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 la organización de sesión se configura en Seguridad y privacidad > Configuración de la directiva de inicio de sesión; no afecta a Teams ni a Outlook.
- Agregar, modificar o quitar un dominio personalizado en Microsoft 365 exige el rol Administrador de nombres de dominio. Con un registrador compatible con Domain Connect, la propiedad y los registros DNS se confirman solos; si no, se verifica con un registro TXT, uno MX o un archivo en el sitio web. Puede haber hasta cinco dominios por defecto; exige Administrador de usuarios), y Perfil de la organización tiene las preferencias de versión, idioma y zona horaria. Un dominio no puede eliminarse mientras haya usuarios, grupos o aplicaciones que lo usen.
- La creación de licencias por grupo asigna productos y planes de servicio a todos los miembros de un grupo 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 anidados y 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 para cada una. El acceso se da con tres permisos de delegado: Acceso completo para abrir y gestionar el contenido, Enviar como para que el mensaje parezca salir del buzón, y Enviar en nombre de, que muestra quién lo envió. Si agregar miembros a un equipo privado y ascender o degradar a otros usuarios; los miembros no. Los canales estándar están abiertos a todo el equipo, los privados limitan la pertenencia a una parte de él y los compartidos por ambos tipos de canal.
- Quien crea un equipo en Microsoft Teams pasa a ser su propietario. Los propietarios pueden eliminar el equipo, Teams, junto a la grabación y la transcripción, y también con Set-CsTeamsMeetingPolicy. El administrador decide 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 organización sin cambiar sus permisos. Restricted Access Control, en cambio, limita quién puede entrar al sitio a permitirse primero en la organización para poder activarlo en un sitio concreto.
- Un despacho de consultoría, Exchange Online usa Enviar como para que sus abogados respondan desde la dirección de un grupo definido. Los informes de gobernanza de acceso a datos de SharePoint Advanced Management ayudan 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 ese plazo puede restaurarse junto con sus licencias.
- La configuración de colaboración externa de Microsoft Entra controla quién puede invitar usuarios invitados, su 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 más amplio. Entra en conflicto con el acceso entre inquilinos, se aplica de forma más restrictiva.
- Microsoft 365 ofrece varios tipos de grupo. los de Microsoft 365 admiten correo y pertenencia dinámica; los de seguridad conceden acceso a recursos y pueden contener usuarios o dispositivos; los de distribución y los habilitados para correo envían correo pero no admiten pertenencia dinámica. El tipo de grupo no se puede cambiar a Administrador global, con acceso casi ilimitado. Privileged Identity Management convierte las asignaciones de tras crearlo y solo necesita el rol Administrador de grupos para crear, editar, eliminar y restaurar grupos.
- Microsoft 365 ofrece roles de distinto alcance, como Administrador de contraseñas para tareas limitadas 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 administración 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.
- Las unidades administrativas de Microsoft Entra ID agrupan usuarios, grupos o dispositivos para delegar la gestión de forma más acotada. Un administrador con privilegios de rol restringida, que protegen objetos sensibles incluso frente a Administradores globales sin un rol asignado en ese ámbito.

Implement and manage authentication and access in Microsoft Entra

- La directiva de métodos de autenticación de Microsoft Entra ID es la forma recomendada de administrar cómo inician sesión los usuarios y realizan la autenticación multifactor, sustituyendo a las directivas heredadas de MFA 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, gestionada por un Administrador de directivas de autenticación. La misma protección se puede extender a Active cuenta sin ayuda de TI. Configurarlo 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 contraseña también se escribe en Active Directory local.
- Microsoft Entra Password Protection bloquea contraseñas débiles comparándolas, tras normalizarlas, con una lista 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); Attachment, OAuth Consent Grant o Drive-by URL, eligiendo destinatarios, carga útil, notificaciones y entrenamiento.
- Microsoft Entra Multi-Factor Authentication añade un segundo factor, como una aplicación de autenticación, una clave de seguridad FIDO2 o un método biométrico, para que un inicio de sesión robado no baste por sí solo. Se puede exigir en todos los usuarios, en grupos concretos o mediante acceso condicional, que evalúa señales como usuario, ubicación, dispositivo, aplicación y riesgo, y se aplica después de la autenticación de primer factor. Microsoft Entra ID Protection detecta entrada fallida incluye un motivo de error y detalles adicionales que suelen indicar la causa y la solución, además de un código de error consultable en la herramienta de búsqueda de errores.
- Los administradores investigan fallos de inicio de sesión en Entra ID > Supervisión y estado > Registros de inicio de sesión, filtrando por usuario, aplicación o estado de error; el rol Lector de informes basta para consultarlos. Cada acceso condicional aplica directivas si-entonces basadas en señales como usuario, ubicación, dispositivo, 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 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 alertas desde Email & collaboration > Policies & rules > Alert policy, porque ahí se crean y editan todas las directivas, incluidas las predeterminadas, y se ajustan umbrales, destinatarios y gravedad. Las alertas de Microsoft Defender for Office 365 se integran con Microsoft Purview.
- En Defender for Office 365, el correo se protege con directivas antimalware, antispam, antiphishing, Safe Links 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 tiene correlaciones para investigar campañas automáticamente. Safe Links reescribe y analiza URL en el momento del clic, y Safe Attachments abre los archivos adjuntos en un entorno aislado antes de entregarlos. Credential Harvest, Malware aprobar esas acciones requiere el rol Search and Purge. AIR, con Plan 2, inicia investigaciones automáticas desde alertas como denuncias de usuarios y pone en cola acciones para que SecOps las apruebe.

Protect data in Microsoft 365 by using Microsoft Purview

- Microsoft Purview DLP identifica y protege información confidencial en Exchange, SharePoint, OneDrive, los mensajes de Teams, los dispositivos mediante DLP de endpoint y, en versión preliminar, Microsoft 365 Copilot. Cada 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 contenedores como sitios de Teams. los dispositivos pueden pegar o imprimir. Las directivas se crean en el portal de Purview.
- Las etiquetas de confidencialidad de Microsoft Purview clasifican y protegen contenido mediante cifrado, marcas Se publican a usuarios y grupos mediante directivas de etiquetas, que fijan una etiqueta predeterminada y pueden exigir justificación para reducir la confidencialidad. Un elemento solo lleva una etiqueta a la vez.
- Las directivas de retención aplican la misma configuración a todo el contenido de un sitio o buzón, mientras que las etiquetas de retención permiten excepciones por elemento, con funciones como iniciar la retención según un evento 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 Purview Data Lifecycle Management (clásico), hasta 10 años.
- Microsoft Purview Data Security Posture Management (DSPM) añade IA 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.
- Microsoft Purview Data Security Posture Management (DSPM) for AI ofrece un panel de control para supervisar 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 que siempre requieren confirmación del administrador.
- 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 excluyen 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 leaver para notificarlo o transferirlo activamente. Cada tarea de administración de agentes exige un rol de Microsoft Entra distinto.
- 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 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.
- La pestaña Seguridad de un agente remite a AI observability, dentro de Data Security Posture Management for AI, para ver la actividad de riesgo de los agentes: uso compartido excesivo, exfiltración y comportamiento poco ético. 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 al crearse.

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 reparte 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.