero no actualizaciones de características. Tampoco hay una ruta de actualización a la próxima versión local principal de Office. Por ejemplo, los usuarios de Office 2016 deben pagar el precio completo de una nueva licencia para instalar Office 2019.
- **Apoyo** Office 2019 y otras versiones locales incluyen soporte técnico gratuito solo para el proceso de instalación. Las suscripciones de Office 365 incluyen soporte técnico gratuito durante la vida de la suscripción.
- **Almacenamiento** Una suscripción a Office 365 ProPlus incluye 1 TB de almacenamiento en la nube OneDrive. Office 2019 y otras versiones locales no incluyen almacenamiento en la nube.
- **Aplicaciones móviles** El acceso a las aplicaciones móviles de Office en dispositivos con pantallas de menos de 10.1 pulgadas con funcionalidad de edición central es gratuito para todos. Los suscriptores de Office 365 reciben funciones adicionales en todas las aplicaciones móviles. Los usuarios de Office 2019 u otras versiones locales no reciben las características adicionales.

## Colaboración

La naturaleza de la colaboración en el lugar de trabajo ha cambiado, por lo que las herramientas que facilitan la colaboración deben cambiar con ella. Una de las principales ventajas de la nube

La informática basada en la nube proporciona a los usuarios la capacidad de acceder a los recursos empresariales desde cualquier ubicación. Microsoft 365 aprovecha ese beneficio al hacer posible acceder a la nube utilizando casi cualquier dispositivo con conexión a Internet. Azure Active Directory y Microsoft Intune son servicios, basados en la nube, que proporcionan funciones de identidad y administración de dispositivos que estas conexiones de usuario a la nube aseguran. Estos componentes, junto con el aumento de las capacidades y el énfasis en los teléfonos inteligentes y otros dispositivos móviles en el mundo empresarial, han hecho de Microsoft 365 una plataforma de colaboración sin precedentes.

Con una infraestructura en el lugar que puede proporcionar a los usuarios todo menos acceso universal a los recursos empresariales, el siguiente paso hacia una plataforma de colaboración son las aplicaciones y servicios que permiten a los usuarios comunicarse y compartir datos. Microsoft 365 incluye cuatro servicios de **colaboración principales**, que se muestran en Dibujo 46 —Que proporcionan diferentes tipos de comunicación para diferentes situaciones. También hay servicios adicionales que proporcionan funciones más específicas para los otros servicios.



**FIGURA 4-6** Servicios de colaboración de Microsoft 365

Los servicios que contribuyen a las capacidades de colaboración en Microsoft 365 son los siguientes:

- **SharePoint en línea** Proporciona servicios de almacenamiento y publicación de contenido para sitios web de intranet grupales y personales y para todas las demás herramientas de colaboración de Microsoft 365. Un sitio de SharePoint puede ser una plataforma de colaboración propia o sus elementos pueden integrarse en otras publicaciones de servicio.
- **Exchange Online / Outlook** Proporciona comunicación estándar por correo electrónico, así como funciones de calendario y programación. El correo electrónico es una comunicación asincrónica que puede ser uno a uno o, con la ayuda de listas de distribución, uno a muchos. Las funciones de programación pueden integrarse en otros servicios.
- **Equipos de Microsoft** Proporciona comunicación sincrónica basada en llamadas y chat entre los miembros del equipo que deben comunicarse de manera rápida y frecuente. Al incorporar elementos de otros servicios,

como la programación de Exchange Online, el contenido de SharePoint Online y la transmisión de video, Teams puede funcionar como una plataforma de colaboración integral.

- **Quejarse** Proporciona un servicio de redes sociales privadas basado en grupos o en toda la empresa que está diseñado para acomodar a grupos más grandes que los equipos o para fomentar un sentido de comunidad dentro de la empresa. Yammer también proporciona una plataforma para las funciones proporcionadas por otros servicios, como el contenido de sitios de SharePoint Online o la programación con Exchange Online.
- **Corriente** Proporciona servicios de almacenamiento y distribución de video, tanto directamente a los usuarios en navegadores web como integrados en otros servicios de colaboración de Microsoft 365, incluidos Exchange Online, SharePoint Online, Teams y Yammer.
- **Planificador** Proporciona servicios de gestión de proyectos que permiten a los usuarios crear programaciones que contienen tareas, archivos, eventos y otro contenido de los servicios de Microsoft 365.
- **OneDrive para hacer negocios** Proporciona almacenamiento de archivos para usuarios individuales que es privado a menos que el usuario explícitamente comparta documentos específicos.

*¿Necesita más revisión ?:*

## Herramientas de colaboración de Microsoft 365

Para obtener más información sobre las capacidades de colaboración de los servicios de Microsoft 365, consulte "[Comprender la colaboración y la movilidad con Microsoft 365](#)" Sección en Capítulo 2 , " [Comprender los servicios y conceptos básicos de Microsoft 365](#) . "

Azure Active Directory y Office 365 Groups proporcionan la infraestructura de administración de identidad para todos los servicios colaborativos de Microsoft 365. Esto permite a los usuarios y administradores configurar y usar estos servicios

como ellos quieran. Sin embargo, el contenido de los diversos servicios se combina, solo hay un conjunto de cuentas de usuario y membresías de grupo que se aplica a todos ellos. Esto convierte la colección de servicios de colaboración de Microsoft 365 en un kit de herramientas flexible e interoperable.

Microsoft ha ilustrado un posible escenario, que se muestra en Figura 4-7 , ilustrando cómo los trabajadores y los equipos pueden usar los servicios de colaboración de Microsoft 365 para trabajar juntos mediante la creación de un plan diario digital que contiene tareas específicas y las circunstancias en las que se pueden realizar.

During morning coffee	On your commute	Meeting at the office	Collaborating with your team	Connecting across the company
 Check e-mail Manage your calendar   Check chats + stay up to date on projects   Create or review documents	 Join personal meetings or chat with voice to text   Watch live video meetings   Connect to a meeting right from Outlook	 Personal meetings with smaller groups Notes + actions managed in Teams channels   Conference room meeting with room hardware or anonymous join	 Chat, video, screen sharing, and file co-authoring in context via Teams   Track actions with Planner, Projects or other tools   Save + share documents from the cloud	 Use Yammer for organizational updates, knowledge sharing, finding answers or providing feedback   Use communication sites + news to keep broad groups of stakeholders up to date

**FIGURA 4-7** Un ejemplo de programación de tareas de colaboración de Microsoft 365

## Seguridad

Para muchos profesionales de TI que dudan en trasladar sus operaciones a la nube, la seguridad es el mayor problema que les preocupa. La idea de almacenar datos confidenciales de la compañía en servidores de Internet, sobre los cuales no tienen control directo y de los cuales ni siquiera conocen la ubicación exacta, puede ser aterradora. Sin embargo, Microsoft ha invertido una enorme cantidad de tiempo, esfuerzo y gasto en asegurar sus centros de datos, y Microsoft 365 incluye una variedad de herramientas de seguridad que los suscriptores pueden utilizar para proporcionar una defensa en profundidad contra intrusiones externas.

Toda situación de seguridad es una cuestión de juicio. Los administradores deben evaluar los datos de la organización y decidir cuánta seguridad requiere. En casos de datos altamente confidenciales, la posibilidad de almacenarlos en la nube debería ser aterradora. En tales casos, puede ser necesario que una organización mantenga el almacenamiento local y divida la funcionalidad de la empresa entre sistemas locales y basados en la nube.

Como se señaló en otra parte de este libro, Microsoft mantiene docenas de centros de datos en todo el mundo. El hecho de que los servicios en la nube de Microsoft estén almacenando datos para miles de organizaciones significa que tienen el incentivo y el capital para construir centros de datos con equipos y seguridad física que solo las corporaciones más grandes podrían duplicar. Para la mayoría de los suscriptores potenciales de Microsoft 365, la nube

brindan mayor seguridad física, mayor disponibilidad y más tolerancia a fallas de lo que podrían proporcionarse ellos mismos.

Por lo tanto, si los centros de datos de Microsoft pueden considerarse seguros contra el robo físico y la mayoría de los desastres naturales, las preocupaciones de seguridad restantes se centrarán en la protección de identidades, dispositivos y documentos. Estas son preocupaciones que son una amenaza para cualquier red empresarial, ya sea local o en la nube. Los usuarios no autorizados pueden obtener acceso a datos confidenciales donde sea que estén almacenados, y los profesionales de TI pueden tratar de evitar que eso suceda.

La seguridad es un desafío en continuo desarrollo, con amenazas que crecen tan rápido como los medios para protegerse contra ellas. Para los administradores que desean utilizar los productos de Microsoft para mantenerse al día con las últimas amenazas en desarrollo, no hay duda de que las mejores y más recientes herramientas de seguridad que Microsoft fabrica se encuentran en plataformas basadas en la nube, como Microsoft 365. Productos locales, como como Exchange Server y Office

2019, se están quedando atrás en sus capacidades de seguridad a favor de los productos de Software como Servicio (SaaS) como Office 365, Exchange Online y SharePoint Online, todos los cuales son parte del producto Microsoft 365.

Los componentes de seguridad de Microsoft 365 incluyen lo siguiente:

- **Microsoft Intune** Proporciona servicios de administración de dispositivos y aplicaciones que permiten que los dispositivos móviles se unan a la red si cumplen con las políticas de seguridad que aseguran que estén equipados y configurados adecuadamente
- **Protección de la información de Azure** Permite a los usuarios y administradores aplicar etiquetas de clasificación a los documentos e implementar varios tipos de protección basados en las etiquetas, como restricciones de acceso y cifrado de datos.
- **Prevención de pérdida de datos** Permite el descubrimiento automatizado de documentos que contienen patrones de datos comunes, como los de las tarjetas de crédito y los números de la Seguridad Social, utilizando tipos de información confidencial preconfigurados
- **Seguridad de aplicaciones en la nube** Analiza los registros de tráfico y los scripts proxy para identificar las aplicaciones a las que acceden los usuarios y permite a los administradores analizar la seguridad de las aplicaciones y sancionar o anular la aplicación de aplicaciones individuales
- **Protección de identidad de Azure Active Directory** Evalúa las actividades de inicio de sesión de cuentas de usuarios individuales y les asigna niveles de riesgo que aumentan cuando ocurren múltiples eventos negativos
- **Protección contra amenazas avanzada de Azure** Utiliza la inteligencia de la máquina para prevenir, detectar y remediar las amenazas de seguridad exclusivas del entorno de Azure mediante el análisis del comportamiento del usuario y su comparación con los patrones de ataque conocidos.
- **Análisis avanzado de amenazas de Microsoft** Captura el tráfico de red y la información de registro y lo analiza para identificar comportamientos sospechosos relacionados con las fases conocidas de los procesos de ataque típicos.

Otro aspecto de Microsoft 365 que podría ayudar a convencer a los tradicionalistas de que una plataforma en la nube puede ser segura es el uso de análisis inteligente para identificar el comportamiento indicativo de un ataque. Herramientas como Windows Defender Threat Protection recopilan información de dispositivos, aplicaciones y servicios de Microsoft 365 y utilizan

sensores de comportamiento de punto final, análisis de seguridad en la nube e inteligencia de amenazas para prevenir, descubrir, investigar y remediar amenazas potenciales y reales.

## Conformidad

A medida que la proliferación y el valor de los datos aumentan con el tiempo, las empresas, agencias e individuos se preocupan cada vez más por la privacidad y la protección de sus datos. Para cuantificar la naturaleza de esta protección de datos, existen cientos de organismos reguladores.

- tanto privados como gubernamentales, que publican estándares para el almacenamiento y manejo de datos.

Algunos de los estándares de privacidad de datos más comunes en uso hoy en día son los siguientes:

- **Ley Federal de Modernización de la Seguridad de la Información (FISMA)**  
Especifica cómo las agencias federales de EE. UU. Deben proteger la información
- **Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA)** Regula la privacidad de la información personal de salud.
- **Ley de Derechos Educativos y Privacidad de la Familia (FERPA)**  
Regula la divulgación de los registros educativos de los estudiantes.
- **Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA)** Especifica cómo las organizaciones comerciales pueden reunir, retener y compartir información personal.
- **Gramm {{#}} 8211; Leach {{#}} 8211; Bliley Act (GLBA)**  
Especifica cómo las instituciones financieras deben proteger y compartir la información personal de sus clientes.
- **Reglamento General de Protección de Datos (GDPR)** Especifica las normas de protección de datos y privacidad para los ciudadanos de la Unión Europea.

Estas normas pueden definir elementos como los siguientes:

- Los controles que las organizaciones deben ejercer para proteger la privacidad de los datos personales.
- Las formas en que las organizaciones pueden y no pueden usar datos personales Los derechos del gobierno y otras agencias oficiales para acceder a los datos personales en poder de una organización
- El período de tiempo que una organización puede y debe retener los datos personales de las personas.
- Los derechos de las personas a acceder a sus datos personales en poder de las organizaciones y corregirlos

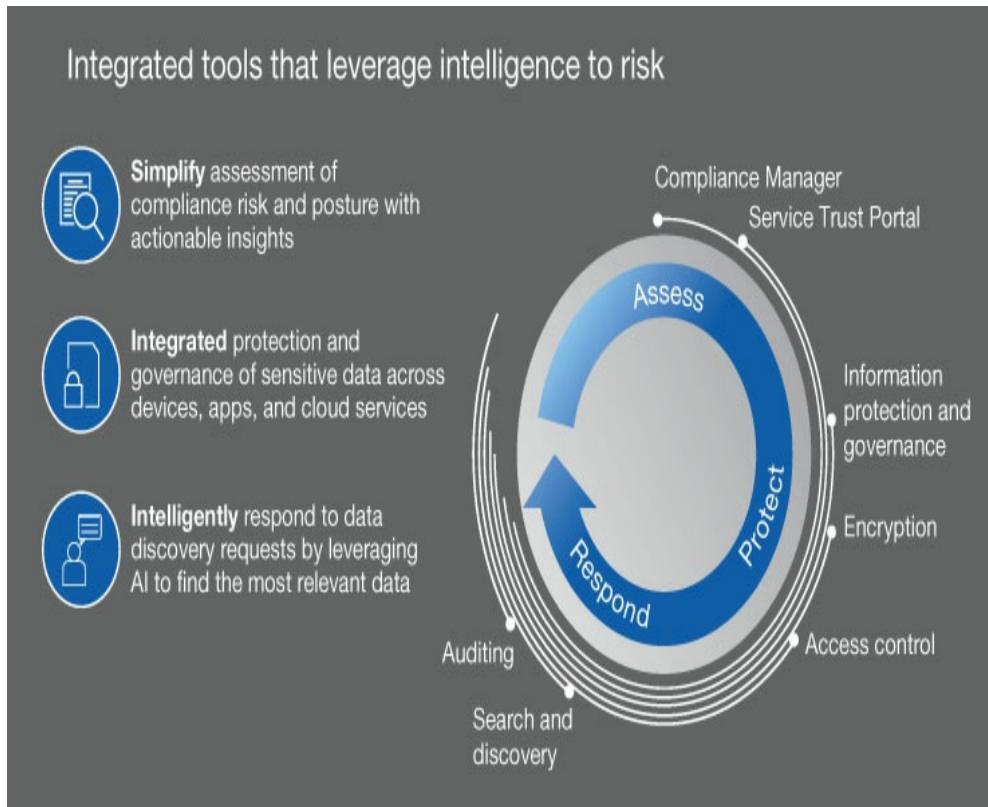
Ya sea que su adopción de ciertos estándares sea obligatoria o voluntaria, muchas organizaciones se preocupan por si las herramientas y los procedimientos que utilizan para almacenar y manejar datos cumplen con estos estándares.

Cada organización debe ser responsable de evaluar sus propios recursos de datos y determinar qué estándares deben aplicarse a ellos. La naturaleza del negocio en el que participa la organización a menudo puede dictar el cumplimiento de estándares particulares. Por ejemplo, las compañías en la industria del cuidado de la salud o aquellas con contratos gubernamentales podrían estar obligadas por ley a almacenar, manejar y proteger sus datos de maneras específicas. De hecho, hay estándares regulatorios que los productos Microsoft 365 por sí solos no pueden cumplir, como los que requieren que los datos se almacenen en dispositivos y

en ubicaciones de propiedad y control de la organización, lo que impide el uso del almacenamiento en la nube por completo.

Sin embargo, muchos de los cientos de estándares de privacidad en uso permiten la posibilidad de cumplimiento cuando los datos se almacenan en la nube, y Microsoft es muy consciente de la importancia de cumplir con estos estándares para muchas organizaciones que están considerando migrar a la nube. Para los profesionales de TI que dudan en convertirse en usuarios de Microsoft 365 porque temen que cambiar la ubicación y las condiciones de su almacenamiento de datos afecte negativamente su cumplimiento con estándares como estos, Microsoft ha probado el cumplimiento de sus productos con muchos estándares diferentes y ha publicado documentos que certifiquen los resultados.

Microsoft divide el esfuerzo de cumplimiento en tres fases, como se muestra en **Figura 4-8**. . Las fases se describen a continuación:



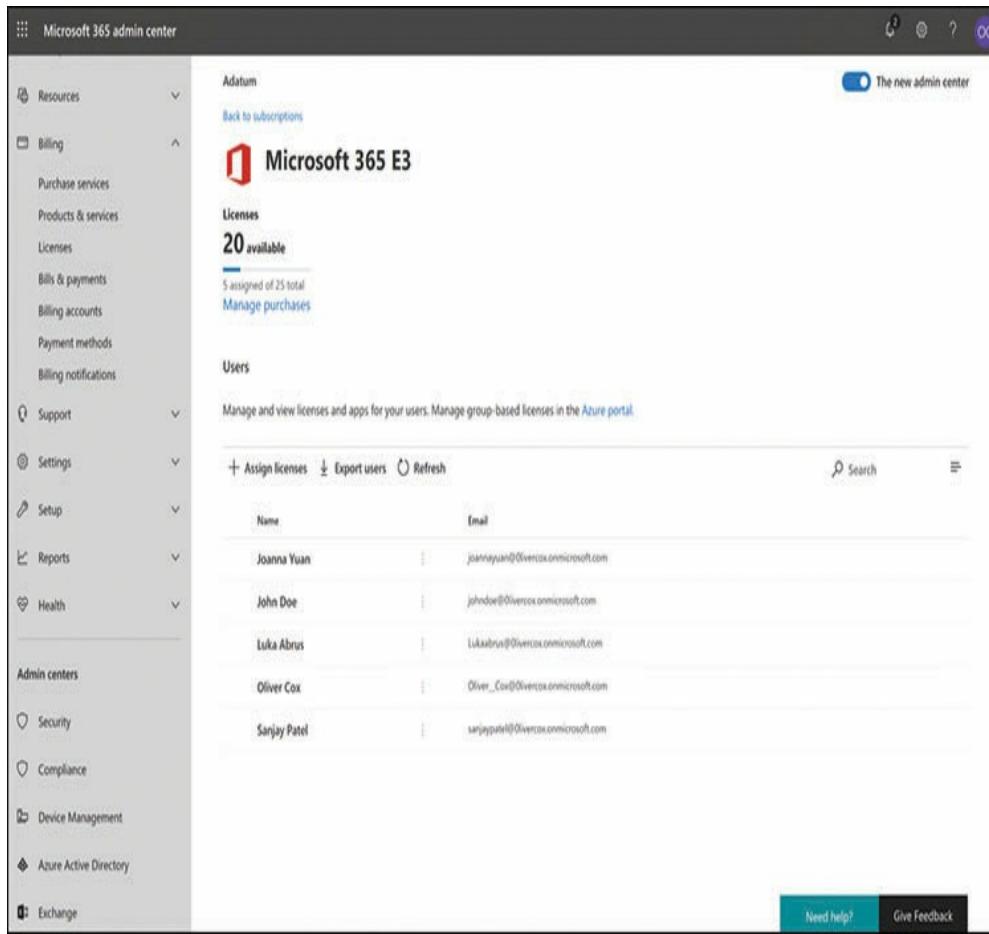
**FIGURA 4-8 Fases de cumplimiento de Microsoft**

- **Evaluar** La organización recopila la información necesaria para evaluar su estado de cumplimiento actual y producir un plan para lograr o mantener el cumplimiento de estándares específicos. El sitio web de Service Trust Portal de Microsoft contiene una amplia biblioteca de documentos que especifican información sobre los procesos de prueba y los terceros involucrados en las pruebas de cumplimiento. Además, el sitio proporciona acceso a Compliance Manager, una herramienta de evaluación de riesgos que las organizaciones pueden usar para registrar las acciones que toman para lograr el cumplimiento de estándares específicos.
- **Proteger** La organización implementa un plan de protección para sus datos, en función de su sensibilidad, utilizando las herramientas proporcionadas en los servicios de Microsoft 365, incluidos los permisos de control de acceso, cifrado de archivos, protección de la información y prevención de pérdida de datos.
- **Responder** La organización desarrolla protocolos para responder a

solicitudes regulatorias que utilizan herramientas de inteligencia artificial como Office 365 eDiscovery para realizar búsquedas complejas de buzones de Exchange Online, grupos de Office 365, sitios de SharePoint Online y OneDrive para empresas, y conversaciones de equipos de Microsoft.

## Licencias de Microsoft 365

Para instalar y ejecutar los componentes de Microsoft 365 y acceder a los servicios en la nube de Microsoft 365, cada usuario de una organización debe tener un Microsoft 365 *licencia de suscripción de usuario (USL)*. Un administrador para una organización que implementa Microsoft 365 generalmente crea una tenencia en Azure Active Directory, compra un número específico de USL y luego los asigna a los usuarios en la consola del Centro de administración de Microsoft 365 seleccionando Licencias en **Facturación** menú, como se muestra en Figura 4-9. .



**FIGURA 4-9** La página de Licencias en el Centro de administración de Microsoft

365

Los administradores globales o los administradores de administración de usuarios pueden asignar licencias a hasta 20 usuarios a la vez desde esta interfaz. También es posible asignar licencias a cuentas de usuario híbridas creadas a través de la sincronización o federación de Active Directory, o al crear nuevas cuentas de usuario en el Centro de administración de Microsoft 365.

Asignar una licencia de Microsoft 365 a un usuario hace que

siguientes eventos a ocurrir:

- Exchange Online crea un buzón para el usuario
- SharePoint Online otorga al usuario permisos de edición para el sitio de grupo predeterminado
- Office 365 ProPlus permite al usuario descargar e instalar las aplicaciones de productividad de Office 365 en hasta cinco dispositivos

Desde el **Servicios de compra** página en el Centro de administración, los administradores también pueden comprar licencias USL o licencias adicionales de Microsoft 365 para productos complementarios, como se muestra en Figura 4-10. .

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with various options like Resources, Billing, Purchase services (which is selected), Products & services, Licenses, Bills & payments, Billing accounts, Payment methods, Billing notifications, Support, Settings, Setup, Reports, Health, Admin centers, Security, Compliance, Device Management, Azure Active Directory, and Exchange.

The main content area has a header "Purchase services" and a sub-header "Select up to three products for a detailed comparison." Below this are three tabs: "Product 1" (selected), "Product 2", and "Compare products". There's also a search bar.

A section titled "Microsoft 365" is shown, with a sub-section "Microsoft 365 Business" which includes a brief description: "Microsoft 365 combines Office 365, Windows 10, and Enterprise Mobility + Security together for your organization. Today's modern workspace allows people to meet, collaborate, and stay connected across boundaries. Microsoft 365 supports teamwork, connecting services like Microsoft Teams, SharePoint, and Yammer and providing a hub for collaboration." Below this are four product cards:

- Microsoft 365 Business**: An integrated product for SMBs to access productivity tools, manage their productivity platform, and
- Microsoft 365 E3**: Starting at \$20.00 user/month
- Microsoft 365 E5**: Starting at \$32.00 user/month
- Microsoft 365 E5 without Audio Conferencing**: Starting at \$57.00 user/month

At the bottom, there's a banner that says "Office empowers your employees to get work done wherever they" followed by "Need help?" and "Give Feedback".

**FIGURA 4-10** La página de Servicios de compra en el Centro de administración de Microsoft

365

Microsoft ofrece cuatro tipos diferentes de USL para cada uno de los productos de Microsoft 365, según la relación existente del comprador con la compañía, de la siguiente manera:

- **USL completo** Una licencia completa de Microsoft 365 para nuevos compradores que no tienen licencias de productos de Microsoft existentes o para propietarios de licencias de productos de Microsoft locales que no incluyen Software Assurance, el acuerdo de mantenimiento de software de Microsoft.
- **Complemento USL** Una licencia para compradores con licencias de productos de Microsoft locales que incluyen Software Assurance y que desean mantener su infraestructura local mientras agregan servicios en la nube de Microsoft 365 en una implementación piloto o híbrida.
- **De SA USL** Una licencia para compradores con licencias existentes de productos de Microsoft en las instalaciones que incluyen Software Assurance y que desean realizar la transición a una infraestructura basada en la nube con Software Assurance continuo para el producto Microsoft 365. Los compradores que califican solo pueden obtener de USL de SA en el momento de la renovación de su contrato, y deben mantener su acuerdo existente de Software Assurance. Un acuerdo de Microsoft 365 Software Assurance incluye beneficios orientados a la nube, tales como Servicios de planificación de implementación, Programa de uso doméstico, cursos de capacitación en línea para usuarios e incidentes de soporte adicionales.
- **Step-up USL** Una licencia para los clientes actuales de Microsoft que desean actualizar sus suscripciones durante un período de inscripción o contrato existente, como de Office 365 a Microsoft 365 o de Microsoft 365 Business a Microsoft 365 Enterprise E3.

Debido a que las USL complementarias, las USL SA y las USL Stepup están destinadas a clientes existentes de Microsoft,

sus precios reflejan importantes descuentos del precio total de USL.

*Necesita más revisión:*

## **Modelos de pago de Microsoft 365**

**Para una discusión sobre las prácticas de facturación y pago de Microsoft, consulte " Planificar, predecir y comparar precios ", Más adelante en este capítulo.**

## **Implementando las mejores prácticas**

Como se menciona en este libro, el producto Microsoft 365 es un paquete que consta de Windows, Office 365 y Enterprise Mobility + Security, todos los cuales continúan disponibles como suscripciones separadas. Además, hay suscripciones disponibles para combinaciones de funciones individuales dentro de estos productos, como los paquetes de Protección de identidad y amenazas y Protección de información y cumplimiento.

Finalmente, para complicar aún más la imagen, es posible combinar diferentes licencias en una sola tenencia de Azure Active Directory. Con todas estas opciones disponibles, las organizaciones que están contemplando una migración a una infraestructura basada en la nube, o que están pensando en agregar servicios en la nube a una infraestructura local, deberían comprometerse a diseñar una estrategia de licencia que cumpla con los siguientes requisitos:

- Brinde a los usuarios de la organización los servicios que necesitan. Evite brindar a los usuarios servicios innecesarios que complican los procesos de mantenimiento y soporte.
- Minimice los costos de suscripción.
- 

En términos generales, una suscripción a Microsoft 365 probablemente será mucho menos costosa que comprar suscripciones para cada uno de sus componentes por separado. Esto podría ser cierto incluso si hay algunos usuarios que no necesitan todos los componentes de Microsoft 365.

Obviamente, la solución más simple es elegir un producto Microsoft 365 y comprar la misma suscripción para todos los usuarios de la organización. Esto puede cumplir fácilmente el primero de los requisitos, pero podría no ser una solución para los otros dos.

Dependiendo de la naturaleza del negocio en el que se dedica la organización, una suscripción Enterprise E5 puede ser adecuada para algunos usuarios, pero también puede haber muchos trabajadores que no necesitan todas las aplicaciones y servicios incluidos en Enterprise E5. Dependiendo del número de usuarios en cada grupo, el gasto de comprar suscripciones E5 para todos podría ser extremadamente derrochador y requerir un esfuerzo administrativo adicional para proporcionar entornos personalizados para los diferentes grupos de usuarios. Esta es una de las razones principales por las que Microsoft ofrece la suscripción Microsoft 365 F1 para trabajadores de primera línea.

**Nota:**

## Microsoft 365 F1

Para obtener más información sobre el paquete Microsoft 365 F1, consulte la sección "Microsoft 365 F1", anteriormente en este capítulo.

### Comprobación rápida

- ¿Cuál de las siguientes no es una de las tres fases del esfuerzo de cumplimiento de Microsoft?
  - 1) Simplificar
  - 2) Evaluar
  - 3) Proteger
  - 4) Responder

### Respuesta de verificación rápida

- R. Las tres fases del esfuerzo de cumplimiento de Microsoft son evaluar, proteger y responder. Simplificar no es una de las tres fases.

Por lo tanto, la mejor práctica es comparar las características incluidas en cada una de las licencias de Microsoft 365 con los requisitos de los distintos tipos de usuarios de la organización. En una gran empresa, esto puede ser un proceso complicado, pero en el caso de una migración importante como esta, la planificación previa es crucial y puede ahorrar una gran cantidad de gastos y esfuerzo.

## HABILIDAD 4.2: PLANIFICAR, PREDECIR Y COMPARAR PRECIOS

---

El costo siempre es un factor al considerar la introducción de una nueva tecnología en una red comercial, y la cuestión de si Microsoft 365 es una opción económicamente sólida en comparación con una infraestructura de red local tradicional es complicada. Toda organización que contemple una entrada en la informática basada en la nube debe tener en cuenta los resultados de un *análisis de costo-beneficio (CBA)* en su decisión. Sin embargo, en una comparación de Microsoft 365 con productos de servidor locales, no es solo una cuestión de cuánto cuestan las tecnologías sino también cuándo se incurre en los costos.

### Análisis de costo-beneficio para la nube versus redes locales

La evaluación del costo total de propiedad (TCO) para una implementación de Microsoft 365 es la parte relativamente simple de un análisis de costo-beneficio. Hay una tarifa mensual o anual por cada suscripción de usuario de Microsoft 365 y esas tarifas de suscriptor son predecibles y continuas. Los contratos pueden renovarse con diferentes precios a intervalos, pero esos costos siguen siendo predecibles. Es posible que los costos aumenten precipitadamente en el futuro

cuando se renuevan los contratos y el suscriptor puede sentirse encerrado en un solo proveedor, pero eso es un riesgo con cualquier producto de software.

Predecir el costo de una red local es más difícil. Es común que las empresas clasifiquen sus gastos distinguiendo entre dos tipos de gastos, de la siguiente manera:

- Los gastos de capital (CapEx) son dinero gastado en activos fijos, como edificios, servidores y otro hardware, gastos de implementación y software comprado.
- Los gastos operativos (OpEx) son gastos continuos, como alquiler, servicios públicos, personal y mantenimiento.

Las diferencias básicas entre los gastos de CapEx y OpEx se muestran en Cuadro 4-2. .

#### **CUADRO 4-2 Gastos de capital versus gastos operativos**

	<b>GASTOS DE CAPITAL (CAPEX) OPERACIONAL</b>	<b>GASTOS (OPEX)</b>
<b>PROPÓSITO</b>	Activos de hardware y software con al menos un año de utilidad	Costos comerciales continuos
<b>PAYMENT</b>	Suma global inicial	Recurrente mensual o anual
<b>CONTABILIDAD</b>	Dos o más años de depreciación de activos	Mes o año actual

<b>DESCRITO IPTIO N</b>	Propiedad, equipo, software.	Costos de operacion
<b>IMPUESTOS</b>	Múltiples años de deducción basados en depreciación	Deducción del año actual

Para una tienda de Microsoft 365, casi todos los gastos son OpEx, incluidas las tarifas de suscripción. Prácticamente no hay gastos de CapEx involucrados, excepto quizás por cosas como capacitación inicial en la nube para administradores. A las empresas les gusta trabajar con gastos OpEx porque les permiten crear presupuestos y pronósticos precisos.

Para una red local, el gasto de CapEx requerido para configurar la infraestructura puede ser enorme, incluido el costo de construir y equipar centros de datos y comprar productos de software de servidor. Dependiendo de la naturaleza del negocio y la sensibilidad de los datos involucrados, estos gastos pueden multiplicarse por la necesidad de equipos y centros de datos redundantes. Estos son grandes gastos que deben pagarse antes de que la red pueda comenzar a funcionar. Estos costos de CapEx se pueden amortizar o depreciar en las cuentas de la compañía durante un período de años, pero la inversión inicial es sustancial en comparación con la de una red basada en la nube, que casi no requiere ninguna.

Una red local también tiene gastos de OpEx, incluidos alquileres, energía y otros servicios públicos que requieren los centros de datos, y los salarios del personal necesario para operar y mantener el equipo del centro de datos. También hay actualizaciones costosas de software para considerar cada dos o tres años. El principal beneficio de costo de una red local es que el hardware y el software se compran directamente y no requieren tarifas de suscripción mensuales.

Hay otros factores a considerar también. Al diseñar una red local, la organización debe considerar la posibilidad de un crecimiento futuro, así como las fluctuaciones estacionales del negocio. Por lo tanto, el gasto de CapEx ya considerable puede incrementarse por el costo del espacio adicional del centro de datos y el equipo necesario para soportar las épocas más ocupadas del año, así como por varios años de crecimiento previsto.

Una infraestructura basada en la nube como la de Microsoft 365 utiliza un modelo de pago por uso, que puede acomodar un crecimiento virtualmente ilimitado y fluctuaciones comerciales ocasionales sin gastos adicionales que no sean las tarifas de suscripción aumentadas para los servicios adicionales. La organización nunca está pagando por hardware y software que no se está utilizando. Además, el crecimiento y las fluctuaciones pueden acomodarse casi de inmediato y reducirse cuando sea necesario, mientras que los recursos locales pueden requerir meses para aprobar, obtener e instalar.

Todo el análisis de costo-beneficio puede complicarse aún más si la organización ya ha realizado una inversión sustancial en infraestructura local. Por ejemplo, si la compañía que se está expandiendo ya tiene suficiente espacio en sus centros de datos y suficiente personal de TI, el CapEx necesario para una expansión de red puede ser mucho menor de lo que sería para una instalación de red completamente nueva. La pregunta entonces es si es más económico agregar a la infraestructura local existente o expandirse a la nube, creando una red híbrida que podría requerir planificación y capacitación adicionales para poner al personal al día en las tecnologías de la nube.

Por lo tanto, el resultado final solo puede ser que cada organización debe considerar sus propias situaciones económicas, de personal y comerciales y calcular el TCO de sus opciones de red por sí misma. En una nueva implementación, una opción basada en la suscripción, basada en la nube, como Microsoft 365, puede ser más rápida y menos costosa de implementar, pero hay muchas situaciones en las que las organizaciones podrían verse obligadas a considerar una red local.



---

#### ***Consejo de examen***

Candidatos para el examen MS-900 que buscan una mayor familiaridad con

las características de los servicios basados en la nube frente a los servicios locales también deben consultar el " **Compare los servicios principales en Microsoft 365 con los servicios locales correspondientes** "Sección en

## **Capítulo 2 .**

---

### **Licencias por volumen**

Es posible que las organizaciones compren suscripciones de Microsoft 365 directamente de Microsoft individualmente o mediante una variedad de acuerdos de licencia por volumen, que incluyen los siguientes:

- **Acuerdo de empresa (EA)** Un acuerdo de licencia por volumen para organizaciones con al menos 500 usuarios o dispositivos que buscan licenciar software por un período de al menos tres años, que ofrece descuentos del 15 al 45 por ciento en función del número de usuarios. Disponible con condiciones de pago por adelantado o por suscripción, el acuerdo incluye Software Assurance y la capacidad de agregar usuarios y servicios durante la vigencia del acuerdo.
- **Acuerdo de productos y servicios de Microsoft (MPSA)** Un acuerdo de licencia transaccional continuo y basado en socios para organizaciones con 250 a 499 usuarios o dispositivos que opcionalmente incluye Software Assurance y no requiere ningún compromiso de toda la organización.
- **Proveedor de soluciones en la nube (CSP)** Un canal de licencias basado en socios que permite a las organizaciones de todos los tamaños obtener productos de Microsoft 365 a través de una relación continua con un socio seleccionado.

### **Seguro de software**

Para Enterprise Agreement y, opcionalmente, para clientes de Microsoft Products and Services Agreement, Software Assurance ofrece una variedad de servicios adicionales, que incluyen los siguientes, que pueden beneficiar a Microsoft 365

licenciatarios:

- **Servicios de planificación** Proporciona una cantidad de días de servicio para socios, en función de la cantidad de usuarios / dispositivos con licencia, con el fin de implementar sistemas operativos, aplicaciones y servicios de Microsoft.
- **Paquete de optimización de escritorio de Microsoft (MDOP)** Proporciona un conjunto de utilidades de virtualización, administración y restauración, que incluyen Microsoft Application Virtualization (App-V), Microsoft User Experience Virtualization (UE-V), Microsoft BitLocker Administration and Monitoring (MBAM) y Microsoft Diagnostics and Recovery Toolset (DaRT)
- .
- **Derechos de acceso al escritorio virtual de Windows (VDA)** Proporciona a los usuarios los derechos necesarios para acceder a instancias de Windows virtualizadas.
- **Derechos de uso de Windows to Go** Permite a los administradores crear y proporcionar a los usuarios dispositivos de almacenamiento USB que contienen imágenes de arranque de Windows que incluyen aplicaciones de línea de negocio y datos corporativos.
- **Windows Thin PC** Permite a los administradores reutilizar computadoras antiguas como terminales de la Interfaz de escritorio virtual (VDI) de Windows.
- **Programa de licencias de fuente empresarial** Proporciona a las organizaciones con al menos 10,000 usuarios o dispositivos acceso al código fuente de Windows para sus propios proyectos de desarrollo de software.
- **Cupones de entrenamiento** Proporciona una cantidad de días de capacitación basados en la cantidad de usuarios / dispositivos con licencia para la capacitación técnica de profesionales de TI y desarrolladores de software.
- **Soporte de resolución de problemas 24x7** Proporciona asistencia telefónica las 24 horas del día, los 7 días de la semana para problemas críticos de negocios y horarios comerciales o asistencia por correo electrónico para problemas no críticos El número de incidentes permitidos se basa en el tipo de acuerdo de licencia por volumen y los productos con licencia.
- **Disponibilidad de licencia progresiva** Proporciona a los licenciatarios la capacidad de migrar sus productos de software con licencia a una edición de alto nivel.
- **Pagos separados** Permite a las organizaciones pagar por tres años

acuerdos de licencia en tres pagos anuales iguales.

**Nota:**

## Software adicional

### Beneficios de aseguramiento

Se incluyen beneficios adicionales de Software Assurance que están destinados a los titulares de licencias de software de servidor local, como los Derechos de nueva versión, que proporciona las últimas versiones del software con licencia publicado durante la vigencia del acuerdo, y los Derechos de recuperación ante desastres del servidor y los Derechos de recuperación ante fallos, que otorgan a los licenciatarios el derecho a mantener servidores redundantes pasivos para fines de tolerancia a fallas.

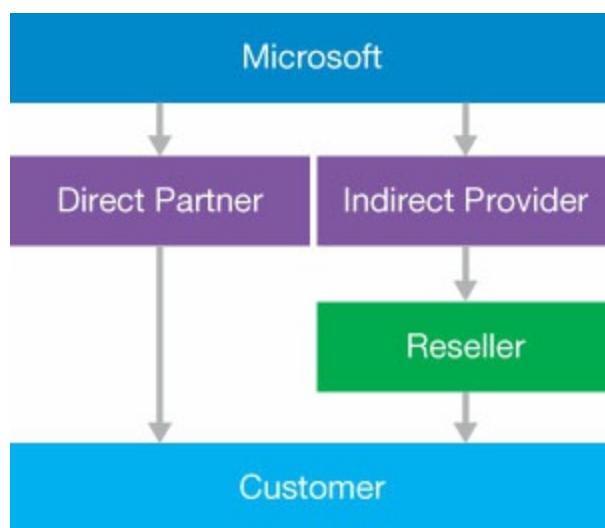
### Proveedores de soluciones en la nube

los *Proveedor de soluciones en la nube (CSP)* El programa permite a los socios establecer relaciones continuas con organizaciones de usuarios finales de todos los tamaños y proporcionarles ventas y soporte para Windows 10 y todos los productos Microsoft 365 Enterprise, Business y Education. Los miembros de Microsoft Partner Network pueden convertirse en CSP y desempeñar un papel más destacado en las soluciones en la nube de sus clientes.

En lugar de simplemente revender productos, como Windows 10 y Microsoft 365, un CSP puede ser el contacto único de un cliente para todo, desde proporcionar soluciones, hasta facturar y proporcionar soporte técnico. Los socios de CSP pueden mejorar sus relaciones con sus clientes agregando valor a los productos de Microsoft,

por ejemplo, combinando productos de software específicos de la industria con Microsoft 365 u ofreciendo servicios administrados, como migraciones de datos y soporte interno de la mesa de ayuda. Los socios de CSP también pueden ofrecer productos de Microsoft que antes no estaban disponibles para compañías más pequeñas. Por ejemplo, en un momento, Windows 10 Enterprise estaba disponible solo para clientes con un Acuerdo de Licenciamiento por Volumen de Microsoft; Los socios de CSP ahora pueden ofrecer la edición Enterprise del sistema operativo a las pequeñas y medianas empresas.

Dependiendo de las capacidades del socio de Microsoft, el programa CSP funciona de dos maneras: directa (Nivel 1) e indirecta (Nivel 2), como se muestra en **Figura 4-11**.



**FIGURA 4-11** Las opciones de socios de Microsoft Cloud Solution Provider

El modelo directo de CSP permite a los socios trabajar

directamente con Microsoft y funcionan como el único punto de contacto de sus clientes. El socio directo de CSP es el único conducto entre los productos y servicios de Microsoft y el cliente. Para que un socio participe en el modelo directo de CSP, la compañía del socio debe tener infraestructuras de facturación y soporte técnico existentes. Toda la relación del cliente es con el socio; no tienen contacto directo con Microsoft en absoluto. La relación del socio CSP con Microsoft y con sus clientes procede de la siguiente manera:

**1) El socio CSP cultiva clientes, los vende en Microsoft 365**

y / u otros productos de suscripción basados en la nube de Microsoft, y les establece un precio basado tanto en el costo de las suscripciones como en el valor agregado que proporciona el socio CSP.

**2) El socio CSP configura la tenencia del cliente en Azure Active**

Directorio y les proporciona el software necesario, como Windows 10 y cualquier otro producto que puedan incluir en el paquete negociado del cliente.

**3) El cliente utiliza los productos de Microsoft suministrados y contacta al**

CSP socio para cualquier problema de soporte que puedan tener.

**4) Cada mes, Microsoft usa el portal del Centro de socios para facturar al CSP**

socio para todas las suscripciones de usuarios que han vendido a sus clientes.

**5) El socio CSP factura a los clientes a su tarifa negociada para el**

Suscripciones de Microsoft, soporte técnico y otros servicios.

La ventaja de este modelo es que la relación con los clientes está totalmente en manos de los socios de CSP. Son responsables de construir y mantener relaciones con sus clientes, y

pueden establecer los precios que consideren apropiados para sus servicios.

Sin embargo, esta responsabilidad también significa que un socio CSP debe tener una infraestructura de la compañía que pueda satisfacer todas las necesidades de los clientes sin la ayuda de Microsoft.

Para los socios que no tienen la infraestructura para manejar todos los problemas de facturación y soporte que sus clientes puedan necesitar, existe el modelo indirecto CSP, que define dos niveles de socios, de la siguiente manera:

- **Proveedor indirecto** Típicamente, esta es una compañía más grande contratada por revendedores indirectos para asumir la responsabilidad de suministrar productos, servicio al cliente, facturación y servicios de soporte técnico a los clientes. Algunos proveedores indirectos también están dispuestos a proporcionar a los revendedores indirectos otro tipo de asistencia, como capacitación técnica y comercialización; algunos también brindan términos de financiamiento y crédito.
- **Revendedor indirecto** Por lo general, se trata de empresas o individuos más pequeños que se concentran en localizar, cultivar y firmar clientes para Windows 10, Microsoft 365 y otros productos y servicios basados en la nube. Para convertirse en un revendedor indirecto, una persona o empresa debe hacer lo siguiente:
  - Únase a la red de socios de Microsoft (MPN) y obtenga una inscripción ID en el programa CSP como revendedor indirecto al proporcionar una identificación MPN, dirección comercial, información bancaria y una dirección de correo electrónico de contacto
  - Establecer una relación con un proveedor indirecto, para obtener productos, facturación y servicios de soporte.

El modelo de socio indirecto CSP permite a los consultores individuales o pequeñas empresas de consultoría registrarse como revendedores indirectos y concentrarse en localizar clientes

y desarrollar relaciones con ellos, en lugar de concentrarse en servicios de fondo, como facturación y soporte.

#### **Comprobación rápida**

- ¿Cuál es la diferencia entre un proveedor de soluciones en la nube que es un revendedor indirecto y uno que es un proveedor indirecto?

#### **Respuesta de verificación rápida**

- Por lo general, un revendedor indirecto es una compañía más pequeña que se concentra en localizar, cultivar y firmar clientes para productos y servicios basados en la nube de Microsoft. Un proveedor indirecto es una compañía más grande contratada por revendedores indirectos para asumir la responsabilidad de suministrar productos, servicio al cliente, facturación y servicios de soporte técnico a los clientes.

## **Facturación y gestión de facturas**

Los productos basados en suscripciones como Microsoft 365 requieren atención regular a la facturación para mantenerse actualizados. Si se permite que las suscripciones caduquen, quedarán inutilizables. Por ejemplo, si una suscripción de Office 365 puede caducar, o si la computadora no se conecta a la nube al menos cada 30 días, se desactiva y entra en modo de funcionalidad reducida. En este modo, los usuarios pueden ver o imprimir sus documentos existentes, pero no pueden crear o editar documentos nuevos.

**los Facturación** El menú en el Centro de administración de Microsoft 365 es donde los administradores pueden administrar todos los aspectos del proceso de facturación. El menú contiene los siguientes elementos:

- **Servicios de compra** Contiene mosaicos con productos de suscripción basados en la nube que los administradores pueden agregar a sus inquilinos
- **productos y servicios** Enumera las suscripciones que están activas actualmente y especifica cuántas licencias se han asignado y el saldo adeudado, como se muestra en Figura 4-12.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar is open, revealing various administrative sections: Home, Users, Devices, Groups, Resources, Billing (which is highlighted with a red box), Purchase services, Products & services, Bills, Payment methods, Licenses, and Billing notifications. The main content area is titled "Products & services" and specifically shows the "Subscriptions" tab. It displays a single subscription entry for "Microsoft 365 Business" under the "Contoso Wines" tenant. The subscription details include a price of "\$240.00 user/year • Commercial direct". Below this, the "Licenses" section shows "3 available of 4 (1 used)". To the right, the "Billing" section shows a total amount of "\$960.00 (excluding tax)" and indicates it is "Billed annually". Other options in this section include "Edit", "View", and "Edit". The "Settings & Actions" section includes links for "Cancel subscription", "Edit service usage address", and "Install". At the bottom of the main content area, there is a link to "View last bill".

**FIGURA 4-12** La página de Productos y servicios en el Centro de administración de Microsoft 365

- **Licencias** Contiene una lista de las suscripciones que actualmente tiene el inquilino.

posee y especifica cuántas licencias se asignan. Al seleccionar una suscripción, se muestra una lista de los usuarios a los que se han asignado las licencias y permite a los administradores crear nuevas asignaciones.

- **Facturas y pagos** Muestra un historial de las facturas de las suscripciones actuales, los métodos de pago configurados por el administrador y la frecuencia de pago (mensual o anual).
- **Cuentas de facturación** Muestra el perfil de la cuenta de la entidad jurídica en la organización del suscriptor responsable de firmar acuerdos de software y realizar compras, así como una lista de las asociaciones del suscriptor.
- **Métodos de pago** Muestra una lista de los métodos de pago actuales del suscriptor y permite agregar otros nuevos.
- **Notificaciones de facturación** Muestra una lista de los usuarios que recibirán notificaciones de facturación y recordatorios de renovación de Microsoft, como se muestra en Figura 4-13. .

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a 'Billing' section with 'Billing notifications' selected. The main content area is titled 'Billing notifications'. It contains a section for 'Receive billing statement as email attachment?' with a toggle switch set to 'On'. Below this is a 'Notification recipients' section with the sub-instruction 'We are sending billing notifications and renewal reminders to these admins. Select user to update preferences.' A table lists two users: John Doe (Primary email address: johndoe@olivercox.onmicrosoft.com, Role: Global administrator) and Oliver Cox (Primary email address: Oliver\_Cox@olivercox.onmicrosoft.com or ol\*\*\*\*\*@outlook.com, Role: Global administrator). At the bottom are 'Need help?' and 'Give Feedback' buttons.

**FIGURA 4-13** La página de notificaciones de facturación en el Centro de administración de Microsoft 365

Para los socios de Microsoft, hay un **Facturación** menú en el **Centro de socios** consola que muestra las facturas de Microsoft para los productos que los socios han revendido a los clientes. Microsoft factura a los socios las tarifas de licencia y uso de sus clientes con 60 días de atraso, para que los socios tengan tiempo de cobrar. Esta

**Facturación** menu solo maneja los cargos que los socios remiten a Microsoft. No hay condiciones ni requisitos en el acuerdo de asociación sobre cómo o cuándo los socios facturan a sus clientes y cobran sus pagos.

## **HABILIDAD 4.3: DESCRIBA OFERTAS DE APOYO PARA LOS SERVICIOS DE MICROSOFT 365**

---

Para muchos profesionales de TI, existen importantes preocupaciones sobre lo que sucede después de que su organización se compromete a utilizar aplicaciones y servicios basados en la nube. Estos problemas incluyen preocupaciones sobre el tiempo de inactividad, el monitoreo de la continuidad de los servicios de Microsoft y el soporte de productos proporcionado por Microsoft y sus socios.

### **Acuerdos de Nivel de Servicio**

Cuando una empresa usa servidores locales, ellos

Conocer los problemas que experimentan que impiden que los servidores funcionen es su problema, y deben tener los recursos para resolverlos. Esta es la razón por la cual las organizaciones a menudo usan componentes redundantes, servidores o incluso centros de datos para mantener disponibles los servicios críticos del negocio. Muchos profesionales de TI prefieren esta autosuficiencia; Al planificar e implementar sus servicios correctamente, pueden confiar en su funcionalidad continua. Sin embargo, una empresa que utiliza servicios basados en la nube debe confiar en otros para mantener sus servicios en funcionamiento.

Para los profesionales de TI, las interrupciones del servicio son uno de los posibles problemas importantes para la adopción de Microsoft 365 y otros servicios basados en la nube. Si los servicios sufren tiempos de inactividad, el negocio se detiene. Si bien puede que no sea culpa de los profesionales de TI, es su responsabilidad. Lo que es peor, no hay nada que puedan hacer al respecto, excepto llamar al proveedor y gritarles. Dependiendo de la naturaleza del negocio de la organización, el tiempo de inactividad del servicio puede resultar en pérdida de productividad, pérdida de ingresos y, en casos extremos, incluso vidas perdidas.

Para abordar este problema, los contratos con proveedores de servicios en la nube generalmente incluyen un *acuerdo de nivel de servicio (SLA)*. El SLA garantiza un cierto porcentaje de tiempo de actividad para los servicios y especifica las consecuencias si esa garantía no se cumple. Es importante recordar que una organización generalmente tiene más de un proveedor de servicios que se necesita para acceder a la nube. Por ejemplo,

una organización puede contratar con Microsoft un cierto número de suscripciones de Microsoft 365, pero la confiabilidad especificada en el SLA de Microsoft no significa nada si el proveedor de servicios de Internet (ISP) de la organización no les proporciona acceso a la nube. Por lo tanto, una organización debe tener un contrato con cada proveedor de servicios en la nube que use que incluya la terminología de SLA.

Al negociar un SLA con cualquier proveedor de servicios en la nube o proveedor de servicios de Internet, debe incluirse un lenguaje para abordar preguntas como las siguientes:

- ¿Qué fórmula se utiliza para calcular los niveles de servicio que realmente se alcanzan?
- ¿Quién es responsable de mantener registros de los niveles de servicio? ¿Cómo y cuándo se proporciona al suscriptor informes escritos de los niveles de servicio alcanzados?
- ¿Se especifican las circunstancias excepcionales en el SLA bajo las cuales las interrupciones del servicio no se clasifican como tiempo de inactividad?
- ¿Cuánto tiempo de inactividad se espera o se permite para el mantenimiento del proveedor, tanto programado como de emergencia?
- ¿Cuáles son los términos del acuerdo con respecto a las interrupciones del servicio que son el resultado de actos de guerra, clima extremo o desastres naturales?
- ¿Cuáles son los términos del acuerdo con respecto a las interrupciones del servicio causadas por servicios de terceros, como cortes de energía? ¿Cuáles son los términos del acuerdo con respecto a las interrupciones del servicio que son el resultado de ataques cibernéticos maliciosos contra el proveedor? ¿Cuáles son los términos del acuerdo con respecto a las interrupciones del servicio?
-

- que son el resultado de ataques cibernéticos maliciosos contra el suscriptor? ¿Qué remedio o penalización proporciona el proveedor cuando no cumple con los niveles de servicio acordados?
- ¿Cuál es la responsabilidad a la que está sujeto el proveedor cuando las interrupciones del servicio causan una pérdida de negocio o productividad?

Estas preguntas están diseñadas para cuantificar la naturaleza del SLA y cómo puede afectar legalmente la relación entre el proveedor y el suscriptor. Por ejemplo, un proveedor puede garantizar una tasa de tiempo de actividad del 99 por ciento. Sin embargo, sin un lenguaje específico que aborde el punto, no hay forma de determinar exactamente qué constituye el tiempo de actividad o el tiempo de inactividad. ¿Qué sucede si un servicio es solo parcialmente operativo, con algunas tareas funcionales y otras no? ¿Eso constituye tiempo de inactividad? También está la cuestión de qué sucede cuando se produce un tiempo de inactividad superior al monto garantizado. ¿Es responsabilidad del suscriptor hacer un reclamo? Si se produce un tiempo de inactividad excesivo, ¿Es el proveedor responsable del negocio perdido del suscriptor durante ese tiempo de inactividad o solo por un monto prorrateado de la tarifa de suscripción? Si temas como estos no se discuten con un lenguaje específico en el SLA, entonces son posibles argumentos que el proveedor puede usar para evitar respaldar su garantía de tiempo de actividad.

## Limitaciones de SLA

Como un ejemplo de los términos que pueden aparecer en un

SLA para limitar la responsabilidad del proveedor de servicios en la nube, considere el siguiente extracto del SLA de Microsoft para Azure Active Directory: este SLA y los niveles de servicio aplicables no se aplican a ningún problema de rendimiento o disponibilidad:

- 1) Debido a factores fuera de nuestro control razonable (por ejemplo, desastres naturales, guerras, actos de terrorismo, disturbios, acciones gubernamentales o fallas de una red o dispositivo externo a nuestros centros de datos, incluso en su sitio o entre su sitio y nuestro centro de datos);**
- 2) El resultado del uso de servicios, hardware o software no proporcionados por nosotros, incluidos, entre otros, problemas derivados de un ancho de banda inadecuado o relacionados con software o servicios de terceros;**
- 3) Eso resulta de fallas en un solo Microsoft Datacenter ubicación, cuando la conectividad de su red depende explícitamente de esa ubicación de una manera no geo-resistente;**
- 4) Causado por su uso de un Servicio después de que le aconsejamos que modifique su uso del Servicio, si no modificó su uso según lo recomendado;**
- 5) Durante o con respecto a la vista previa, prelanzamiento, beta o prueba versiones de un Servicio, función o software (según lo determinemos nosotros) o para compras realizadas con créditos de suscripción de Microsoft;**
- 6) El resultado de su acción no autorizada o falta de acción.**  
cuando sea necesario, o de sus empleados, agentes, contratistas o proveedores, o cualquier persona que obtenga acceso a nuestra red mediante sus contraseñas o equipos, o que resulte de su incumplimiento de las prácticas de seguridad adecuadas;
- 7) El resultado de su incumplimiento de cualquier requisito**  
configuraciones, usar plataformas compatibles, seguir cualquier política para un uso aceptable o su uso del Servicio de una manera inconsistente con las características y funcionalidades del Servicio (por ejemplo, intentos de realizar operaciones que no son

*compatible) o inconsistente con nuestra guía publicada;*

**8) El resultado de una entrada, instrucciones o argumentos defectuosos (para ejemplo, solicitudes para acceder a archivos que no existen);**

**9) El resultado de sus intentos de realizar operaciones que exceder las cuotas prescritas o que resultaron de nuestra limitación del comportamiento sospechoso de abuso;**

**10) Debido a su uso de las características del Servicio que están fuera de las asociadas Soporte de Windows; o**

**11) Para licencias reservadas, pero no pagadas, en el momento del Incidente.**

Estas limitaciones no son estándar para todos los SLA, pero son típicas.

Como con cualquier contrato, un SLA es un contrato, y el lenguaje debe ser negociable; ambas partes deben aceptar todos los términos finales. Si un proveedor se niega a negociar los términos del SLA o modificar cualquiera de sus idiomas, esto debería activar las alarmas para el posible suscriptor. Las alternativas en este caso son encontrar un proveedor de servicios diferente o comprar un seguro para cubrir a la organización por cualquier pérdida en la que puedan ocurrir como resultado de interrupciones del servicio que no están cubiertas por el SLA.

En el *Acuerdo de nivel de servicio de licencias por volumen de Microsoft para servicios en línea de Microsoft* documento, fechado el 1 de agosto de 2019, los términos para cada uno de los servicios en la nube individuales se enumeran con la siguiente información:

- **Falta del tiempo** Especifica exactamente qué tipo o tipos de interrupción del servicio constituyen legalmente el tiempo de inactividad en los términos del acuerdo. Algunos de

las definiciones de tiempo de inactividad para servicios en la nube incluidos en Microsoft 365 se muestran en [Tabla 4-3](#).

- **Porcentaje de tiempo de actividad mensual** Especifica la fórmula mediante la cual se calcula el porcentaje de tiempo de actividad para cada mes, teniendo en cuenta la cantidad de minutos que el servicio se consideró inactivo y la cantidad de licencias de usuario afectadas por la interrupción. Por ejemplo, la siguiente fórmula resta el número total de minutos de inactividad para todos los usuarios del total de minutos de usuario y calcula un porcentaje a partir de eso:

$$\frac{\text{User Minutes} - \text{Downtime Minutes}}{\text{User Minutes}} \times 100$$

- **Servicio de crédito** Especifica el porcentaje de la tarifa de suscripción mensual que se acreditará a la cuenta del suscriptor, en función del porcentaje de tiempo de actividad mensual calculado. Las garantías de SLA de Microsoft 99,9 por ciento de tiempo de actividad, por lo que el crédito de servicio para los meses que no cumplen con ese porcentaje se calcula como se muestra en [Tabla 4-4](#).
- **Terminos adicionales** Identifica otras partes del documento que podrían definir otras condiciones que constituyen una interrupción del servicio reembolsable. Por ejemplo, una falla de Exchange Online para detectar virus o filtrar correo no deseado según lo acordado en el SLA puede calificar para un crédito de servicio, incluso si no se produce un tiempo de inactividad.

#### CUADRO 4-3 Definiciones de tiempo de inactividad en el Acuerdo de nivel de servicio de licencias por volumen de Microsoft para servicios en línea de Microsoft

SERVICIO DE ALMACENAMIENTO EN LA NUBE	DEFINICIÓN DE HORARIO
Azure Active Direct	Cualquier período de tiempo en que los usuarios no puedan iniciar sesión en el servicio, iniciar sesión en el Panel de acceso, acceder a las aplicaciones en el Panel de acceso y restablecer contraseñas o cualquier período de tiempo en que los administradores de TI no puedan crear, leer, escribir y eliminar

Premi um	entradas en el directorio y / o provisión / desaprovisionamiento de usuarios a aplicaciones en el directorio.
Intercambiar en línea	Cualquier período de tiempo cuando los usuarios no pueden enviar o recibir correos electrónicos con Outlook Web Access.
Micros oft Teams	Cualquier período de tiempo cuando los usuarios no pueden ver el estado de presencia, realizar conversaciones de mensajería instantánea o iniciar reuniones en línea.
Office 365 ProPlu s	Cualquier período de tiempo cuando las aplicaciones de Office se ponen en modo de funcionalidad reducida debido a un problema con la activación de Office 365.
Oficina en línea	Cualquier período de tiempo en que los usuarios no puedan usar las aplicaciones web para ver y editar cualquier documento de Office almacenado en un sitio de SharePoint Online para el que tengan los permisos adecuados.
OneDr ive para Busine ss	Cualquier período de tiempo en que los usuarios no puedan ver o editar archivos almacenados en su almacenamiento personal de OneDrive para la Empresa.
Compartir punto en línea	Cualquier período de tiempo en que los usuarios no puedan leer o escribir ninguna parte de una colección de sitios de SharePoint Online para la que tengan los permisos adecuados.
Yam Mer Enterp subida	Cualquier período de tiempo superior a 10 minutos cuando más del 5 por ciento de los usuarios no pueden publicar o leer mensajes en ninguna parte de la red de Yammer para la cual tienen los permisos adecuados.

Microsoft Intune	Cualquier período de tiempo en que el administrador de TI del cliente o los usuarios autorizados por el cliente no puedan iniciar sesión con las credenciales adecuadas. El tiempo de inactividad programado no excederá de 10 horas por año calendario.
Los micros ofrecen protección avanzada contra amenazas	El total de minutos acumulados que forman parte de los minutos máximos disponibles en los que el cliente no puede acceder a ninguna parte de las colecciones de sitios del portal de Protección contra amenazas avanzadas de Microsoft Defender para las cuales tiene los permisos adecuados y el cliente tiene una licencia válida y activa.

**CUADRO 4-4 Crédito de servicio para porcentajes de tiempo de actividad mensual en el**

Acuerdo de nivel de servicio de licencias por volumen de Microsoft para servicios en

línea de Microsoft

PORCENTAJE HORARIO MENSUAL	CRÉDITO DE SERVICIO
Mayor o igual que 99.9 por ciento	0 por ciento
Menos del 99.9 por ciento	25 por ciento
Menos del 99 por ciento	50 por ciento
Menos del 95 por ciento	100 por ciento

Microsoft requiere que los suscriptores presenten un reclamo por créditos de servicio, que contenga evidencia de los cortes, como

descrito en el siguiente extracto de SLA:

*Para que Microsoft considere un reclamo, debe enviar el reclamo al servicio de atención al cliente de Microsoft Corporation, incluida toda la información necesaria para que Microsoft valide el reclamo, que incluye, entre otros: (i) una descripción detallada del Incidente; (ii) información sobre el tiempo y la duración del tiempo de inactividad; (iii) el número y la ubicación de los usuarios afectados (si corresponde); y (iv) descripciones de sus intentos de resolver el Incidente en el momento del suceso.*

En términos generales, parece que el SLA para los servicios en línea de Microsoft rara vez se necesita. Tabla 4-5 enumera los porcentajes de tiempo de actividad trimestrales mundiales para los servicios en la nube de Office 365 desde 2017, y ninguna de las cifras se acerca a caer por debajo del 99,9 por ciento garantizado. Esto no quiere decir que no hubo algunas interrupciones aisladas que dieron como resultado créditos de servicio, pero el registro general de los productos de Office 365 es impresionante.

**CUADRO 4-5** Porcentajes trimestrales de tiempo de actividad para Office 365, 2017 a 2019

AÑO	TRIMESTRE 1	TRIMESTRE 2	TRIMESTRE 3	TRIMESTRE 4	
2017	99,99 por ciento	99,97 por ciento	99,98 por ciento	99,99 por ciento	

<b>2018</b>	99,99 por ciento	99,98 por ciento	99,97 por ciento	99,98 por ciento
<b>2019</b>	99,97 por ciento	99,97 por ciento		

## Crear solicitudes de soporte

El soporte que reciben los suscriptores para Microsoft 365 depende de su nivel de suscripción y de cómo lo obtuvieron. Casi todas las páginas de la consola del Centro de administración de Microsoft 365 tienen un **¿Necesitas ayuda?** botón en la esquina inferior derecha, y hay un **Apoyo** menú que permite a los administradores buscar ayuda con problemas específicos y crear una solicitud de soporte cuando una solución no está disponible en la información de ayuda existente. Soporte telefónico y por correo electrónico también están disponibles.

Para evitar el uso excesivo y el abuso de sus servicios de soporte, Microsoft define cuidadosamente la división de responsabilidades entre el equipo de soporte de Microsoft y los administradores en los sitios de suscripción de Microsoft 365.

Tabla 4-6 enumera algunas de las responsabilidades de cada una de estas entidades.

### CUADRO 4-6 Responsabilidades de los administradores de Microsoft

365 y soporte técnico de Microsoft

RESPONSABILIDADES DEL ADMINISTRADOR DE MICROSOFT 365	RESPONSABILIDADES DE SOPORTE DE MICROSOFT
Servicio de configuración, configuración y	Responder a problemas de soporte

mantenimiento	enviado por suscriptores
Creación de cuenta de usuario, configuración y mantenimiento.	Recopilar información sobre problemas de soporte técnico de los suscriptores
Contacto de soporte primario para usuarios empresariales	Proporcionar a los suscriptores orientación técnica para los problemas enviados.
Recopilar información de los usuarios sobre problemas de soporte técnico.	Solucione problemas de suscriptores y transmita la información pertinente de la solución
Abordar problemas de instalación y configuración del software del usuario	Mantener comunicación con los suscriptores con respecto a los problemas de servicio en curso.
Solucionar problemas de disponibilidad de servicios dentro de los límites de la organización	Brindar orientación a los evaluadores de preventa y edición de prueba.
Utilice los recursos en línea de Microsoft para resolver problemas de soporte	Proporcionar licencias, suscripción y soporte de facturación.
Autorización y envío de problemas de soporte a Microsoft	Recopilar comentarios de los clientes para mejorar el servicio

Se espera que los administradores de Microsoft 365 hagan lo que puedan para resolver un problema de soporte antes de enviar una solicitud de soporte a Microsoft. Existen considerables recursos de soporte, capacitación, blog y foro en línea de Microsoft disponibles para este propósito, incluyendo el

siguiendo:

- Soporte de Microsoft ( [support.microsoft.com](http://support.microsoft.com) )
  - Ayuda y capacitación de Office ( [support.office.com](http://support.office.com) )
  - Comunidad de Microsoft ( [answers.microsoft.com](http://answers.microsoft.com) )
  - Microsoft 365 Tech Community ( [techcommunity.microsoft.com/t5/Microsoft-365/ctp/microsoft365](http://techcommunity.microsoft.com/t5/Microsoft-365/ctp/microsoft365) )
- 

Cuando un administrador hace clic en **¿Necesitas ayuda?**

botón en la consola del Centro de administración de Microsoft 365 o abre el **Apoyo** menú y selecciona **Nueva solicitud de servicio**, una **¿Necesitas ayuda?** aparece el panel, solicitándole una descripción del problema. Según la descripción proporcionada, aparece material relevante, como procedimientos paso a paso y enlaces a la documentación del producto que podrían ser útiles, como se muestra en Figura 4-14. .

---

Need help?

How do I create users? X

[View insights](#)

**Add a user to Office 365**

1. In the Microsoft 365 admin center, go to [Users > Active users](#).
2. Click **Add a user**.
3. Fill in the information for the user. Choose **Finish adding** when you are done.

Are you using the old admin center? For old steps, or to learn more [see Add users individually or in bulk to Office 365](#)

**Recommended articles**

[Add users individually or in bulk to Office 365 - Admin ...](#)  
To learn more about what a user with these privileges can do, see [About Office 365 admin roles](#). ... Then the Create a new user

[Add users individually or in bulk to Office 365 ...](#)  
The people on your team each need a user account before they can sign in and access Office 365 for business. The easiest way to

[Create users in Dynamics 365 for Customer Engagement app](#)  
You need to have the System Administrator security role or equivalent permissions in Dynamics 365 for Customer

**Contact support**  
Open a service request and get help from a support agent.

**FIGURA 4-14 ¿Necesitas ayuda? panel del Centro de administración de Microsoft 365**

En la parte inferior de la **¿Necesitas ayuda?** el panel es un **Soporte de contacto** enlace que abre el panel que se muestra en Figura 4-15 . En este panel, el administrador puede proporcionar una descripción más detallada del problema, agregar información de contacto, especificar referencias de zona horaria e idioma, y adjuntar documentos pertinentes al problema.

② ③ ④

## Contact support

Title\*

How do I create users

Description

Describe your issue in detail

Confirm your number\*

Confirm your email\*

Oliver\_Cox@olivercox.onmicrosoft.com

Preferred contact method\*

Phone (Response within 21 minutes)  
 Schedule a Callback

Attachments

5 of 5 available. Each file must be less than 25 MB in size.

Add a file

Regional settings

Contact me

**FIGURA 4-15** El panel de soporte de contacto del Centro de administración de Microsoft 365

El soporte que ofrece Microsoft con el producto Microsoft 365 está destinado principalmente a proporcionar ayuda con problemas de instalación y configuración del servicio, como los siguientes:

- **Azure Active Directory** Configuración de dominio, sincronización con servicios de dominio de Active Directory locales y configuración de inicio de sesión único
- **Microsoft 365** Problemas de configuración del servicio
- **Intercambio en línea** Migración y configuración de buzones, configuración de detección automática, configuración de permisos de buzones, uso compartido de buzones y creación de reglas de reenvío de correo
- **SharePoint en línea** Creación de grupos de usuarios, asignación de permisos del sitio y configuración de usuarios externos.
- **Office 365 ProPlus** Instalación de aplicaciones de Office en varias plataformas de dispositivos.
- **Equipos de Microsoft** Configuración de un entorno de equipos y creación de contactos.
- **Microsoft Intune** Dispositivo móvil y configuración de gestión de aplicaciones

Cuando los suscriptores envían solicitudes de soporte a Microsoft, pasan por un proceso de clasificación y se les asigna un nivel de gravedad, utilizando los valores que se muestran en

**Tabla 4-7 .**

**CUADRO 4-7** Niveles de gravedad de soporte de Microsoft

DESCRIPCIÓN DE SEVERI	EJEMPLOS
-----------------------	----------

TY LEVEL		
Crítico al (Sev UNA)	<ul style="list-style-type: none"> <li>● Uno o más servicios son inaccesibles o no funcionan.</li> <li>● La productividad o el beneficio se ven afectados.</li> <li>● Múltiples usuarios se ven afectados.</li> <li>● Se requiere atención inmediata.</li> </ul>	<ul style="list-style-type: none"> <li>● Problemas al enviar o recibir correos electrónicos con Outlook / Exchange Online.</li> <li>● SharePoint Online o OneDrive para sitios de negocios inaccesibles.</li> <li>● Incapacidad para enviar o recibir mensajes o llamadas en Microsoft Teams.</li> </ul>
Alto (Sev SI)	<ul style="list-style-type: none"> <li>● Uno o más servicios están deteriorados, pero aún son utilizables.</li> <li>● Un solo usuario o cliente se ve afectado.</li> <li>● La atención puede esperar hasta el horario comercial.</li> </ul>	<ul style="list-style-type: none"> <li>● La funcionalidad crítica del servicio está retrasada o parcialmente deteriorada, pero operativa.</li> <li>● Las funciones no críticas de un servicio crítico están deterioradas.</li> <li>● Una función es inutilizable</li> </ul>

		en una interfaz gráfica pero accesible usando PowerShell.
No crítico (Sev C)	<ul style="list-style-type: none"> <li>● Una o más funciones con una productividad mínima o impacto en las ganancias se ven afectadas.</li> <li>● Uno o más usuarios se ven afectados, pero una solución alternativa permite una funcionalidad continua.</li> </ul>	<ul style="list-style-type: none"> <li>● Problemas al configurar las opciones de caducidad de la contraseña.</li> <li>● Problemas al archivar mensajes en Outlook / Exchange Online.</li> <li>● Problemas al editar sitios de SharePoint / Online.</li> </ul>

Después de enviar solicitudes de soporte, los administradores pueden monitorear su progreso en el Centro de administración de Microsoft 365 seleccionando **Ver solicitudes de servicio desde el Apoyo** menú para mostrar una lista de todos los tickets de soporte asociados con la cuenta.

Todas las suscripciones de Microsoft 365 incluyen acceso a servicios básicos de soporte, pero para algunos tipos de suscriptores

o suscriptores con necesidades especiales, existen métodos alternativos para obtener soporte, como los siguientes:

- **Vía rápida** El programa FastTrack de Microsoft utiliza un equipo especializado de ingenieros y socios seleccionados para brindarles a los suscriptores que realizan la transición a la nube asistencia en los procesos de previsión, incorporación y administración continua. Los suscriptores que participan en este programa reciben un contacto al que pueden recurrir para problemas de soporte durante la transición de FastTrack.
- **Licencias por volumen** Los suscriptores con un Acuerdo de empresa o un Acuerdo de productos y servicios de Microsoft que incluye Software Assurance reciben un número específico de incidentes de soporte como parte de su acuerdo. El programa Software Assurance incluye asistencia telefónica las 24 horas del día, los 7 días de la semana para problemas críticos de negocios y horario comercial o asistencia por correo electrónico para problemas no críticos.
- **Proveedores de soluciones en la nube** Para los suscriptores que obtienen Microsoft 365 a través de un Proveedor de soluciones en la nube (CSP), el CSP debe ser su primer punto de contacto para todos los problemas de servicio y soporte durante la vigencia de la suscripción. El acuerdo de revendedor entre los CSP y Microsoft exige que el CSP asuma toda la responsabilidad de apoyar a sus clientes, aunque el CSP aún puede escalar los problemas a Microsoft cuando no pueden resolverlos por su cuenta.
- **Soporte profesional de Microsoft** Los suscriptores con problemas de soporte que van más allá del servicio estándar provisto con Microsoft 365 pueden usar el Soporte Profesional de Microsoft para abrir **solicitudes de soporte sobre una base de incidentes de pago**, como se muestra en Figura 4-16. . Hay incidentes individuales disponibles, al igual que cinco paquetes de incidentes.

New support request

1 Product Selection    2 Issue Details    3 Support Plan    4 Severity    5 Contact Information    6 Review    7 Complete

What can we help you with?

Select the product family

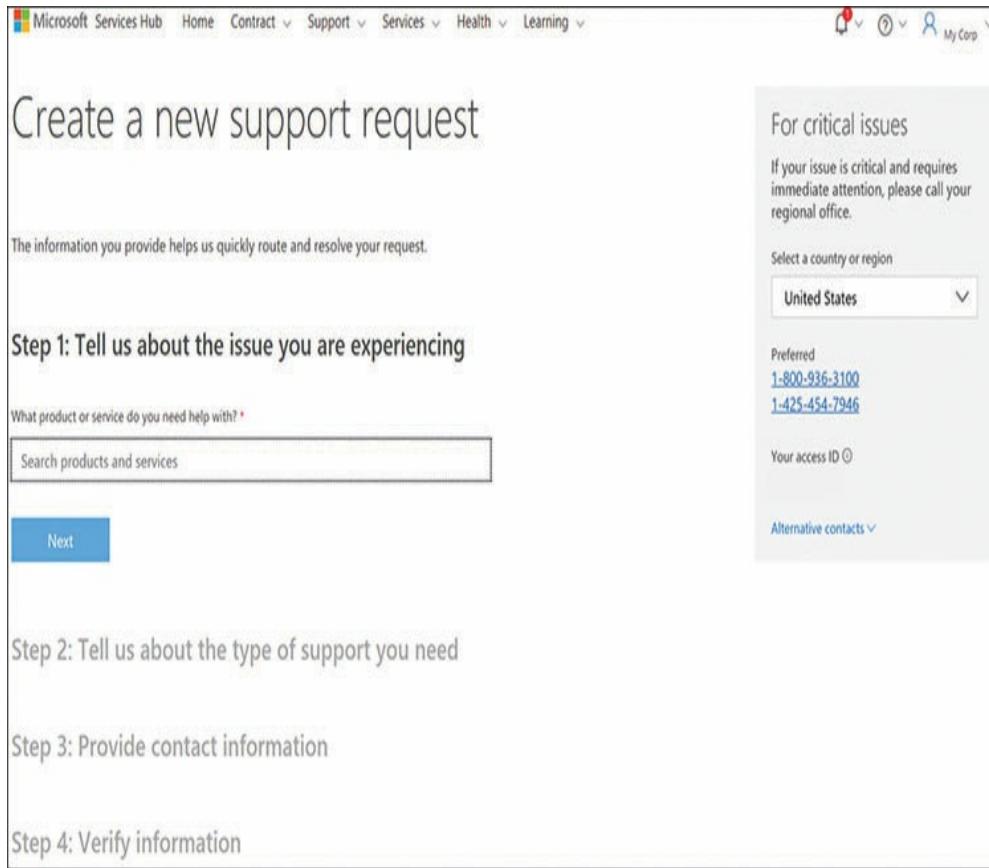
Select the product family

Next

The screenshot shows the 'New support request' wizard with 7 steps. Step 1, 'Product Selection', is active and highlighted in blue. Below it, a dropdown menu is open with the placeholder 'Select the product family'. At the bottom left, a 'Next' button is visible.

**FIGURA 4-16** La pantalla Nueva solicitud de soporte en Soporte profesional de Microsoft

- **Soporte unificado de Microsoft** Los suscriptores pueden comprar un plan de soporte unificado de Microsoft además de sus suscripciones de Microsoft 365. El soporte unificado de Microsoft está disponible en tres niveles: soporte básico, soporte avanzado y rendimiento; cada nivel proporciona niveles crecientes de horas de soporte incluidas, tiempos de respuesta a incidentes y acceso a un administrador de cuentas técnico (TAM), junto con precios crecientes. Los clientes también reciben acceso a Microsoft Services Hub, un portal de soporte que proporciona formularios para enviar solicitudes de soporte (como se muestra en Figura 4-17 ), acceso a incidentes de soporte técnico continuos de Microsoft, herramientas para evaluar las cargas de trabajo de la empresa y materiales de educación y capacitación a pedido.



**FIGURA 4-17** La pantalla de solicitud Crear un nuevo soporte del Centro de servicios de Microsoft

## Determinando la salud del servicio

El monitoreo del funcionamiento continuo de los servicios de Microsoft 365 es una parte crítica del proceso de administración, y el Centro de administración de Microsoft 365 incluye un

**Salud** menú que proporciona una visualización en tiempo real del estado de los servicios individuales cuando los administradores seleccionan **Servicio de salud** opción, como se muestra en Dibujo 418 .

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with options like Home, Users, Devices, Groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, and Health. The 'Service health' option under the Health section is selected. The main content area is titled 'Service health' and shows a table of service status. The table has two columns: 'Name' and 'Status'. The services listed are: Microsoft Intune (Advisory), Office 365 Portal (Advisory), Office for the web (Advisory), Azure Information Protection (Healthy), Exchange Online (Healthy), Flow in Microsoft 365 (Healthy), Identity Service (Healthy), and Microsoft Bookings (Healthy). At the bottom right of the table are 'Need help?' and 'Give Feedback' buttons.

Name	Status
Microsoft Intune	! Advisory
Office 365 Portal	! Advisory
Office for the web	! Advisory
Azure Information Protection	Healthy
Exchange Online	Healthy
Flow in Microsoft 365	Healthy
Identity Service	Healthy
Microsoft Bookings	Healthy

**FIGURA 4-18** La página de mantenimiento del servicio en el Centro de administración de Microsoft 365

Además de mostrar los servicios que son saludables, el **Servicio de salud** La pantalla también enumera otras condiciones del estado del servicio, de la siguiente manera:

- **Avisos** Indica que el servicio aún está disponible pero que existe una condición conocida que inhibe su rendimiento. La condición puede causar interrupciones intermitentes, afectar solo a algunos usuarios o tener un alcance limitado. En algunos casos, una solución alternativa podría estar disponible.
- **Incidentes** Indica que se ha descubierto un problema crítico que hace que todo o una parte significativa del servicio no esté disponible o no se pueda usar. Por lo general, los incidentes se actualizan en sus páginas de detalles con información sobre la investigación, mitigación y resolución del problema.

## Seleccionando el Avisos pestaña en el Servicio de salud

La página muestra detalles sobre los avisos actuales, como se muestra en Figura 4-19 , incluido el servicio afectado, su estado actual y la hora en que se publicó el aviso. los **Incidentes** La página muestra la misma información sobre sucesos más graves. los **Historia** La página enumera todos los incidentes y avisos ocurridos durante los últimos 7 o 30 días.

The screenshot shows the Microsoft 365 Admin Center interface. The top navigation bar includes 'Microsoft 365 admin center', a profile picture for 'Adatum', and a link to 'The new admin center'. The date 'September 21, 2019 11:54 AM' is also displayed. On the left, there's a sidebar with various icons. The main content area is titled 'Service health' and has tabs for 'All services', 'Incidents', 'Advisories' (which is underlined, indicating it's selected), and 'History'. Below this, a note says 'An advisory is a service issue that is typically limited in scope or impact.' A table lists three items:

Title	Service	ID	Status	Start time
Intermittent failures when installing Online Licensed Microsoft Store for Business (MSFB) apps via Microsoft Intune	Microsoft Intune	IT111101	Service degradation	September 19, 2019 5:13 PM
Delayed admin snapshot reports and data freshness issue for Yammer snapshot reports	Office 365 Portal	MO109001	Service degradation	August 28, 2019 12:00 AM
Visio app delays or stalling	Office for the web	OO109105	Service degradation	May 20, 2019 5:00 PM

At the bottom right, there are buttons for 'Need help?' and 'Give Feedback'.

**FIGURA 4-19** La pestaña Avisos de la página Estado del servicio en el Centro de administración de Microsoft 365

los **Estado** indicadores en el **Servicio de salud** Las páginas pueden tener valores como los siguientes:

- **Investigando** Indica que Microsoft conoce el problema y está

Actualmente recopila información antes de tomar medidas

- **Degrado del servicio** Indica que el servicio está experimentando interrupciones intermitentes, ralentizaciones del rendimiento o fallas de funciones específicas
- **Interrupción del servicio** Indica que se está produciendo un problema importante y repetible que impide que los usuarios accedan al servicio
- **Servicio de restauración** Indica que se ha determinado la causa del problema y que se está solucionando el problema, lo que resultará en la restauración del servicio
- **Recuperación Extendida** Indica que la solución del problema está en progreso, pero la restauración del servicio para todos los usuarios puede llevar algún tiempo o que exista una solución provisional que restaure el servicio hasta que se aplique una solución permanente
- **Investigación suspendida** Indica que Microsoft está esperando información de los suscriptores u otras partes antes de que se pueda diagnosticar el problema o se puedan tomar medidas adicionales
- **Servicio restaurado** Indica que Microsoft ha tomado medidas correctivas para abordar el problema y ha logrado que el servicio vuelva a su estado correcto.
- **Informe posterior al incidente publicado** Indica que se ha publicado documentación sobre el problema que contiene una explicación de la causa raíz y los pasos para evitar que vuelva a ocurrir.

Cada aviso o incidente incluye una página de detalles que contiene más información, como se muestra en Figura 4-20 . Esta información puede incluir una mayor elaboración sobre el impacto del usuario del aviso o incidente y un registro de su estado a medida que avanza en el proceso de ser abordado, documentado y resuelto.

X

# Intermittent failures when installing Online Licensed Microsoft Store for Business (MSfB) apps via Microsoft Intune

IT191101, Microsoft Intune; Last updated: September 20, 2019 1:19 PM

Start time: September 19, 2019 5:13 PM

## Status

Service degradation

## User impact

Users may be intermittently unable to install Online Licensed MSfB apps via Microsoft Intune.

[Are you experiencing this issue?](#)

[Is this post helpful?](#)

---

[Latest message](#) [View history](#)

Title: Intermittent failures when installing Online Licensed Microsoft Store for Business (MSfB) apps via Microsoft Intune

User Impact: Users may be intermittently unable to install Online Licensed MSfB apps via Microsoft Intune.

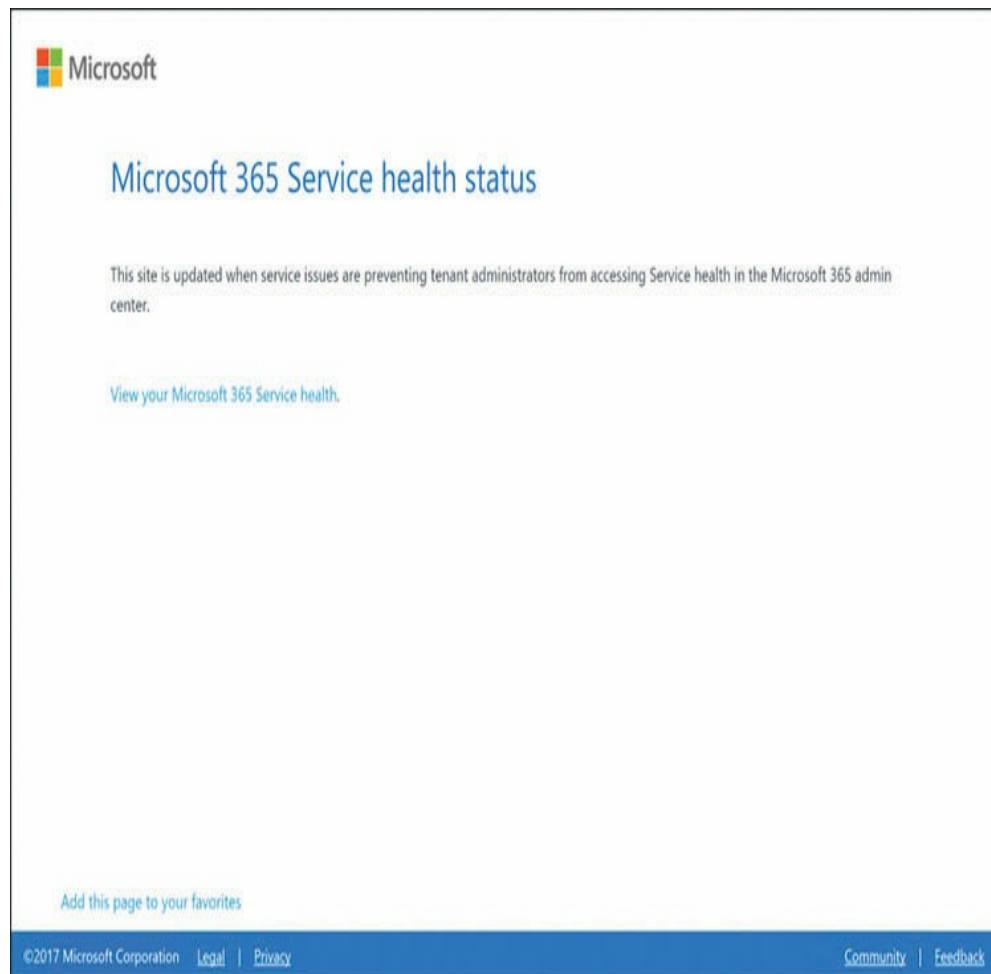
More info: Users may notice that the app may occasionally fail to install without an error message. Users may be able to install Offline Licensed MSfB apps as a potential alternative method to avoid this problem.

Current status: We're continuing to review Mobile Device Management (MDM) logs and we've gathered the relevant product information for the affected apps to determine the underlying cause of the issue.

**FIGURA 4-20** Una página de detalles de asesoramiento en el Centro de administración de Microsoft 365

Cuando se produce un incidente que impide que los administradores inicien sesión en la consola del Centro de administración de Microsoft 365, hay una página de estado de servicio de Microsoft 365 separada disponible en [status.office365.com](http://status.office365.com) eso indica el estado del servicio Microsoft 365 en sí, como se muestra en

Figura 4-21. .



**FIGURA 4-21** El estado de mantenimiento del servicio Microsoft 365

página

**los Servicio de salud** Las páginas del Centro de administración de Microsoft 365 no contienen eventos de mantenimiento planificados que pueden causar interrupciones en el servicio. Para obtener información sobre estas interrupciones, consulte la publicación **Centro de mensajes** página, accesible desde **Salud** menú, como se muestra en Figura 4-22. .

The screenshot shows the Microsoft 365 Admin Center interface with the title 'Microsoft 365 admin center' at the top left and the user 'Adatum' at the top right. A sidebar on the left contains icons for users, groups, devices, and more. The main content area is titled 'Message center'. It displays a list of messages under the heading 'Each message gives you a high-level overview of a planned change and how it may affect your users, and links out to more detailed information to help you prepare. Learn more about managing change.' Below this, there are tabs: 'All active messages' (selected), 'High importance' (underlined), 'Unread messages', and 'Dismissed messages'. The list shows 27 items. Each item has a small red icon, a message title, an 'Act by' date, a 'Category', a 'Last updated' date, and a 'Message ID'. The titles include: 'Basic Authentication Retirement for legacy protocols in Exchange Online' (Act by Oct 31, 2020, Plan For Change, Sep 20, 2019, MC191153); 'Office 2013 Client Connectivity to Office 365 Services' (Act by Oct 13, 2020, Plan For Change, Sep 18, 2019, MC190854); 'Configuration Change for Whiteboard' (Act by Oct 10, 2019, Plan For Change, Sep 17, 2019, MC190301); 'Upload Center is being replaced by the in-app Files Needing Attention experience' (Act by Sep 4, 2019, Plan For Change, Sep 17, 2019, MC190284); 'Office 365 connector to Facebook to be retired' (Act by Sep 4, 2019, Plan For Change, Aug 31, 2019, MC189263); 'Licensing updates for Microsoft Flow & PowerApps in Microsoft 365' (Act by Dec 31, 2019, Plan For Change, Aug 30, 2019, MC189160); and 'Move from Fabric JS to Fabric React or Fabric Core' (Act by TBA, Stay Informed). At the bottom right of the list are buttons for 'Need help?' and 'Give Feedback'.

**FIGURA 4-22** La página del Centro de mensajes en el Centro de administración de Microsoft 365

## HABILIDAD 4.4: ENTENDER EL CICLO DE VIDA DEL SERVICIO EN MICROSOFT 365

---

Con la introducción de sus productos de software basados en suscripción, como Microsoft 365, Microsoft ha tenido que redefinir sus políticas de ciclo de vida del servicio. El ciclo de vida del servicio define durante cuánto tiempo un producto en particular sigue siendo compatible con Microsoft a través del lanzamiento de actualizaciones de software, la aceptación de solicitudes de diseño de características y la disponibilidad de soporte de productos. Microsoft ahora tiene dos políticas de ciclo de vida, como sigue:

- **Política de ciclo de vida fijo** Se aplica a productos con licencia permanente disponibles a través de canales de compra minorista o licencias por volumen y define un período de soporte de 10 años; la licencia sigue siendo válida después de este tiempo, pero se suspende el soporte.
- **Política moderna del ciclo de vida** Se aplica a los productos y servicios basados en suscripción que tienen licencia continua y para los cuales el soporte está en curso, siempre que el cliente se mantenga actualizado aplicando todas las actualizaciones de servicio dentro de un período de tiempo específico.

En la política de Ciclo de vida fijo, el período de soporte de 10 años se divide en dos fases: Soporte principal y Soporte extendido.

- **Soporte principal** Durante la fase de soporte principal de cinco años, el producto recibe actualizaciones de seguridad y características, el soporte de incidentes está disponible y se aceptan solicitudes de mejoras de características.
- **Soporte extendido** Una vez que expira el período de soporte principal, el producto entra en una fase de soporte extendido de cinco años en la que solo se lanzan actualizaciones de seguridad, y el soporte solo está disponible de forma paga. Al final de la fase de Soporte Extendido, el producto ingresa a la fase Más allá del Fin del Soporte, en la que no se lanzan actualizaciones, y solo el soporte pagado está disponible.

La Política de ciclo de vida moderno está destinada a productos para los que el desarrollo y el soporte están en curso, como Microsoft 365. No hay un final fijo para el ciclo de vida, por lo que los suscriptores continúan recibiendo actualizaciones de seguridad y no seguridad, actualizaciones de características y nuevas compilaciones de productos. El soporte telefónico y en línea está en curso. Cuando Microsoft decide finalizar el soporte para un producto regido por la Política de ciclo de vida moderno sin proporcionar un producto sustituto o sucesor, proporcionan un aviso mínimo de 12 meses al final del ciclo de vida.

Los únicos requisitos del cliente para un producto moderno de ciclo de vida son los siguientes:

- El cliente debe mantener una licencia para el producto pagando las tarifas de suscripción requeridas.
- El cliente debe mantenerse actualizado aceptando todas las actualizaciones de servicio para el producto antes de que venza un período de tiempo especificado.

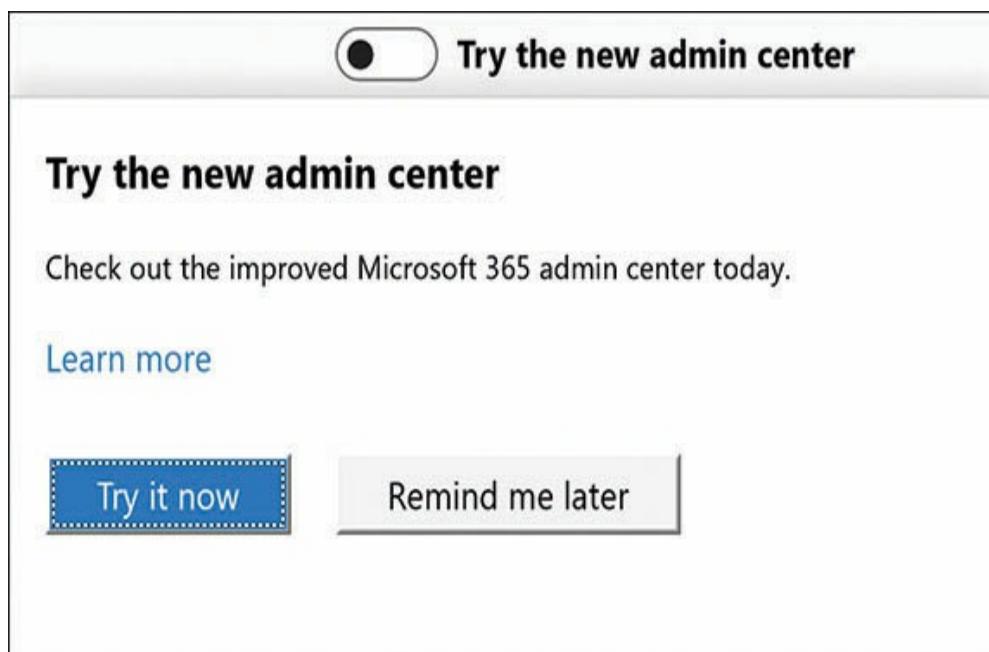
Debido a que los productos de ciclo de vida moderno basados en suscripción como Microsoft 365 no tienen actualizaciones de versiones importantes, se lanzan características nuevas y mejoradas a medida que están disponibles. Debido a que Microsoft 365 es un producto integrado que consta de muchas aplicaciones y servicios, las nuevas características para componentes individuales se desarrollan ylanzan por separado.

En algunos casos, las características y las actualizaciones de características se someten a un ciclo de lanzamiento de vista previa, para que los clientes puedan evaluar la tecnología y proporcionar comentarios a los desarrolladores

en Microsoft Dependiendo del producto y la función, el ciclo de lanzamiento puede incluir las siguientes fases:

- **Vista previa privada** Una vista previa solo por invitación distribuida a un pequeño número de clientes seleccionados para fines de evaluación por parte del equipo de desarrollo del producto o característica.
- **Vista previa pública** Una versión preliminar de un producto o función lanzada a todos los usuarios por el equipo de desarrollo que el cliente puede activar o desactivar según sea necesario. Por ejemplo, el Centro de administración de Microsoft 365 incluye un **Prueba el nuevo centro de administración** cambiar en la esquina superior derecha de la mayoría de sus pantallas, lo que permite a los administradores cambiar entre la interfaz original y la nueva del Centro de administración, como se muestra en

Figura 4-23. .



**FIGURA 4-23** El interruptor Probar el nuevo centro de administración en el Centro de administración de Microsoft 365

- **Disponibilidad general (GA)** Según las pruebas y los comentarios de los clientes, las versiones preliminares pueden retirarse y devolverse para un mayor desarrollo y vistas previas adicionales. Sin embargo, cuando la vista previa

las fases se completan con éxito, el producto o la característica se puede liberar a Disponibilidad general, lo que significa que se proporciona a todos los clientes como un componente oficial del producto.

Los términos y condiciones de las versiones preliminares son específicos del producto que se está probando. En casi todos los casos, son gratuitos y pueden estar cubiertos o no por los términos de atención al cliente especificados en la licencia del producto. Sin embargo, en la mayoría de los casos, existe un mecanismo para proporcionar comentarios a los desarrolladores sobre el rendimiento o la usabilidad de la versión de vista previa.

Para proporcionar información a los clientes sobre el estado de las versiones de actualización para productos específicos, Microsoft mantiene sitios de hoja de ruta que enumeran las actualizaciones en varias fases de finalización. Las actualizaciones figuran en una de las siguientes categorías:

- **En desarrollo** Actualizaciones que aún no se han publicado porque actualmente están en proceso de desarrollo o prueba
- **Rodando** Actualizaciones que han ingresado al proceso de lanzamiento, pero que aún no están disponibles para todos los clientes
- **Lanzado** Actualizaciones que han completado el desarrollo y cualquier fase de vista previa y ahora han entrado en la fase de Disponibilidad general, que las pone a disposición de todos los clientes

El sitio Microsoft 365 Roadmap, que se muestra en Dibujo 424 , contiene un total de 644 actualizaciones al momento de escribir esto. Los **Filtros** en el lado izquierdo de la pantalla, permite al usuario reducir la lista de actualizaciones que se muestran, según los productos, las plataformas, las instancias de la nube y la fecha de la función.

The screenshot shows the Microsoft 365 Roadmap interface. At the top, it says "Microsoft 365 Roadmap" and "Get the Latest Updates". Below that, a message states: "Microsoft 365 is a complete, intelligent solution, including Office 365, Windows 10, and Enterprise Mobility + Security, that empowers everyone to be creative and work together, securely." A banner below the message says "Office 365 is now part of the Microsoft 365 Roadmap. Take a quick tour >". There is a search bar with the placeholder "Search for a product, release or specific update". On the left, there are filters for "Products" (Enterprise Mobility + Security, Office 365, Windows 10), "Platform", "Cloud Instance", and "New & Updated Features". The main area shows "Showing 644 updates<sup>1</sup>:" with three categories: "In development" (169), "Rolling out" (141), and "Launched" (333). A table below lists updates with columns for "Description", "Status", "Tags", and "Release". One update listed is "Risky IP for Active Directory Federation Services (ADFS) extranet lockout protection | Public Preview" with status "Rolling out", tags "Azure Active Directory", and release "Q2 CY2019". Another update is "Improvements in reporting of 'bad items' during mailbox migrations" with status "In development", tags "Exchange", and release "Q3 CY2019". The third update is "Microsoft Information Protection API on Graph" with status "In development", tags "Azure Information Protection", and release "Q4 CY2019". A "Feedback" button is at the bottom right.

Showing 644 updates <sup>1</sup> :				Download	Share	RSS
	In development	Rolling out	Launched			
<input type="checkbox"/> Enterprise Mobility + Security	169	141	333			
<input type="checkbox"/> Office 365						
<input type="checkbox"/> Windows 10						
Platform	+ Risky IP for Active Directory Federation Services (ADFS) extranet lockout protection   Public Preview	Rolling out	Azure Active Directory	Q2 CY2019		
Cloud Instance	+ Improvements in reporting of 'bad items' during mailbox migrations	In development	Exchange	Q3 CY2019		
New & Updated Features	Microsoft Information Protection API on Graph	In development	Azure Information Protection	Q4 CY2019		

**FIGURA 4-24** El sitio de hoja de ruta de Microsoft 365

Cada actualización en la lista contiene una descripción, un indicador de estado, etiquetas o palabras clave que pertenecen al lanzamiento y una fecha de lanzamiento anticipada. Cuando un usuario selecciona una de las actualizaciones, se expande para mostrar información adicional sobre su función y fechas pertinentes, como

se muestra en la Figura 4-25. En algunos casos, la descripción ampliada incluye un **Más información** enlace a documentación adicional de Microsoft de la función y un **Correo** para vincular para reenviar la información a otro usuario.

Description	Status	Tags	Release
Risky IP for Active Directory Federation Services (ADFS) extranet lockout protection   Public Preview	Rolling out	Azure Active Directory	Q2 CY2019
Risky IP is a feature in Azure Active Directory Connect Health for ADFS. Depends on the threshold setup from the portal, Connect Health will notify admins if there are potential IP attacks through ADFS. With Extranet Lockout feature, ADFS will "stop" authenticating the "malicious" user account from outside for a period of time. This prevents your user accounts from being locked out in Active Directory. In addition to protecting your users from an AD account lockout, AD FS extranet lockout also protects against brute force password guessing attacks. The whole IP address list can also be exported from the Connect Health Portal. To get started, visit our documentation today!			
<a href="#">More info</a>			
Featured ID: 33729 Added to Roadmap: 9/21/2018 Last Modified: 3/4/2019 Tags: Azure Active Directory			

**FIGURA 4-25** Detalles de actualización del sitio Microsoft 365 Roadmap

# RESUMEN

---

- Todas las ediciones de Microsoft 365 incluyen Windows 10 Enterprise, Office 365 Pro Plus y Enterprise Mobility + Security. Sin embargo, todos estos componentes están disponibles en sus propios planes, y las ediciones de Microsoft 365 los incluyen en varias combinaciones.
- Los puntos de venta clave para Microsoft 365 se dividen en cuatro áreas principales: productividad, seguridad de colaboración y cumplimiento. Para instalar y ejecutar los componentes de Microsoft 365 y acceder a los servicios en la nube de Microsoft 365, cada usuario de una organización debe tener un Microsoft 365 *licencia de suscripción de usuario (USL)*.
- Evaluar el costo total de propiedad (TCO) para una implementación de Microsoft 365 es relativamente simple; hay una tarifa mensual o anual por cada suscripción de usuario de Microsoft 365 y esas tarifas de suscriptor son predecibles y continuas. Predecir el costo de una red local requiere que las empresas clasifiquen sus gastos distinguiendo entre gastos de capital (CapEx) y gastos operativos (OpEx).
- Las organizaciones pueden comprar suscripciones de Microsoft 365 directamente de Microsoft individualmente o mediante el uso de una variedad de acuerdos de licencias por volumen, incluidos los Acuerdos empresariales (EA), los Acuerdos de productos y servicios de Microsoft (MPSA) o los acuerdos con proveedores de soluciones en la nube (CSP).
- Por lo general, los contratos con proveedores de servicios en la nube incluyen un *acuerdo de nivel de servicio (SLA)*, que garantiza un cierto porcentaje de tiempo de actividad para los servicios y especifica las consecuencias si no se cumple esa garantía.
- Microsoft define cuidadosamente la división de responsabilidades entre el equipo de soporte de Microsoft y los administradores en los sitios de suscripción de Microsoft 365.
- La página de mantenimiento del Servicio en el Centro de administración de Microsoft 365, que muestra una lista de los servicios de Microsoft 365 con un indicador de estado para cada uno.

- Microsoft tiene dos políticas de ciclo de vida: Política de ciclo de vida fijo y Política de ciclo de vida moderno.

## EXPERIMENTO MENTAL

---

En este experimento mental, demuestre sus habilidades y conocimiento de los temas tratados en este capítulo. Puede encontrar la respuesta a este experimento mental en la siguiente sección.

Ralph es responsable de planificar el despliegue de TI para la nueva sucursal de su compañía, que tendrá 50 usuarios. Actualmente está tratando de determinar cuál es la opción más viable económicamente: una solución basada en la nube o servidores locales. Para la solución basada en la nube, Ralph está considerando Microsoft 365 Business, que tiene un precio de \$ 20.00 por usuario, por mes. Para una alternativa local que ofrezca los servicios que sus usuarios más necesitan, Ralph ha buscado en varias fuentes en línea y ha encontrado los precios de licencias de software que se muestran en Tabla 4-8. .

---

**CUADRO 4-8** Precios de licencia de software de muestra

CANTIDAD NECESARIA	PRODUCTO	PRECIO CADA
2	Microsoft Windows Server 2019 Standard (16 núcleos)	\$ 976. 00

1	Licencias de acceso de cliente de Microsoft Windows Server 2019 (paquete de 50)	\$ 1,869 . 99
50	Microsoft Office Hogar y Empresa 2019	\$ 249. 99
1	Microsoft Exchange Server 2019 Standard	\$ 726,9 9
50	Microsoft Exchange Server 2019 CAL estándar \$ 75.99	
1	Microsoft SharePoint Server	\$ 5,523 . 99
50	Licencia de acceso de cliente de Microsoft SharePoint	\$ 55.99

Para Ralph es obvio que la solución local requerirá un gasto de capital mucho mayor, pero se pregunta si podría ser la solución más económica a largo plazo. Según estos precios y sin tener en cuenta todos los demás gastos (incluidos el hardware, las instalaciones y el personal), ¿cuánto tiempo pasaría antes de que las tarifas de suscripción de Microsoft 365 Business para 50 usuarios se vuelvan más caras que los costos de licencias de software locales?

## PENSAMIENTO RESPUESTA DEL EXPERIMENTO

---

Ralph ha calculado los costos totales de licencia de software

para su propuesta de solución local y ha llegado a un gasto total de \$ 29,171.47, como se muestra en **Tabla 4-9**.

**CUADRO 4-9** Muestra de precios de licencias de software (con totales)

CANTIDAD NECESARIA	PRODUCTO	PRECIO CADA	TOTAL
2	Microsoft Windows Server 2019 Standard (16 núcleos)	\$ 976 . 00	\$ 1,95 2,00
1	Licencias de acceso de cliente de Microsoft Windows Server 2019 (paquete de 50)	\$ 1,86 9,99	\$ 1,86 9,99
50	Microsoft Office Hogar y Empresa 2019	\$ 249 . 99	\$ 12,4 99,50
1	Microsoft Exchange Server 2019 Standard	\$ 726 . 99	\$ 726. 99
50	CAL estándar de Microsoft Exchange Server 2019	\$ 75. 99	\$ 3,79 9.50
1	Microsoft SharePoint Server	\$ 5,5 23.99	\$ 5,523.99
50	Licencia de acceso de cliente de Microsoft SharePoint	\$ 55. 99	\$ 2,79 9.50
	<b>Gran total</b>		<b>\$ 29,1 71,47</b>

Las tarifas de suscripción de Microsoft 365 Business para 50 usuarios ascienden a \$ 1,000.00 por mes. Por lo tanto, Ralph ha concluido que después de 30 meses, el costo actual de las suscripciones excederá el costo único de las tarifas de licencia del servidor local.

# Índice

## UNA

Suscripciones A1 / A3 / A5. Ver Microsoft 365 Education

Comportamiento anormal Machine Learning, 89

listas de control de acceso (ACL), 116 - 117

Cuadro de acceso desde cualquier lugar (Usage Analytics), 94

ACL (listas de control de acceso), 116 - 117

activando aplicaciones, 178

Directorio Activo. Ver AD DS (Servicios de dominio de Active Directory) ;

AD FS (Servicios de federación de Active Directory); Azure AD (Active Directory)

AD DS (Servicios de dominio de Active Directory)

  Directorio activo de usuarios y computadoras, 125

  en comparación con los servicios locales, 40 - 41

  características y capacidades de, 114 - 116 , 146 - 148

  políticas de contraseña, 133 - 134

  identidades locales, 124 - 125

  estructura y jerarquía de, 146 - 148

  cuentas de usuario, creación, 114 - 116

AD FS (Servicios de federación de Active Directory), 52 , 131

Complemento USL (licencia de suscripción de usuario), 186

Centro de administración

Menú de facturación, 185 , 194 - 195

Configuración de Exchange Online, 26 - 27

características y capacidades de, 46 - 47

Menú de salud, 204 204 - 208

Página de licencias, 185

Nueva interfaz de grupo, 71

Página de servicios de compra, 185 - 186

Página de salud del servicio, 204 204 - 208

Menú de soporte, 200 - 205

Pruebe la opción El nuevo centro de administración, 209

Menú de Centros de administración (Centro de administración), 47

administración, 36

Cuadro de adopción (análisis de uso), 94

Análisis avanzado de amenazas (ATA), 33 - 34 , 85 , 88 - 91 91 , 143

Protección avanzada contra amenazas (ATP), 22 , 35 , 143 , 182

avisos, 205

AIP (Azure Information Protection), 33 , 85 , 105 - 106 ,

117 - 118 , 139 - 143 , 182

alertas, 154

analítica

Análisis de uso de Microsoft 365, 92 - 94

Microsoft ATA (Advanced Threat Analytics), 33 - 34 ,

85 , 88 - 91 91 , 143

MyAnalytics, 94 - 96

Workplace Analytics, 96 - 99

inicios de sesión anómalos, 89

anticipación de amenazas, 111

Proxy de aplicación, 129 129

Conector proxy de aplicación, 129 129

escaneos de aplicaciones, 112

Virtualización de aplicaciones (App-V), 24 , 64

aplicaciones, definidas, 13 . *Ver también aplicaciones individuales y servicios* es App-V (virtualización de aplicaciones), 24 , 64

arquitectura, nube, 8

arquitectura, servicios en la nube, 9 - 11

nube híbrida 12 - 13

nube privada, 11 - 12

Evaluar la fase (cumplimiento), 184

Inventario de activos, 104 - 106

ATA (Advanced Threat Analytics), 33 - 34 , 85 , 88 - 91 91 , 143

ATP (Protección avanzada contra amenazas), 22 , 35 , 143 , 182

informes de auditoría, 156

autenticación

con Azure AD (Active Directory), 130 - 132

autenticación federada, 131

autenticación de paso, 130

autenticación de contraseña, 128

definicion de, 113 - 114

multifactor

exploraciones biométricas, 134

basado en teléfono celular, 134

definicion de, 134

visión general de, 132

contraseña

Azure AD (Active Directory), 128

cambios de contraseña, 153

sincronización de hash de contraseña, 129 129

políticas de contraseña, 133 - 134

SSPR (restablecimiento de contraseña de autoservicio), 52 - 53 , 153

autorización, 113 - 114

actualizaciones automáticas de funciones, 61

Registre automáticamente nuevos dispositivos unidos al dominio de Windows 10

con la configuración del cliente de Azure Active Directory, 150

Piloto automático, 24

disponibilidad

definicion de, 105

alto, 108

Azur. Ver también Azure AD (Active Directory) ; servicios en la nube

AIP (Azure Information Protection), 33 , 85 , 105 - 106 ,

117 - 118 , 139 - 143 , 182

ATP (Protección avanzada contra amenazas), 22 , 35 , 143 , 182

interfaz de gestión, 6 6

regiones, 162  
mecanismos de fiabilidad, 6 6  
Gestión de derechos (RMS), 33  
RMS (gestión de derechos), 33  
Administración de actualizaciones, dieciséis  
Azure AD (Active Directory)  
Azure AD Connect, 142  
Azure Information Protection, 145  
identidades de nubes, 126 - 127  
características y capacidades de, 13 , 32 , 85 , 143 - 145  
características y servicios de, 144 - 145  
identidades híbridas  
Proxy de aplicación, 129 129  
autenticación, 130 - 132  
definición de, 127  
primera sincronización, 128  
SSO (inicio de sesión único), 129 129  
sincronización, 128 - 129 129  
Protección de identidad, 136 - 139 , 182  
licencias, 143  
MFA (autenticación multifactorial) en, 135 - 136  
servicios locales versus, 40 - 41  
Planes premium, 142 , 144 - 145  
cuentas de usuario, creación, 114 - 116

si

barreras para la adopción de la nube, superando  
factores de costo, 160 - 161  
preocupaciones de seguridad de datos, 161  
ubicaciones de almacenamiento de datos, 162  
visión general de, 158 - 159  
latencia de rendimiento, 159  
requisitos de personal, 163  
escenario de muestra para, 165 - 166  
selección de proveedor de servicios, 159 - 160  
proceso de transición, 163  
dependencia de un proveedor, 160  
robustez del vendedor, 160  
grandes transiciones de interruptor, 43  
Opción de cuentas de facturación (menú de facturación), 194  
facturación y gestión de facturas, 194 - 196  
Menú de facturación (Centro de administración), 47 , 185 , 194 - 195  
Opción de notificaciones de facturación (menú de facturación), 194  
Opción de facturas y pagos (menú de facturación), 194  
exploraciones biométricas, 134  
BranchCache, 45  
Trae tu propio dispositivo. Ver BYOD (traiga su propio dispositivo)  
  
ataques de fuerza bruta, 89  
suscripciones comerciales Ver Microsoft 365 Business  
BYOD (traiga su propio dispositivo), 57 , 102 , 120 , 141

# C

- calendarios, Exchange Online, 25 , 68 , 69
- CapEx (gastos de capital), 188 - 190
- CASB (agente de seguridad de acceso a la nube), 34
- CBA (análisis de costo-beneficio), 188 - 190 , 212 - 213
- autenticación basada en teléfono celular, 134
- Política de CJIS (Servicios de información de justicia penal), 173
- clasificación de usuarios, 109 - 111
- Herramientas de clasificación, 155
- Hacer clic para ejecutar, 64 - 66
- monitoreo de salud del cliente, 150
- Herramientas de gestión de clientes (CMT), 140
- agente de seguridad de acceso a la nube (CASB), 34
- Seguridad de aplicaciones en la nube, 34 , 121 - 122 , 143 , 182
- identidades de nubes, 126 - 127
- servicios en la nube. *Ver también* Azur
- barreras de adopción, superación
- Estudio de caso de Contoso Corp. 165 - 166
- factores de costo, 160 - 161
- preocupaciones de seguridad de datos, 161
- ubicaciones de almacenamiento de datos, 162
- visión general de, 158 - 159
- latencia de rendimiento, 159
- requisitos de personal, 163
- selección de proveedor de servicios, 159 - 160

proceso de transición, 163

dependencia de un proveedor, 160

robustez del vendedor, 160

ventajas de, 3

- administración, 36
- consolidación, 44 - 55
- costos y ahorros monetarios, 3 - 44 , 35 - 36
- despliegue, 35
- infraestructura, 77 - 8
- manejabilidad, 66
- fiabilidad, 55 - 66
- escenario de muestra para, 19
- escalabilidad 55
- seguridad, 77 , 38
- actualizaciones, 35

arquitectura de 8

- nube híbrida 12 - 13
- nube privada, 11 - 12
- nube pública, 9 - 11

concepto de, 1 - 2

desventajas de, 8

recursos en línea, 15

modelos de servicio

- FaaS (Función como servicio), 17
- IaaS (Infraestructura como servicio), 14 - dieciséis
- capas de infraestructura, 13 - 14

PaaS (Plataforma como servicio), dieciséis - 17

SaaS (software como servicio), 18 años

transición a, 163

Estudio de caso de Wingtip Toys, 19

Programa de proveedor de soluciones en la nube (CSP), 190 - 193 , 204 204

cmdlets

    Enable-App, 24

    New-ADUser, 125

    Set-MsolPasswordPolicy, 133

    Set-MsolUser, 133

CMT (herramientas de gestión de clientes), 140

Gráfico de colaboración (Usage Analytics), 94

Panel de colaboración (MyAnalytics), 95

herramientas de colaboración. *Ver también EMS (movilidad empresarial + seguridad)*

análisis para

    MyAnalytics, 95

    Análisis de uso, 94

    Workplace Analytics, 97

Intercambio en línea

    Configuración del Centro de administración, 26 - 27

    herramientas de colaboración, 67 - 68

    en comparación con Exchange Server, 39 - 40

    características y capacidades de, 67 - 68

    servicios, 25 - 26

    planes de suscripción, 26

Microsoft Graph, 81 - 82  
Microsoft Planner, 72 , 76  
Microsoft Stream, 75  
Equipos de Microsoft, 29 - 31 , 77 , 180  
Microsoft Yammer, 72  
Grupos de Office 365, 69 - 73  
Office 365 ProPlus, 62  
OneDrive para la Empresa, 62 , 75 , 180  
visión general de, 66 - 67 , 179 - 181  
Planificador, 180  
selección de, 78 - 80  
SharePoint en línea  
    características y capacidades de, 27 - 29 , 73 - 74 , 180  
    SharePoint Server en comparación con, 40  
Skype Empresarial en línea, 31 , 77  
Corriente, 75 , 180  
Quejarse, 74 - 75 , 175 , 180  
Asistente de configuración de gestión conjunta, 150 - 151  
modelo de cogestión, 44 , 148 - 152  
Cuadro de comunicación (Usage Analytics), 94  
conformidad  
    Gerente de Cumplimiento, 157 - 158  
    conformidad y configuración del dispositivo, 86 - 87  
    servicios para, 182 - 184  
Gerente de Cumplimiento, 157 - 158  
acceso condicional, 149

confidencialidad 105  
consolidación, servicios basados en la nube y, 44 - 55  
Panel de contacto de soporte, 202  
Estudio de caso de Contoso Corp. 165 - 166  
Servicios principales. Ver también EMS (movilidad empresarial + seguridad)

---

ventajas de

administración, 36  
costos, 35 - 36  
despliegue, 35  
seguridad, 38  
actualizaciones, 35

Intercambio en línea

Configuración del Centro de administración, 26 - 27

herramientas de colaboración, 67 - 68

en comparación con Exchange Server, 39 - 40

EOP (Exchange Online Protection), 25

características y capacidades de, 180

servicios, 25 - 26

planes de suscripción, 26

Equipos de Microsoft, 29 - 31 , 180

Office 365 ProPlus

despliegue de, 54 - 56 , 63 - 66

características de, 59 - 61 , 178 - 179

Microsoft Office suite en comparación con, 38 - 39 ,

61 - 63

servicios locales versus

**Directorio Activo, 40 - 41**

**Intercambiar, 39 - 40**

    implementaciones de servicios híbridos, 40

**Oficina, 38 - 39**

**SharePoint, 40**

SharePoint en línea

    Centro de administración, 72

    colaboración con, 180

    en comparación con SharePoint Server, 40

**características y capacidades de, 27 - 29 , 73 - 74 , 180**

    SharePoint Server en comparación con, 40

Windows 10 Business, 25

Windows 10 Enterprise

**despliegue de, 53 - 54**

**características y capacidades de, 22**

    administración, 24

    seguridad, 22

    actualizaciones, 22 - 24

Grupo de servicios básicos y operaciones de ingeniería (CSEO), 103

modelos de costo, 3 - 4 4 , 35 - 36 , 160 - 161

análisis de costo-beneficio (CBA), 188 - 190 , 212 - 213

Crear una interfaz de máquina virtual, 2

Política de servicios de información de justicia penal (CJIS), 173

Nivel de gravedad crítico (Sev A), 203

Programa CSP (Proveedor de soluciones en la nube), 190 , 191 - 193 ,

204 204

Arquitectura de referencia de ciberseguridad, 155

re

Prevención de pérdida de datos (DLP), 26 , 59 , 139 - 140 , 182

estándares de privacidad de datos, cumplimiento con, 182 - 184

ubicaciones de almacenamiento de datos, 162

escaneos de bases de datos, 112

nube pública dedicada, 9

Suplemento de Regulación Federal de Adquisiciones de Defensa (DFARS), 174

Optimización de entrega, 45

DEM (administrador de inscripción de dispositivos), 58

despliegue, 35

servicio híbrido 40

Microsoft 365 49 - 59

estrategias de despliegue, 49 - 50

documentación para, 50

identidad, 51 - 53

protección de la información, 58 - 59

MAM (Gestión de aplicaciones móviles), 57

MDM (Gestión de dispositivos móviles), 56 - 58

redes, 51

Office 365 ProPlus, 54 - 56

Windows 10 Enterprise, 53 - 54

procesos de gestión modernos, 43

Office 365 ProPlus, 63 - 66

    aplicaciones para instalar, seleccionar, 63 - 64

    Hacer clic para ejecutar, 64 - 66

despliegue, *continuado*

    opciones de personalización, 64 - sesenta y cinco

    Implementaciones de Office 2016 y 2019, 66

escenario de muestra para, 99 - 100

autodespliegue, 50

Desktop Analytics, 23

administrador de inscripción de dispositivos (DEM), 58

Estado del dispositivo (Desktop Analytics), 23

protección del dispositivo, 178

    BYOD (traiga su propio dispositivo), 57 , 102 , 120 , 141

    con Cloud App Security, 121 - 122

    con MAM (Gestión de aplicaciones móviles), 121

    con MDM (Gestión de dispositivos móviles), 121

    con Microsoft Intune, 119 - 120

    visión general de, 118 - 119

escenarios de uso de seguridad, 152 - 153

Menú de dispositivos (Centro de administración), 46

DFARS (Suplemento de Regulación Federal de Adquisiciones de Defensa), 174

finca digital, 102

directorío de Servicios. Ver **AD DS (Servicios de dominio de Active Directory)** ; **Azure AD (Active Directory)**

recuperación de desastres, 108

listas de distribución, 67

**DLP (Prevención de pérdida de datos)**, 26 , 59 , 117 - 118 , 139 - 140

protección de documentos

ACL (listas de control de acceso)

**AIP (Azure Information Protection)**, 117 - 118

definición de, 116 - 117

**DLP (Prevención de pérdida de datos)**, 117 - 118

**AIP (Azure Information Protection)**, 33 , 105 - 106 ,  
117 - 118 , 139 - 140 , 143

**DLP (Prevención de pérdida de datos)**, 26 , 59 , 117 - 118 , 139 - 140

visión general de, 116 - 118

Documentos y recursos (Service Trust Portal), 157

Servicios de dominio. Ver **AD DS (Servicios de dominio de Active Directory)**

---

falta del tiempo, 198 - 199

Fase de valor de conducción de la incorporación, 163

listas de distribución dinámica, 67

**mi**

E3 / E5 suscripciones. Ver **Microsoft 365 Enterprise**

EA (Acuerdo de empresa), 190

suscripciones educativas. Ver Microsoft 365 Education

alojamiento de correo electrónico, 62

EMM (gestión de movilidad empresarial), 141

EMS (Enterprise Mobility + Security). Ver también Azure AD (Active Directory)

AIP (Azure Information Protection), 33 , 85 , 105 - 106 ,  
117 - 118 , 139 - 143 , 182

ATA (Advanced Threat Analytics), 33 - 34 , 143

ATP (Protección avanzada contra amenazas), 22 , 35 , 143 , 182

Seguridad de aplicaciones en la nube, 34 , 121 - 122 , 143 , 182

características y capacidades de, 31 , 84 - 85 , 142 - 143

Microsoft Intune

función de gestión conjunta, 148 - 152

conformidad y configuración del dispositivo, 86 - 87

características y capacidades de, 32 - 33 , 85 , 107 ,  
141 - 142 , 182

arquitectura de servicio, 119 - 120

obstáculos a la movilidad y 85

Cmdlet Enable-App, 24

puntos finales, UEM (gestión unificada de puntos finales)

desarrollo de, 140 - 143

EMS (Enterprise Mobility + Security), 142 - 143

Acuerdo de empresa (EA), 190

Movilidad empresarial + seguridad. Ver EMS (movilidad empresarial +  
seguridad)

gestión de movilidad empresarial (EMM), 141

Programa de licencias de fuente empresarial, 191

suscripciones empresariales *Ver Microsoft 365 Enterprise*

Fase de previsión de la incorporación, 163

EOP (Exchange Online Protection), 25

Intercambio en línea

Configuración del Centro de administración, 26 - 27

herramientas de colaboración, 67 - 68

EOP (Exchange Online Protection), 25

Exchange Server en comparación con, 39 - 40

características y capacidades de, 180

servicios, 25 - 26

planes de suscripción, 26

Exchange Server, Exchange Online en comparación con, 39 - 40

ExcludeApp, 64

gastos, capital versus operacional, 188 - 190

Actualizaciones Express, Windows 10 , 45

Indicador de recuperación extendida (estado del servicio), 206

Soporte extendido, 209

Métricas de colaboración externa (Workplace Analytics), 97

## F

Suscripciones F1. *Ver Microsoft 365 F1*

FaaS (Función como servicio), 17

reconocimiento facial, 134

Derechos de falla, 191

Ley de Derechos Educativos y Privacidad de la Familia (FERPA),

183

Programa FastTrack, 49 , 163 , 203

FBI, Política de Servicios de Información de Justicia Criminal (CJIS), 173

Ley Federal de Modernización de la Seguridad de la Información (FISMA), 182

Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP), 156

, 174

autenticación federada, 131

FERPA (Ley de Derechos Educativos y Privacidad de la Familia),

183

lectores de huellas digitales, 134

trabajadores de primera línea, 170

FISMA (Ley Federal de Modernización de la Seguridad de la Información), 182

Política de ciclo de vida fijo, 209

Panel de enfoque (MyAnalytics), 94

carpetas públicas 68

Ataques PAC forjados, 88

De SA USL (licencia de suscripción de usuario), 186

USL completo (licencia de suscripción de usuario), 186

Función como servicio (FaaS), 17

## GRAMO

Versiones de GA (disponibilidad general), 210

Gateway (ATA), 90

GDPR (Reglamento general de protección de datos), 156 , 183

Botón de geografía (Microsoft Graph), 81

Ataques Golden Ticket, 88

suscripciones gubernamentales *Ver Gobierno de Microsoft*

365

Ley Gramm-Leach-Bliley (GLBA), 183

Graph (Microsoft), 81 - 82

grupos

    Política de grupo, 133 - 134

    transición grupo por grupo, 43

    Consultas de grupo a grupo (Workplace Analytics), 98

    modificación de, 89

    Oficina 365, 69 - 73

Menú de grupos (Centro de administración), 46

## H

inventario de hardware, 106 - 108

Requisitos de hardware, 3

hashes 128 - 129 129

Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA), 11 - 12 , 183

Menú de salud (Centro de administración), 47 , 204 204 - 208

Nivel de gravedad alto (Sev B), 203

alta disponibilidad, 108

HIPAA (Ley de Responsabilidad y Portabilidad del Seguro de Salud), 11 - 12 , 183

escala horizontal, 5 5

escaneos de host, 112

Herramientas de caza, 155

Azure AD híbrido, 149

nube híbrida 12 - 13

identidades híbridas 127 - 132

en Azure AD (Active Directory)

Proxy de aplicación, 129 129

autenticación, 130 - 132

contraseñas 128

SSO (inicio de sesión único), 129 129

definicion de, 127

primera sincronización, 128 - 129 129

implementaciones de servicios híbridos, 40

hipervisores 14

yo

IaaS (Infraestructura como servicio), 14 - dieciséis

Fase de identidad (despliegue), 51 - 53

protección de identidad

en AD DS (Servicios de dominio de Active Directory)

identidades híbridas 127 - 132

identidades locales, 124 - 125  
cuentas de usuario, creación, 114 - 116  
autenticación  
definición de, 113 - 114  
multifactor, 134 - 136  
visión general de, 132  
contraseña, 128 - 129 129 , 133 - 134  
autorización, 113 - 114  
en Azure AD (Active Directory), 13 , 114 - 116  
Proxy de aplicación, 129 129  
autenticación, 130 - 132  
identidades de nubes, 126 - 127  
identidades híbridas 127 - 132  
Protección de identidad, 136 - 139 , 182  
contraseñas 128  
SSO (inicio de sesión único), 129 129  
cuentas de usuario, creación, 114 - 116  
identidades de nubes, 126 - 127  
identidades híbridas 127 - 132  
procesos de gestión modernos, 43  
visión general de, 113 - 116 , 123 , 170  
autenticación de contraseña  
en Azure AD (Active Directory), 128  
cambios de contraseña, 153  
sincronización de hash de contraseña, 129 129  
políticas de contraseña, 133 - 134

SSPR (restablecimiento de contraseña de autoservicio), 52 - 53 , 153

identidades en las instalaciones, 124 - 125

niveles de riesgo, 136 - 139

Windows Hello para empresas, 116

En estado de lanzamiento de Desarrollo, 210

incidentes 205

proveedores indirectos, 193

revendedores indirectos, 193

Cuadro de uso del servicio individual (Usage Analytics), 94

Industrias y Regiones (Service Trust Portal), 157

dispositivos infectados, 153

protección de la información, 58 - 59 , 170

infraestructura, servicios en la nube, 7 7 - 8

Infraestructura como servicio (IaaS), 14 - dieciséis

Botón Insertar datos (Microsoft Graph), 82

Panel Insertar desde archivo (Microsoft Graph), 81

instalación. *Ver despliegue*

integridad, datos, 105

Métricas de redes internas (Workplace Analytics), 97

Organización Internacional de Normalización (ISO),

156

Reglamento del Tráfico Internacional de Armas (ITAR),

173 - 174

usuarios internacionales, 173

Internet de las cosas (IoT), 141 - 142

Afinado. *Ver Microsoft Intune*

inventario

bienes, 104 - 106

hardware, 106 - 108

Indicador investigador (Servicio de Salud), 206

Indicador de investigación suspendida (Servicio de salud), 206

IoT (Internet de las cosas), 141 - 142

ISO (Organización Internacional de Normalización),  
156

ITAR (Reglamento de Tráfico Internacional de Armas),  
173 - 174

## JKL

Kerberos 41 , 125

KMS (Servicio de gestión de claves), 66 , 178

etiquetas

retencion, 58

sensibilidad, 58 - 59

movimiento lateral, 89

Estado de lanzamiento lanzado, 210

Opción de licencias (menú de facturación), 194

Página de licencias, 185

opciones de licencia

Azure AD (Active Directory), 143

componentes básicos, 167 - 168

mejores prácticas, 187

CBA (análisis de costo-beneficio) de, 188 - 190 , 212 - 213  
comparación de características, 171 - 173  
**Microsoft 365 Business**, 168 - 169 , 171 - 173  
**Microsoft 365 Education**, 174 - 177  
**Microsoft 365 Enterprise**, 169 - 173  
**Microsoft 365 F1**, 170 - 173  
**Gobierno de Microsoft 365**, 173 - 174  
**Office 365 ProPlus**, 61  
**USL (licencia de suscripción de usuario)**, 185 - 186  
licencias por volumen  
    Programa CSP (Proveedor de soluciones en la nube), 191 - 193  
    tipos de acuerdos de licencia, 190  
**Seguro de software**, 190 - 191  
    apoyo, 203  
políticas de ciclo de vida, 208 - 211  
listas, distribución, 67  
pérdida de dispositivos, 152  
**LTSB** (sucursal de servicio a largo plazo), 24  
**LTSC** (Canal de servicio a largo plazo), 24

## METRO

buzones de correo, Exchange Online, 25 , 68 - 69  
grupos de seguridad con correo habilitado, 68  
Soporte principal, 209  
**MAK** (claves de activación múltiple), 66 , 178

replicaciones maliciosas 88

**MAM (Gestión de aplicaciones móviles), 57 , 121 , 152**

manejabilidad, servicios basados en la nube, 6 6

administración

moderno. *Ver también* Centro de administración

concepto de, 42 - 43

configuración, 43

despliegue, 43

identidad, 43

Modelo de implementación y lanzamiento de Microsoft, 49 - 59

Portal de Office 365, 47 - 49

gestión tradicional en comparación con, 42

transición a, 43 - 44

actualizaciones, 43

WaaS (Windows como servicio), 44 - 45

cargas de trabajo y escenarios, 59

enfoque tradicional para, 42

Windows 10 Enterprise, 24

Métricas de gestión y entrenamiento (Workplace Analytics), 97

**MDM (Gestión de dispositivos móviles), 56 - 58 , 121 , 140 ,**

152

MDOP (Paquete de optimización de escritorio de Microsoft), 191

Consultas de reuniones (Workplace Analytics), 98

Métricas de resumen de reuniones (Workplace Analytics), 97

@menciones, 81

Página del Centro de mensajes, 207 - 208

mensajería

- Intercambio en línea
- Configuración del Centro de administración, 26 - 27
- servicios, 25 - 26
- planes de suscripción, 26

Equipos de Microsoft, 29 - 31 , 180

MFA (autenticación multifactorial)

- Azure AD (Active Directory) y, 135 - 136
- exploraciones biométricas, 134
- basado en teléfono celular, 134
- definición de, 134
- visión general de, 52

Microsoft 365 Business, 168 - 169 , 171 - 173

Microsoft 365 DoD, 174

Microsoft 365 Education, 174 - 177

Microsoft 365 Enterprise, 169 - 173

Microsoft 365 F1, 170 - 173

Gobierno de Microsoft 365, 173 - 174

Hoja de ruta de Microsoft 365, 210 - 211

Microsoft 365 Comunidad del Gobierno de EE. UU. (GCC), 174

Microsoft 365 Comunidad del Gobierno de EE. UU. (GCC) Alta, 174

Análisis de uso de Microsoft 365, 92 - 94

Virtualización de aplicaciones de Microsoft (App-V), 24 , 64

Microsoft ATA (Advanced Threat Analytics). Ver ATA

(Análisis avanzado de amenazas)

**Microsoft Azure.** Ver Azur

Grupo Microsoft CSEO (Servicios principales y operaciones de ingeniería), 103

Arquitectura de referencia de seguridad cibernetica de Microsoft, 155

Protección avanzada contra amenazas (ATP) de Microsoft Defender,

22

Paquete de optimización de escritorio de Microsoft (MDOP), 191

**Microsoft FastTrack.** Ver Programa FastTrack

Red global de Microsoft, 108

**Microsoft Graph,** 81 - 82

Gráfico de seguridad inteligente de Microsoft, 155

Microsoft Intune

función de gestión conjunta, 148 - 152

conformidad y configuración del dispositivo, 86 - 87

características y capacidades de, 32 - 33 , 85 , 107 , 141 - 142 ,

182

Intune para la educación, 176

arquitectura de servicio, 119 - 120

**Microsoft Office 365.** Ver Office 365 ProPlus

Suite de Microsoft Office, 38 - 39 , 61 - 63

**Microsoft Planner,** 72 , 76 , 180

Acuerdo de productos y servicios de Microsoft (MPSA),

190

Soporte profesional de Microsoft, 204 204

**Microsoft Services Hub,** 204 204 - 205

Microsoft Stream, 75 , 180

Equipos de Microsoft, 29 - 31 , 77 , 180

Protección contra amenazas de Microsoft, 153 - 155

Soporte unificado de Microsoft, 204 204

Virtualización de la experiencia del usuario de Microsoft (UE-V), 24

*Acuerdo de nivel de servicio de licencias por volumen de Microsoft para los servicios en línea de Microsoft, 198 - 200*

Microsoft Yammer. *Ver Quejarse*

middleware 13

Minecraft Education Edition con Code Builder, 175

Gestión de aplicaciones móviles (MAM), 57 , 121 , 152

aplicaciones móviles, 178

Administración de dispositivos móviles (MDM), 56 - 58 , 121 , 140 , 152

dispositivos móviles. *Ver protección del dispositivo*

movilidad. *Ver EMS (movilidad empresarial + seguridad)*

Política moderna de ciclo de vida, 209

gestión moderna *Ver también Centro de administración*

concepto de, 42 - 43

configuración, 43

despliegue, 43

identidad, 43

Modelo de implementación y lanzamiento de Microsoft, 49 - 59

estrategias de despliegue, 49 - 50

documentación para, 50

identidad, 51 - 53

protección de la información, 58 - 59

MAM (Gestión de aplicaciones móviles), 57 , 121 ,  
152

MDM (Gestión de dispositivos móviles), 56 - 58 , 121 ,  
140 , 152

redes, 51

Office 365 ProPlus, 54 - 56

Windows 10 Enterprise, 53 - 54

Portal de Office 365, 47 - 49

gestión tradicional en comparación con, 42

transición a, 43 - 44

actualizaciones, 43

WaaS (Windows como servicio), 44 - 45

cargas de trabajo y escenarios, 59

supervisión

salud del cliente, 150

servicio de salud, 204 204 - 208

Canal mensual 56

Canal mensual (dirigido), 56

MPSA (Acuerdo de productos y servicios de Microsoft),  
190

Autenticación multifactorial. Ver MFA (autenticación  
multifactorial)

Claves de activación múltiple (MAK), 66 , 178

replicación maestra múltiple, 124 - 125

Mi biblioteca (Portal de confianza de servicio), 157

MyAnalytics, 94 - 96

## norte

Instituto Nacional de Estándares y Tecnología (NIST),

156

¿Necesitas ayuda? cristal, 201 - 202

Panel de red (MyAnalytics), 95

Fase de red (despliegue), 51

redes

requisitos para, 3 - 4

escaneos de 112

modelo de seguridad, 118 - 119

VPN (redes privadas virtuales), autenticación sobre,

115

Nuevo objeto: cuadro de diálogo Usuario, 125

Derechos de nueva versión, 191

Nuevo cmdlet ADUser, 125

NIST (Instituto Nacional de Estándares y Tecnología),

156

Nivel de gravedad no crítico (Sev C), 203

cuadernos, OneNote, 70 , 175

NT LAN Manager (NTLM), 41

## O

OAuth (Autorización abierta), 41 , 127

ODT (herramienta de implementación de Office), 55 , 63 - sesenta y cinco

Grupos de Office 365, 69 - 73

Portal de Office 365, 47 - 49

Office 365 ProPlus

despliegue de, 54 - 56 , 63 - 66

aplicaciones para instalar, seleccionar, 63 - 64

Hacer clic para ejecutar, 64 - 66

opciones de personalización, 64 - sesenta y cinco

Implementaciones de Office 2016 y 2019, 66

características de, 59 - 61 , 178 - 179

Microsoft Office suite en comparación con, 38 - 39 , 61 - 63

Gráfico de activación de Office (Usage Analytics), 94

Herramienta de implementación de Office (ODT), 55 , 63 - sesenta y cinco

Lente de oficina, 176

Fase de incorporación de la incorporación, 163

OneDrive para la Empresa, 62 , 75 , 180

Cuadernos OneNote, 70 , 175

contraseñas de un solo uso (OTP), 135 - 136

Autorización abierta (OAuth), 41 , 127

Opción de paquete de actualización del sistema operativo, 53

sistemas operativos

definido, 14

apoyo para, 61 - 62

OpEx (gastos operativos), 188 - 190

OTP (contraseñas de un solo uso), 135 - 136

Ataques de paso elevado, 88

## PAGS

- PaaS (Plataforma como servicio), dieciséis - 17
- PAC (Certificado de atributo privilegiado), 88
- Ataques Pass-the-Hash (PtH), 88
- Ataques Pass-the-Ticket (PtT), 88
- autenticación de paso, 130
- autenticación de contraseña
- Azure AD (Active Directory), 128
- OTP (contraseñas de un solo uso), 135 - 136
- cambios de contraseña, 153
- sincronización de hash de contraseña, 129 129
- políticas de contraseña, 133 - 134
- uso compartido de contraseñas, 89
- SSPR (restablecimiento de contraseña de autoservicio), 52 - 53 , 153
- Opción de métodos de pago (menú de facturación), 194
- PBX (intercambio de sucursal privada), 30
- latencia de rendimiento, 159
- persistencia (ataques), 89
- Consultas de persona (Workplace Analytics), 98
- Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA), 183
- requisitos de personal, 4 4 , 163
- Consultas de persona a grupo (Workplace Analytics), 98
- redes físicas 14
- seguridad física, 108

PIPEDA (Ley de Protección de Información Personal y Documentos Electrónicos), 183

Planificador, 72 , 76 , 180

Servicios de planificación, 190

Plataforma como servicio (PaaS), dieciséis - 17

políticas

Centro de seguridad de Microsoft 365, 155

contraseña, 133 - 134

manejo de amenazas, 59

Indicador publicado del informe posterior al incidente (salud del servicio), 206

Power BI. *Ver Analítica de uso*

Cmdlets de PowerShell. *Ver cmdlets*

precios y soporte. *Ver también suscripciones*

componentes básicos, 167 - 168

facturación y gestión de facturas, 194 - 196

puntos de venta clave, 177 - 178

colaboración, 179 - 181

conformidad, 182 - 184

productividad, 178 - 179

seguridad, 181 - 182

Office 365 ProPlus, 62

servicio de salud, monitoreo, 204 204 - 208

políticas de ciclo de vida del servicio, 208 - 211

SLA (acuerdos de nivel de servicio), 195 - 200

limitaciones de, 197

*Acuerdo de nivel de servicio de licencias por volumen de Microsoft*

*para los servicios en línea de Microsoft,*

**198 - 200**

**negociando 195 - 196**

**solicitudes de soporte, creación, 200 - 205**

*responsabilidades del administrador y del equipo de soporte,*

**200 - 201**

**métodos de soporte alternativos, 203 - 205**

*Panel de contacto de soporte, 202*

*¿Necesitas ayuda? cristal, 201 - 202*

*soportar niveles de gravedad, 203*

*tickets de soporte, visualización, 203*

*problemas soportados, 202 - 203*

**USL (licencia de suscripción de usuario), 185 - 186**

*licencias por volumen*

*Programa CSP (Proveedor de soluciones en la nube), 191 - 193*

*tipos de acuerdos de licencia, 190*

**Seguro de software, 190 - 191**

*apoyo, 203*

**centralita privada (PBX), 30**

**nube privada, 11 - 12**

*Vista previa privada, 209*

*Certificado de atributo privilegiado (PAC), 88*

*Gráfico de uso del producto (análisis de uso), 94*

**servicios de productividad, 178 - 179**

*Opción de productos y servicios (menú de facturación), 194*

Fase de protección (cumplimiento), 184  
PSTN (red telefónica pública conmutada), 30  
Ataques PtH (Pass-the-Hash), 88  
Ataques PtT (Pass-the-Ticket), 88  
nube pública, 9 - 11  
carpetas públicas, 68  
Vista previa pública, 209  
Red telefónica pública conmutada (PSTN), 30  
Opción de servicios de compra (menú de facturación), 194  
Página de servicios de compra, 185 - 186

## QR

porcentajes trimestrales de tiempo de actividad, 199 - 200  
Botón de análisis rápido (Microsoft Graph), 82  
reconocimiento, 89  
modo de funcionalidad reducida (Office 365 ProPlus), 62  
redundancia, 4 4  
regiones, Microsoft Azure, 162  
ciclos de liberación, 209 - 211  
fiabilidad de los servicios basados en la nube, 5 5 - 6 6  
acciones remotas, 149  
ejecución remota 89  
informes  
auditoría, 156  
Centro de seguridad de Microsoft 365, 155

Menú de informes (Centro de administración), 47

## Recursos

Centro de administración, 47

Service Trust Portal, 157

Fase de respuesta (cumplimiento), 184

Indicador de servicio de restauración (salud del servicio), 206

etiquetas de retención, 58

Gestión de derechos (RMS), 33

gestión de riesgos

anticipación de amenazas, 111

Inventario de activos, 104 - 106

definición de, 103

inventario de hardware, 106 - 108

niveles de riesgo de protección de identidad, 136 - 139

naturaleza continua de 112

visión general de, 103

clasificación de usuario, 109 - 111

evaluaciones de vulnerabilidad, 112

RMS (gestión de derechos), 33

Mapa vial, 210 - 211

Despliegue de estado de lanzamiento, 210

tiempo de ejecución 13

## S

SaaS (software como servicio), 18 años

SAML (lenguaje de marcado de aserción de seguridad), 41

escalabilidad de servicios basados en la nube, 5 5

exploraciones

solicitud, 112

biométrico 134

base de datos, 112

anfitrión, 112

red, 112

SCCM (Administrador de configuración de System Center)

función de gestión conjunta, 148 - 152

características y capacidades de, 23 , 140 , 142

características de, 148 - 149

actualización en el lugar a Windows 10 Enterprise, 53 - 54

Implementación de Office 365 ProPlus, 63

Instalación de Office 365 ProPlus, 54

SDS (sincronización de datos escolares), 175

inicio de sesión único sin interrupciones, 129 129

puntaje seguro, 155

seguridad, 22 . *Ver también* protección de identidad

ATA (Advanced Threat Analytics), 33 - 34 , 85 , 88 - 91 91 ,

143

ATP (Protección avanzada contra amenazas), 22 , 35 , 143 , 182

tipos de ataque, 88 - 89

desafíos de 101 - 103

Gerente de Cumplimiento, 157 - 158

protección del dispositivo, 178

BYOD (traiga su propio dispositivo), 57 , 102 , 120 , 141  
con Cloud App Security, 121 - 122  
con MAM (Gestión de aplicaciones móviles),  
121  
con MDM (Gestión de dispositivos móviles), 121  
con Microsoft Intune, 119 - 120  
visión general de, 118 - 122  
escenarios de uso de seguridad, 152 - 153  
  
protección de documentos  
ACE (entradas de control de acceso), 116 - 117  
ACL (listas de control de acceso), 116 - 117  
AIP (Azure Information Protection), 33 , 105 - 106 ,  
117 - 118 , 139 - 140 , 143  
DLP (Prevención de pérdida de datos), 117 - 118 , 139 - 140  
visión general de, 116 - 118  
  
Microsoft 365 Business, 168 - 169  
modelo de seguridad de red, 118 - 119  
visión general de, 77 , 38  
físico, 108  
  
gestión de riesgos  
anticipación de amenazas, 111  
Inventario de activos, 104 - 106  
definición de, 103  
inventario de hardware, 106 - 108  
naturaleza continua de 112  
visión general de, 103

clasificación de usuario, 109 - 111  
evaluaciones de vulnerabilidad, 112  
**SCCM (System Center Configuration Manager), 140 ,**  
**142 , 148 - 152**  
centro de Seguridad, 154 - 155  
principios de seguridad, 113  
servicios de seguridad, 181 - 182  
**STP (Service Trust Portal), 156 - 157**  
**UEM (gestión de punto final unificada), 140 - 143**  
escenarios de uso, 152 - 153  
  
Lenguaje de marcado de aserción de seguridad (SAML), 41  
  
Autoservicio de restablecimiento de contraseña (SSPR), 52 - 53 , 153  
autodespliegue, 50  
  
Canal semestral  
Office 365 ProPlus, 56  
Ventanas 10 , 44  
  
Canal semestral (dirigido), 56  
  
Botón Enviar (Microsoft Graph), 81  
  
etiquetas de sensibilidad, 58 - 59  
  
Derechos de recuperación de desastres del servidor, 191  
  
computación sin servidor, 17  
  
créditos de servicio, 199  
  
Indicador de degradación del servicio (mantenimiento del servicio), 206  
  
Página de salud del servicio, 204 204 - 208  
  
Indicador de interrupción del servicio (salud del servicio), 206  
  
Acuerdos de Nivel de Servicio. Ver SLA (nivel de servicio)

**acuerdos)**

políticas de ciclo de vida del servicio, 208 - 211

modelos de servicio (servicios en la nube)

FaaS (Función como servicio), 17

IaaS (Infraestructura como servicio), 14 - dieciséis

capas de infraestructura, 13 - 14

PaaS (Plataforma como servicio), dieciséis - 17

SaaS (software como servicio), 18 años

Controles de organización de servicios (SOC), 156

proveedores de servicio

robustez de 160

selección de, 159 - 160

dependencia de un proveedor, 160

Indicador de servicio restaurado (salud del servicio), 206

**Service Trust Portal (STP), 156 - 157**

Configurar la aplicación de PC de la escuela, 175

Cmdlet Set-MsolPasswordPolicy, 133

Cmdlet Set-MsolUser, 133

Menú de configuración (Centro de administración), 47

Menú de configuración (Centro de administración), 47

soporte de niveles de gravedad, 203

Shadow IT, 34

buzones compartidos, 68 - 69

nube pública compartida, 9

SharePoint en línea

Centro de administración, 72

**características y capacidades de, 27 - 29 , 73 - 74 , 180**

SharePoint Server en comparación con, 40

riesgo de inicio de sesión, 137

**replicación maestra única, 126 - 127**

inicio de sesión único (SSO), 129 129

contrato de seis nueves 4 4

Herramienta de dimensionamiento (ATA), 90

**Skype Empresarial en línea, 31 , 77**

**SLA (acuerdos de nivel de servicio), 159 , 195 - 200**

limitaciones de, 197

*Acuerdo de nivel de servicio de licencias por volumen de Microsoft para los servicios en línea de Microsoft, 198 - 200*

**negociando 195 - 196**

SOC (Controles de organización de servicios), 156

Software como servicio (SaaS), 18 años

**Seguro de software, 190 - 191**

licencias de software, 3

pagos separados, 191

SSPR (restablecimiento de contraseña de autoservicio), 52 - 53 , 153

Indicadores de estado (salud del servicio), 206

Step-up USL (licencia de suscripción de usuario), 186

almacenamiento, 14 , 178

Tabla de uso de almacenamiento (Usage Analytics), 94

**STP (Service Trust Portal), 156 - 157**

Corriente, 75 , 180

suscripciones, 168

Azure AD (Active Directory), 145  
mejores prácticas para, 187

CBA (análisis de costo-beneficio) de, 188 - 190 , 212 - 213

suscripciones, *continuado*

- Intercambio en línea, 26
- comparación de características, 171 - 173
- Microsoft 365 Business**, 168 - 169 , 171 - 173
- Microsoft 365 Education**, 174 - 177
- Microsoft 365 Enterprise**, 169 - 173
- Microsoft 365 F1**, 170 - 173
- Gobierno de Microsoft 365**, 173 - 174
  - licencias por volumen
    - Programa CSP (Proveedor de soluciones en la nube), 191 - 193
    - tipos de acuerdos de licencia, 190
  - Seguro de software**, 190 - 191
    - apoyo, 203

apoyo. *Ver precios y soporte*

Menú de soporte (Centro de administración), 47 , 200 - 205

sincronización

Azure AD (Active Directory), 128 - 129 129

datos del dispositivo, 153

Administrador de configuración de System Center. *Ver SCCM (Administrador de configuración de System Center)*

Servidor de gestión de sistemas, 148

## T

Tome una aplicación de prueba, 175

TAM (gerentes técnicos de cuentas), 204 204

TCO (costo total de propiedad)

calculador, 188 - 190

modelos de costos, comparación de, 160 - 161

escenario de licencia de software de muestra, 212 - 213

Equipos (Microsoft), 29 - 31 , 77 , 180

Métricas de colaboración de equipos (Workplace Analytics), 97

gerentes de cuentas técnicas (TAM), 204 204

amenazas *Ver seguridad*

contrato de tres nueves, 4 4

modelo de servicio en la nube en niveles, dieciséis - 17

costo total de la propiedad. *Ver TCO (costo total de propiedad)*

cupones de entrenamiento, 191

transición a la nube, 163

Centro de confianza (Service Trust Portal), 157

Pruebe la opción El nuevo centro de administración, 209

contrato de dos nueves 4 4

## U

UEM (gestión de punto final unificada), 140 - 143

UE-V (virtualización de experiencia de usuario de Microsoft), 24

UM (mensajería unificada), 25

Mensajería unificada (UM), 25

Administración de actualizaciones (Azure), dieciséis  
**actualizaciones / mejoras, 3 , 22 - 24 , 35 , 43 , 178**  
Disponibilidad de actualización (Desktop Analytics), 23  
Regiones del gobierno de los Estados Unidos, 162  
**Análisis de uso, 92 - 94**  
escenarios de uso, seguridad, 152 - 153  
clasificación de usuario, 109 - 111  
riesgo de usuario, 137  
licencia de suscripción de usuario (USL), 185 - 186  
Menú de usuarios (Centro de administración), 46  
**USL (licencia de suscripción de usuario), 185 - 186**

## V

VDA (Derechos de acceso al escritorio virtual de Windows), 191  
vendedores  
robustez de 160  
**selección de, 159 - 160**  
dependencia de un proveedor, 160  
escala vertical, 5 5  
Ver la opción Solicitudes de servicio (menú Soporte), 203  
**VM (máquinas virtuales), 4 4 - 5 5**  
**VoIP (Voz sobre IP), 30**  
licencias por volumen  
Programa CSP (Proveedor de soluciones en la nube), 191 - 193  
tipos de acuerdos de licencia, 190

Seguro de software, 190 - 191  
apoyo, 203  
VPN (redes privadas virtuales), autenticación sobre,  
115  
evaluaciones de vulnerabilidad, 112

## W X Y Z

WaaS (Windows como servicio), 44 - 45  
WDAC (Control de aplicaciones de Windows Defender), 22  
Semana en las métricas de vida (Workplace Analytics), 96  
Panel de bienestar (MyAnalytics), 95  
Windows 10 Business, 25  
Windows 10 Enterprise  
despliegue de, 53 - 54  
características y capacidades de, 22  
administración, 24  
seguridad, 22  
actualizaciones, 22 - 24  
Windows como servicio (WaaS), 44 - 45  
Piloto automático de Windows, 24 , 150 , 168  
Windows Defender  
Guardia de aplicación, 22  
ATP (Protección avanzada contra amenazas), 22  
WDAC (Control de aplicaciones de Windows Defender), 22  
Windows Hello para empresas, 116 , 134

Protección de la información de Windows (WIP), 59

Windows Insider Channel, 44

Servicio de actualización de Windows Server (WSUS), 23

Windows Thin PC, 191

Derechos de uso de Windows to Go, 191

Windows Update para empresas, 23

Derechos de acceso al escritorio virtual de Windows (VDA), 191

WIP (Protección de información de Windows), 59

escaneos de red inalámbrica, 112

asistentes, configuración de gestión conjunta, 150 - 151

Workplace Analytics, 96 - 99

WSUS (Servicio de actualización de Windows Server), 23

Quejarse, 72 , 74 - 75 , 175 , 180

## Fragmentos de código

Muchos títulos incluyen código de programación o ejemplos de configuración. Para optimizar la presentación de estos elementos, vea el libro electrónico en modo horizontal de una sola columna y ajuste el tamaño de fuente a la configuración más pequeña. Además de presentar el código y las configuraciones en el formato de texto reembolsable, hemos incluido imágenes del código que imitan la presentación que se encuentra en el libro impreso; por lo tanto, cuando el formato reembolsable pueda comprometer la presentación de la lista de códigos, verá el enlace "Haga clic aquí para ver la imagen del código". Haga clic en el enlace para ver la imagen del código de fidelidad de impresión. Para volver a la página vista anteriormente, haga clic en el botón Atrás en su dispositivo o aplicación.

```
<Add SourcePath="\\$Server\\share" Version="15.1.2.3" OfficeClientEdition="32">
  <Product ID="0365ProPlusRetail" >
    <Language ID="en-us" />
    <ExcludeApp ID="Publisher" />
  </Product>
</Add>
```