

AB-650 · CHEAT SHEET · CERTIFYDECK

Microsoft 365 Certified: Microsoft 365 and AI Services Administrator Associate

Dominios, pesos oficiales y habilidades clave del temario de AB-650, para repasar antes del examen.

Nivel: Intermediate (Associate) Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Configure and manage Microsoft 365 tenants and workloads

20–25%

Configure and manage a Microsoft 365 tenant

- El tema de la organización controla el logotipo, los colores y el texto de la barra superior de Microsoft 365; se configura en Perfil de la organización > Temas personalizados y solo lo modifica un administrador global. Un inquilino admite hasta cinco temas: uno predeterminado y cuatro de grupo, ligados solo a grupos de Microsoft 365. La marca de dominio. Con un registrador compatible con Domain Connect, la propiedad y los registros DNS se confirman solos; la configuración de la seguridad de la información y la verificación de la autenticación de la dirección de correo electrónico (no si no, se verifica con un registro TXT, uno MX o un archivo en el sitio web. Puede haber hasta cinco dominios).
 - La configuración de licencias y una suscripción de seguridad, con correo o de Microsoft 365 desde con versión estándar o de destino para todos o para usuarios concretos, lo que exige Administrador global. El Facturación > Licencias, y exige al menos Administrador de grupos, de licencias o de usuarios; no admite grupos.
 - El sistema operativo es determinado por las políticas de la nube de eventos, como el efecto de desactivación de Microsoft 365. Los errores y problemas muestra los fallos. El pago por uso conecta una suscripción de Azure con una 365 muestra los informes de Copilot con el rol Administrador de IA, Power Platform gestiona la capacidad de Copilot directiva y un presupuesto opcional, pero llegar al 100 % no detiene el servicio; solo desconectar el pago lo hace.
- Manage Microsoft 365 workloads**
- Un buzón compartido permite que varias personas lean y envíen correo desde una dirección común sin una cuenta de agentes limita la gobernanza al Administrador de IA o al Administrador global.
 - Quien crea un equipo en Microsoft Teams pasa a ser su propietario. Los propietarios pueden eliminar el equipo. Enviar como para que el mensaje parezca salir del buzón, y Enviar en nombre de, que muestra quien lo envió. Si agregar miembros a un equipo privado y ascender o degradar a otros usuarios; los miembros no. Los canales de la disponibilidad de los miembros, Exchange Sender Policy Framework de reunión del centro de administración de estándar están abiertos a todo el equipo, los privados limitan la pertenencia a una parte de el y los compartidos Teams, junto a la grabación y la transcripción, y también con Set-CsTeamsMeetingPolicy. El administrador decide para el administrador de SharePoint o a los equipos sin acceso a un grupo de Microsoft 365, o sitios de si Copilot exige guardar la transcripción o si el organizador puede elegir. Cuando el organizador desactiva Copilot comunicaciones. En los primeros los permisos se gestionan con los propietarios y miembros del grupo; en los segundos, con los grupos de SharePoint de propietarios, miembros y visitantes. El uso compartido externo debe organizarse sin cambiar sus permisos. Restricted Access Control, en cambio, limita quien puede entrar al sitio a permitirse primero en la organización para poder activarlo en un sitio concreto.
 - El administrador de SharePoint y la barra de comando de SharePoint a Copilot y a la búsqueda de toda la organización, sin cambiar sus permisos. Restricted Access Control, en cambio, limita quien puede entrar al sitio a permitirse primero en la organización para poder activarlo en un sitio concreto.

a localizar sitios con riesgo de sobreexposición antes de extender Copilot.

2. Govern and secure Microsoft 365 tenants and workloads

40–45%

Manage identities in Microsoft Entra

- En Microsoft Entra ID, crear un usuario requiere al menos el rol Administrador de usuarios, e invitar a un invitado externo requiere el rol Invitador de invitados. Al crear la cuenta se define su nombre principal, su contraseña inicial y si el inicio de sesión queda habilitado. Al eliminarla, queda suspendida 30 días antes del borrado definitivo, y en acceso al directorio y qué dominios se permiten o bloquean. Por defecto cualquiera puede invitar invitados, que reciben acceso limitado al directorio, y el rol Invitador de invitados permite delegar esa tarea sin un rol administrativo de seguridad conceden acceso a recursos y pueden contener usuarios o dispositivos; los de distribución y los de seguridad de la información de acceso a recursos, como Administrador de contraseñas para resúmenes frente a Administrador global, con acceso casi ilimitado. Privileged Identity Management convierte las asignaciones de roles en asignaciones aptas que exigen activación, con posible aprobación y autenticación multifactor y solo un administrador a una parte concreta de la organización, no a todo el inquilino. Un Administrador de roles con Administrador de roles con privilegios o un Administrador global puede gestionarlas para otros administradores.

Implement and manage conditional access and device compliance

- La directiva de métodos de autenticación de Microsoft Entra ID es la forma recomendada de administrar como incluso frente a Administradores globales sin un rol asignado en ese ámbito, inician sesión los usuarios y realizan la autenticación multifactor, sustituyendo a las directivas heredadas de MFA.
- Microsoft Entra Password Protection bloquea contraseñas débiles comparándolas, tras normalizarlas, con una lista y de restablecimiento de contraseña. Un Administrador de directivas de autenticación la edita desde Entra ID > global (automática y no configurable) y una lista personalizada de hasta 1000 términos propios de la organización.
- Métodos de autenticación con contraseña, cada método o para un grupo de usuarios o para grupos de roles bloquear su gestión por un Administrador de directivas de autenticación. La misma protección se puede extender a Active cuenta sin ayuda de TI. Configurar requiere al menos el rol de Administrador de directivas de autenticación, y se recomienda exigir un método más para el registro que para el restablecimiento. Con Password Writeback la nueva sesión, filtrando por usuario, aplicación o estado de error; el rol Lector de informes basta para consultarlos. Cada contraseña condicional se aplica en tres niveles: directiva, sesión y entrada fallida incluye un motivo de error y detalles adicionales que suelen indicar la causa y la solución, además aplicación y riesgo y se aplica después de la autenticación de primer factor. Microsoft Entra ID Protection detecta de un código de error consultable en la herramienta de búsqueda de errores.

Secure Microsoft 365 workloads

- Las directivas de alerta del portal de Microsoft Defender generan alertas cuando una actividad maliciosa o que otorgan distinto acceso a informes, gestión de riesgo o configuración de directivas.
- Sospechosa afecta a una entidad, como el correo, un usuario o un buzón; hay directivas predeterminadas que vigilan, por ejemplo, la asignación de privilegios de administrador en Exchange Online. Microsoft recomienda gestionar las y Safe Attachments, gestionadas en Threat policies. Standard y Strict aplican la configuración recomendada por Microsoft y siempre tienen prioridad sobre las directivas personalizadas, sin importar su prioridad. Built-in protection propiedades como Delivery action y Directionality, y corregirlo moviéndolo o eliminándolo (soft delete, hard delete); en el caso de Microsoft Defender lanzar simulaciones de phishing, Credential Harvest, Malware aprobación esas acciones requiere el rol Search and Purge, AIR, con Plan 2, inicia investigaciones automáticas desde Attachment, OAuth Consent Grant o Drive-by URL, eligiendo destinatarios, carga útil, notificaciones y entrenamiento.

Protect data in Microsoft 365 by using Microsoft Purview

- Microsoft Purview DLP identifica y protege información confidencial en Exchange, SharePoint, OneDrive, los Simulation Administrator (control total) o Attack Payload Author (solo cargas útiles).
- mensajes de Teams, los dispositivos mediante DLP de endpoint y, en versión preliminar, Microsoft 365 Copilot. Cada Las etiquetas de confidencialidad de Microsoft Purview clasifican y protegen contenido mediante cifrado, marcas ubicación admite condiciones y acciones distintas: SharePoint y OneDrive pueden bloquear el acceso externo, y de contenido (encabezados, pies de página, marcas de agua) y protección de contenidos como sitios de Teams.
- Los dispositivos de retención de información clasifican la información por categorías de retención, como el sitio o versión, mientras que las Se publican a usuarios y grupos mediante directivas de etiquetas, que fijan una etiqueta predeterminada y pueden etiquetas de retención permiten excepciones por elemento, con funciones como iniciar la retención según un evento
- En el panel de DLP se ven las reglas de retención, un informe de solo, la configuración de la regla y ajuste. Se investigan o marcar como registro. Cuando coexisten varias configuraciones, la retención siempre gana a la eliminación y el principalmente en el portal de Microsoft Defender, que las agrupa en incidentes y las conserva seis meses, o en Microsoft Defender DLP se ven los casos de retención de información, que ofrece un punto central para supervisar el panel de alertas de DLP de Purview, que solo las conserva 30 días. Acceder al panel requiere los roles Manage el uso de Copilot, agentes y otras aplicaciones de IA generativa. Incluye directivas preconfiguradas de un clic, alerts y DLP Compliance Management, o su versión de solo lectura.

evaluaciones de riesgo de datos que detectan el exceso de uso compartido, con una evaluación semanal automática para los 100 sitios de SharePoint más usados, y un Activity explorer con los prompts y respuestas detectados.

3. Manage and secure AI services in Microsoft 365

35–40%

Enable and manage Microsoft 365 Copilot

- El centro de administración de Microsoft 365 ofrece el informe de preparación de Copilot (Informes > Uso > Microsoft Copilot), con la elegibilidad de licencias, el canal de actualización y el uso por aplicación de cada usuario. El agente Microsoft 365 Admin complementa esto respondiendo preguntas de preparación en lenguaje natural, con cambios de configuración y configuración de Copilot.
- SharePoint Advanced Management ofrece el Content Management Assessment e informes de gobernanza de acceso a datos para detectar contenido sobrecompartido antes de habilitar Copilot. Controles como el acceso restringido y el descubrimiento de contenido restringido limitan después el acceso o la visibilidad para Copilot, y Purview Data Security Posture Management añade directivas que detectan, y a veces bloquean, datos confidenciales.
- La directiva Allow web search in Copilot, disponible solo en Cloud Policy Service para Microsoft 365, controla si Copilot y Copilot Chat pueden apoyarse en Bing, con opciones para habilitarla, deshabilitarla o deshabilitarla solo en el modo de trabajo. Un interruptor a nivel de usuario permite además desactivarla; en GCC y DoD permanece desactivada de forma predeterminada hasta configurar la directiva.
- Microsoft 365 Copilot Search no requiere configuración inicial; los usuarios con licencia apta la obtienen automáticamente en el módulo de búsqueda, y los conectores, marcadores y acrónimos ya definidos para Microsoft Search se reutilizan sin cambios. Desde Copilot > Search, los administradores publican, guardan como borrador, programan o ejecutan acrónimos y marcadores, uno a uno o por CSV.
- Desde Copilot > Settings, los administradores deciden si los usuarios pueden autoadquirir Copilot (permitir, solo prueba o no permitir), si el personal admin puede usar Copilot en los centros de administración de Microsoft 365, Exchange, SharePoint y Teams, y si Copilot genera imágenes nuevas o solo ofrece stock. El aviso de IA requiere el rol Administrador de IA, y las preferencias de lanzamiento, Administrador global.

Implement and manage agents in Microsoft 365 and Agent 365

- Microsoft Entra Agent ID exige un patrocinador humano responsable de las decisiones de acceso y permanencia de cada identidad de agente. Si el patrocinador deja la organización, el patrocinio se transfiere automáticamente a su gestor, y Lifecycle Workflows añade tareas de tipo mover o leave para notificarlo o transferirlo activamente.
- Los paquetes de acceso conceden a las identidades de agente grupos, roles de Microsoft Entra y permisos de API OAuth de forma auditable y limitada en el tiempo, mediante solicitud del propio agente, de su patrocinador o asignación directa. El acceso condicional se dirige al usuario en el flujo on-behalf-of, a la identidad de agente en el flujo de credenciales de cliente, y a la cuenta de usuario de agente cuando esta existe.
- En Microsoft Entra Agent ID, los propietarios son administradores técnicos (usuarios individuales o entidades de servicio, nunca grupos) que pueden modificar credenciales y reactivar identidades deshabilitadas; los patrocinadores aportan responsabilidad de negocio con permisos limitados a acciones no destructivas. En los agentes de Agent Builder, varios usuarios comparten el rol de propietario y los administradores pueden reasignarlo.
- La página Agent settings del centro de administración de Microsoft 365 centraliza el gobierno de los agentes: Allowed agent types decide qué categorías aparecen en el catálogo, Sharing controla el uso compartido de los agentes de Agent Builder, y User access decide quién puede usarlos. Las plantillas de Agent 365 agrupan controles de Entra, Purview, SharePoint y Defender que solo se aplican a nuevas activaciones, no de forma retroactiva.
- El Registro de agentes en Agentes > Todos los agentes > Registro, ofrece una vista centralizada de todos los agentes del inquilino, clasificados en agentes de Microsoft, de partners externos, publicados por la organización y compartidos por su creador. Permite filtrar por estado, canal y origen de datos, exportar el inventario, identificar agentes sin propietario y revisar señales de riesgo agregadas de Entra, Defender y Purview.

Secure and govern agents by using Agent 365

- En el Centro de administración de Microsoft 365, la pestaña Seguridad de cada agente permite supervisar su actividad apoyándose en Microsoft Purview. La actividad se revisa con Activity explorer, que muestra la actividad de etiquetado en Exchange, SharePoint, OneDrive y endpoints, y también se puede buscar en el registro de auditoría unificado, que cubre interacciones agente humano, humano-agente, agente-herramientas y agente-agente.
- Purview también permite proteger las instancias de agente con DLP, etiquetas de confidencialidad, Insider Risk Management y eDiscovery, tratándolas de forma explícita como a un usuario en cada directiva.
- Desde la pestaña Seguridad de un agente, si existe una evaluación de referencia de IA disponible, el administrador puede evaluar sus brechas de cumplimiento con Microsoft Purview Compliance Manager. Compliance Manager ofrece plantillas normativas premium para regulaciones de IA, como la Ley de IA de la UE y el NIST AI Risk Management Framework, y cada instancia de agente de Agent 365 se incluye automáticamente en esas evaluaciones.

Monitor AI services in Microsoft 365

- En el centro de administración de Microsoft 365, los administradores gestionan el gasto de IA desde Billing > Cost management, donde revisan costes y crean presupuestos, y desde Copilot > Cost Management, donde configuran directivas de gasto de Créditos de Copilot para servicios como Cowork. Los servicios de pago por uso, como Copilot Chat, se activan con directivas de facturación que enlazan una suscripción de Azure a un grupo de usuarios.
- El informe de uso de Microsoft Copilot en Reports > Usage > Microsoft Copilot del centro de administración de Microsoft 365, muestra usuarios habilitados y activos, tasa de adopción y prompts enviados, además de un desglose de adopción por aplicación (Word, Excel, Teams, Outlook, etc.) que revela qué cargas de trabajo adoptan Copilot con más fuerza. Un usuario cuenta como activo solo al realizar una acción intencionada, como enviar un prompt.
- El Copilot Control System, aparte la medición y los informes de adopción de Copilot entre varias herramientas, el Copilot Dashboard de Viva Insights muestra tendencias de adopción por aplicación e impacto en la productividad; el Advanced Insights Analyst Workbench crea consultas e informes de Power BI personalizados; y el Power Platform admin center, con Copilot Studio Analytics, ofrece métricas de consumo y rendimiento de agentes.
- Los administradores comprueban el estado del servicio de Microsoft Copilot y del resto de servicios de Microsoft 365 en Health > Service health, dentro del centro de administración de Microsoft 365. Esta página distingue entre advisories, que afectan a algunos usuarios pero mantienen el servicio disponible, e incidents, que dejan una función importante inaccesible, y permite configurar notificaciones por correo para uno o varios servicios.