MD-102 · CHEAT SHEET · CERTIFYDECK

Microsoft 365 Certified: Endpoint Administrator Associate

Apuntes, pesos oficiales y habilidades clave del temario de MD-102, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 100 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Prepare infrastructure for devices

20–25%

Add devices to Microsoft Entra ID

- La unión a Microsoft Entra es para dispositivos de la organización que inician sesión con una cuenta de trabajo y se administran solo por MDM; el registro en Microsoft Entra sirve para BYOD con cuenta personal; la unión híbrida mantiene la unión al dominio local para directiva de grupo o aplicaciones con autenticación de equipo. Entra join no admite Windows Home.
- Los dispositivos Windows se unen a Microsoft Entra ID por autoservicio en OOBE o Configuración, con Windows Autopilot o con inscripción masiva mediante un paquete de aprovisionamiento. En el autoservicio, quien une el dispositivo es su usuario principal y administrador local de forma predeterminada; la directiva de registro de dispositivos controla quién puede unir y cuántos dispositivos por usuario.
- El registro en Microsoft Entra identifica los dispositivos BYOD sin exigir una cuenta de trabajo para iniciar sesión: en Windows desde Configuración o al abrir una aplicación de trabajo, en iOS y Android con Company Portal o Authenticator, y en macOS con Company Portal. Registrar no es inscribir en Intune, y el número máximo de dispositivos por usuario se controla en Microsoft Entra ID.
- Los grupos de seguridad de Microsoft Entra pueden ser asignados o dinámicos. Las reglas de dispositivos solo evalúan atributos del dispositivo (deviceOSType, devicePhysicalIds con [ZTDId] u [OrderID], enrollmentProfileName, deviceTrustType, deviceOwnership con el valor Company) y se escriben en el cuadro de texto; no pueden mezclar usuarios y dispositivos. Para asignaciones solo de Intune conviene valorar los filtros de asignación.

Enroll devices to Microsoft Intune

- Intune ofrece restricciones de plataforma (plataforma, versión del sistema, fabricante en Android y propiedad personal) y de límite de dispositivos, cada una con una directiva predeterminada que se aplica hasta asignar otra de mayor prioridad. Solo afectan a inscripciones controladas por el usuario y no son una medida de seguridad. Los permisos corporativos permiten marcar dispositivos como corporativos antes de registrarse.
- La inscripción automática de Windows inscribe en Intune los dispositivos al unirse o registrarse en Microsoft Entra ID, según el ámbito de usuario MDM (Ninguno, Algunos o Todos). Se usa con BYOD, inscripción masiva, directiva de grupo para dispositivos con unión híbrida, administración conjunta y Windows Autopilot. Las URL de MDM se dejan en blanco y los valores predeterminados.
- Para iPhone y iPad personales, Intune ofrece la inscripción de dispositivos con Company Portal o basada en web, que administra todo el dispositivo, y la inscripción de usuario basada en cuenta, que separa los datos de trabajo y requiere un archivo de detección de servicios en el dominio. En Mac personales, el usuario instala Company Portal desde el paquete de Mac y aplica el perfil de inscripción.
- Android Enterprise ofrece perfil de trabajo personal (BYOD), totalmente administrado (un usuario, solo trabajo), dedicado (quiosco sin usuario, con o sin modo compartido de Entra) y corporativo con perfil de trabajo. Los perfiles corporativos generan un token y un código QR, y requieren restablecer de fábrica. En los fallos de inscripción se revisa el acceso condicional (que exige cumplimiento) y los límites de dispositivos por usuario.
- La inscripción automatizada (ADE) inscribe iPhone, iPad y Mac corporativos (antes Apple Business Manager) mediante un token: se descarga la clave pública de Intune, se crea el servidor MDM en Apple, se carga el token .p7m y se asignan los dispositivos. Conviene fijar una directiva predeterminada, y los cambios en una directiva solo se aplican tras restablecer el dispositivo, salvo la plantilla de nombre.

Implement identity and compliance

- Intune RBAC combina roles integrados (como Intune Role Administrator, Policy and Profile Manager o Help Desk Operator), roles personalizados con permisos concretos y asignaciones de rol con grupos de administradores, grupos de ámbito y etiquetas de ámbito. Con Windows 365 aparecen Cloud PC Administrator y Cloud PC Reader, y los roles personalizados de Cloud PC se crean en el centro de administración de Intune.
- En Intune, los roles definen qué puede hacer un administrador y las etiquetas de ámbito qué objetos ve. Una asignación de roles combina miembros, Ámbito (grupos) y Ámbito (etiquetas); los objetos que crea un administrador reciben sus etiquetas, y una asignación sin etiquetas ve todos los objetos. El rol Administrador de Intune de Microsoft Entra concede todos los permisos de Intune y los derechos de unirse a Windows Autopilot para agregar.
- La aprobación de varios administradores de Intune usa directivas de acceso por tipo de recurso (aplicaciones, cumplimiento, catálogo de configuración, acciones del dispositivo, roles, scripts y configuración de inquilinos), para que otra cuenta apruebe cada cambio. El grupo de aprobadores debe ser de seguridad y estar asignado a un rol de Intune, nunca aprueba sus propias solicitudes y el solicitante selecciona la directiva y la configura tras la aprobación.
- Cada plataforma necesita su propia directiva de cumplimiento, y el motor de cumplimiento decide si un dispositivo sin directiva se marca como conforme o no conforme. La acción integrada Marcar el dispositivo como no conforme se programa a cero días; retrasarla crea un periodo de gracia, y otras acciones envían correos, bloquean o añaden el dispositivo a la lista de vetados.
- Intune informa del estado de cumplimiento a Microsoft Entra ID y el control de concesión Requerir que el dispositivo esté marcado como conforme lo usa para permitir o bloquear el acceso. Conviene crear antes la directiva de cumplimiento, excluir las cuentas de emergencia y empezar en Solo informe; el control no bloquea la inscripción en Intune y puede combinarse con MFA mediante Requerir uno de los controles seleccionados.

2. Manage and maintain devices

25–30%

Deploy and upgrade Windows clients by using cloud-based tools

- Windows Autopilot con perfiles de implementación requiere registrar los dispositivos, usa la ESP y admite preaprovisionamiento, autoimplementación y unión híbrida. La preparación de dispositivos de Windows Autopilot no requiere registro, solo hace unión a Microsoft Entra en modo controlado por el usuario o automático, añade el dispositivo a un grupo asignado cuyo propietario es Intune Provisioning Client e instala aplicaciones Win32 y LOB juntas.
- El modo controlado por el usuario asocia el dispositivo a quien inicia sesión y admite unión a Microsoft Entra o híbrida. El preaprovisionamiento divide el proceso: un técnico aplica lo dirigido al dispositivo y lo vuelve a sellar, y luego el usuario termina. La autoimplementación no pide credenciales, sirve para quioscos y equipos compartidos, solo admite unión a Microsoft Entra y, como el preaprovisionamiento, necesita TPM 2.0 físico.
- En un perfil de implementación con unión a Microsoft Entra, Aplicar plantilla de nombre de dispositivo usa %SERIAL% para el número de serie y %RAND:x% para dígitos aleatorios, y el nombre no puede ser solo números. En la unión híbrida solo hay un prefijo en el perfil Domain Join, y en la preparación de dispositivos la plantilla requiere asociar el dispositivo al inquilino.
- Para implementar con Windows Autopilot se registra el hash de hardware (por el fabricante, con Get-WindowsAutopilotInfo o con un CSV), se crea un grupo dinámico con reglas como [ZTDid] u [OrderID] para la etiqueta de grupo y se asigna el perfil. Si dos perfiles apuntan al mismo grupo gana el más antiguo, y la unión híbrida requiere Intune Connector for Active Directory y un perfil Domain Join.
- La página de estado de inscripción (ESP) muestra el progreso del aprovisionamiento y puede bloquear el dispositivo hasta que se instalen las aplicaciones y perfiles requeridos. Intune aplica primero el perfil de mayor prioridad asignado al dispositivo, luego el del usuario y, si no hay ninguno, el predeterminado; con una lista de aplicaciones seleccionadas, la ESP solo espera a esas aplicaciones.

Plan and implement device configuration profiles

- Para Windows, Intune ofrece el catálogo de configuración, las plantillas y las plantillas administrativas importadas a partir de archivos ADMX y ADML personalizados o de terceros, que deben importarse respetando sus dependencias de espacio de nombres. Group Policy analytics importa los GPO exportados como XML, muestra qué configuraciones admite MDM y permite migrarlas a una directiva del catálogo de configuración.
- En Android Enterprise, los perfiles de restricciones de dispositivos (plantillas o catálogo de configuración) controlan los dispositivos corporativos y el perfil de trabajo de los personales. En dispositivos dedicados y totalmente administrados, el modo de quiosco ejecuta una sola aplicación o varias con Managed Home Screen, requeridas y asignadas; en el perfil de trabajo se regulan el portapapeles y el uso compartido entre perfiles.
- Los perfiles de restricciones de dispositivos de iOS/iPadOS usan las restricciones de Apple y muchas opciones exigen dispositivos supervisados mediante la inscripción automatizada de dispositivos. El modo de quiosco (App Lock) y la lista de aplicaciones visibles u ocultas requieren supervisión; la lista de aplicaciones restringidas solo informa y, para impedir que una aplicación se ejecute, se usa el catálogo de configuración.
- En macOS, Intune ofrece el catálogo de configuración, las plantillas de características y restricciones de dispositivos y los perfiles personalizados con archivos .xml o .mobileconfig, que admiten tokens de dispositivo entre llaves dobles. Las preferencias de privacidad aprueban o deniegan de antemano el acceso de aplicaciones a recursos protegidos.
- Los dispositivos Zebra con Android Enterprise se configuran con perfiles OEMConfig y la aplicación OEMConfig de Zebra de Managed Google Play; los perfiles MX con StageNow son para el administrador de dispositivos Android. HoloLens 2 usa perfiles de Windows Holographic for Business, con VPN solo en ámbito de dispositivo. Los Teams Rooms de Autopilot se agrupan por la etiqueta MTR- y se excluyen de las demás directivas.

Implement Intune Suite add-on capabilities

- La Administración con privilegios para puntos de conexión (Endpoint Privilege Management, EPM) deja a usuarios estándar elevar archivos concretos. La directiva de configuración de elevación activa el cliente y fija la respuesta predeterminada de todo el dispositivo y el ámbito de los informes; las reglas de elevación definen el tipo (automática, confirmada por el usuario, aprobada por soporte o denegada) y los procesos secundarios.
- El catálogo de aplicaciones empresariales (Enterprise App Catalog) ofrece apps Win32 preparadas por Microsoft con comandos, requisitos y reglas de detección ya rellenados; las instala la extensión de administración de Intune, no WinGet. Con una asignación Requerida se puede activar la actualización automática; si quieres revisar o escalonar versiones, usa la sustitución guiada, que no copia asignaciones ni etiquetas de ámbito.
- Ayuda remota (Remote Help) se habilita para todo el inquilino y exige que ayudante y usuario inicien sesión con cuentas de Microsoft Entra de la misma organización. El ayudante necesita Remote Tasks - Offer remote assistance, Remote Assistance Connector - Read y al menos un permiso de Remote Help (ver pantalla, control total, elevación o control desatendido), con el ámbito que cubra al usuario o dispositivo.
- Microsoft Cloud PKI crea en la nube una CA raíz y una CA emisora (o una CA emisora anclada a tu propia CA) y aporta un servicio SCEP, sin NDES ni Intune Certificate Connector. Por plataforma creas perfiles de certificado de confianza para la raíz y la emisora y un perfil SCEP con el SCEP URI de la CA emisora. El panel de cada CA emisora muestra certificados activos, caducados y revocados y permite revocarlos.
- Microsoft Tunnel Gateway se ejecuta en un contenedor sobre un servidor Linux; Tunnel for MAM lo extiende a dispositivos Android e iOS no inscritos. En Android, Defender es el cliente del túnel y hacen falta dos directivas de configuración de aplicaciones (Defender y Edge) y una directiva de protección de aplicaciones que inicia el túnel al abrir la app. El estado se revisa en el centro de administración, con mst-cli y con journalctl.

Perform remote actions on devices

- Sincronizar fuerza un registro inmediato del dispositivo con Intune y reiniciar depende de una notificación push. Retirar quita los datos, apps y perfiles corporativos y anula la inscripción, pero conserva los datos personales; borrar restablece el dispositivo a la configuración de fábrica. En Windows, el borrado puede conservar el estado de inscripción y la cuenta de usuario o continuar aunque se pierda la alimentación.
- Las acciones masivas de dispositivo ejecutan una acción en muchos dispositivos a la vez: eliges el sistema operativo y la acción, seleccionas los dispositivos y creas la tarea. Las acciones disponibles dependen de la plataforma; en Windows incluyen Autopilot Reset, recopilar diagnósticos, cambiar nombre, sincronizar, reiniciar, retirar, borrar y eliminar. Retirar, borrar y eliminar tienen prioridad sobre las demás acciones pendientes.
- La acción Actualizar la inteligencia de seguridad de Windows Defender descarga al momento los archivos de inteligencia de seguridad de Microsoft Defender Antivirus, distinta del examen rápido y del completo. En Graph es windowsDefenderUpdateSignatures, que requiere DeviceManagementManagedDevices.PrivilegedOperations.All. En la directiva de antivirus, el intervalo de comprobación con valor 0 desactiva la búsqueda de actualizaciones.
- La acción de rotación de claves de BitLocker renueva en remoto la clave de recuperación de la unidad del sistema, por ejemplo después de que el soporte técnico la haya compartido. En dispositivos unidos a Microsoft Entra o con unión híbrida, la directiva de BitLocker debe habilitar la rotación de contraseñas de recuperación controlada por el cliente y guardar la información de recuperación en Microsoft Entra ID.
- La acción Rotate local admin password cambia a mano la contraseña de la cuenta de administrador local que gestiona Windows LAPS, fuera de la programación de la directiva, y reinicia el plazo de PasswordAgeDays. El dispositivo debe tener Windows LAPS haciendo copia de la cuenta en el directorio y, si está unido a Microsoft Entra, estar en línea. Se rota de uno en uno, no como acción masiva.

3. Protect devices

15–20%

Configure endpoint security

- Las directivas de antivirus de seguridad de los puntos de conexión agrupan solo la configuración de Microsoft Defender Antivirus para Windows, macOS y Linux, con perfiles de antivirus, exclusiones, Windows Security experience (incluida la protección contra alteraciones) y controles de actualización. Las exclusiones se combinan entre directivas; en el resto de conflictos gana la más segura y después la última modificada.
- La directiva de cifrado de discos usa perfiles BitLocker y Personal Data Encryption en Windows y FileVault en macOS; el cifrado silencioso exige desactivar la advertencia de otro cifrado y no pedir PIN de inicio. Las claves se guardan en Microsoft Entra ID, se rotan con una acción remota y los usuarios pueden recuperarlas en autoservicio. El informe de cifrado muestra la preparación y el estado de la unidad del sistema.
- La directiva de firewall configura el firewall integrado de macOS y Windows, y también de Windows Server mediante la administración de la configuración de seguridad de Defender for Endpoint. Dos perfiles Windows Firewall con valores distintos para la misma opción no la envían; las reglas sin conflicto de varios perfiles de reglas se combinan y las que chocan llegan ambas al dispositivo.
- Las directivas de reducción de la superficie expuesta a ataques incluyen reglas ASR, Device Control, Exploit Protection y otros perfiles, y requieren que Defender Antivirus sea el antivirus principal. Las reglas se combinan por dispositivo y solo se retienen las que chocan; las exclusiones pueden ser globales o por regla. Siguiendo Confianza cero, las reglas no estándar se prueban en Audit por anillos antes de Block.
- Las líneas base de seguridad son grupos de opciones preconfiguradas por los equipos de seguridad de Microsoft (Windows, Defender for Endpoint, Microsoft 365 Apps, Edge, Windows 365) que puedes personalizar. Al salir una versión nueva, los perfiles antiguos quedan de solo lectura; la actualización crea una copia sin asignaciones ni etiquetas de ámbito. Varias líneas base o directivas pueden chocar y hay que revisar los valores.

Manage device updates

- Planificar actualizaciones en Intune es combinar herramientas por plataforma: en Windows, anillos de actualización y directivas de características, calidad y controladores (estas últimas no admiten dispositivos registrados en Microsoft Entra); en móviles, restricciones de inscripción, directivas de cumplimiento con versión mínima y protección de aplicaciones para avisar o bloquear. Las ventanas de mantenimiento limitan cuándo se instala.
- Los anillos de actualización controlan el comportamiento del cliente (aplazamientos, fechas límite, reinicios) y permiten pausar hasta 35 días, desinstalar o ampliar la pausa. Las directivas de actualizaciones de características fijan una versión de Windows hasta que se cambian, y las de calidad añaden orquestación, hotpatch y aceleración, que anula el aplazamiento solo de la actualización indicada.
- Windows Autopatch automatiza las actualizaciones de Windows, Microsoft 365 Apps, Edge y Teams, y sus grupos reúnen grupos de Microsoft Entra de dispositivos en anillos de implementación, con Test y Last siempre presentes. Hotpatch aplica las actualizaciones de seguridad sin reiniciar si la directiva de calidad o el valor del inquilino lo permiten; exige VBS activada y, en Arm64, deshabilitar CHPE.
- En Intune, las actualizaciones de iOS/iPadOS y macOS se configuran en el catálogo con la administración declarativa de dispositivos: Enforce Latest instala la última versión tras Delay in Days a una hora local, y la versión objetivo exige un Target OS Version antes de Target Date Time. Software Update Settings controla cómo interactúa el usuario, y el estado Success solo indica que la directiva llegó al dispositivo.
- En Android Enterprise corporativo, el perfil de restricciones de dispositivos controla las actualizaciones con System update (Device Default, Automatic, Postponed o Maintenance window) y con periodos de congelación que bloquean incluso la búsqueda manual. Para el firmware, Intune integra Samsung Knox E-FOTA y Zebra LifeGuard OTA; las implementaciones de Zebra son puntuales y no se pueden modificar una vez creadas.

4. Manage and secure applications

15–20%

Deploy and update apps

- Preparar aplicaciones para Intune empieza por elegir el tipo: las aplicaciones Win32 se convierten a .intunewin con Microsoft Win32 Content Prep Tool, que comprime toda la carpeta de origen, y deben instalarse en silencio; las LOB de Windows admiten .msi, .appx o .msix con un solo argumento. Para proteger aplicaciones LOB sin código fuente se usa App Wrapping Tool; con código, Intune App SDK.
- Las aplicaciones Win32 se empaquetan como .intunewin con Microsoft Win32 Content Prep Tool y admiten comandos de instalación, reglas de requisitos y de detección, dependencias y reemplazo; las LOB de Windows (.msi, .appx, .msix) solo aceptan un argumento de línea de comandos. Microsoft Store app (new) busca en la Store desde Intune, actualiza las aplicaciones automáticamente y exige contexto Sistema en dispositivos registrados en Microsoft Entra.
- Las directivas de tiempo de silencio (Quiet Time) silencian las notificaciones de correo de Outlook y de Teams en iOS/iPadOS y Android. Hay tres tipos: Intervalo de fechas (inicio y fin), Días de la semana (todo el día o ciertas horas, con opción de que el usuario cambie la configuración) y Tiempo no laborable, que solo afecta a Teams y exige integrar el inquilino con la API de tiempo de trabajo. Se asignan a grupos de usuarios.
- El tipo Microsoft 365 Apps (Windows 10 y posteriores) se configura con el diseñador o con datos XML (obligatorio para la edición para negocios) y descarga el conjunto desde la CDN de Office. Conviene quitar las versiones .msi de Office, porque si no la instalación falla; la versión de 32 bits sirve en equipos de 32 y 64 bits, y solo se entrega una implementación de Microsoft 365 por dispositivo.
- La directiva en la nube (Cloud Policy) aplica configuraciones de usuario de Aplicaciones Microsoft 365 aunque el dispositivo no esté administrado; solo usa objetos de usuario, gana la prioridad 0, prevalece sobre la directiva de grupo y surte efecto al reiniciar la aplicación. Para opciones de equipo, como el canal de actualización, en dispositivos inscritos se usa el catálogo de configuración de Intune.

Plan and implement app protection and app configuration policies

- Las directivas de protección de aplicaciones se dirigen a usuarios y protegen los datos en dispositivos inscritos y no inscritos; con filtros de aplicaciones administradas (app.deviceManagementType) se separan directivas para BYOD y para dispositivos administrados. En Android hace falta Company Portal, el borrado selectivo de MAM no quita la aplicación y el marco tiene tres niveles de protección.
- El acceso condicional basado en aplicaciones combina directivas de protección de aplicaciones de Intune con la concesión Requerir directiva de protección de aplicaciones, que Microsoft recomienda para directivas nuevas. El dispositivo se registra en Microsoft Entra ID mediante Authenticator en iOS o Company Portal en Android, y conviene crear la directiva en Solo informe antes de activarla.
- Las directivas de configuración de aplicaciones usan el canal MDM (dispositivos administrados) en dispositivos inscritos o el canal MAM (aplicaciones administradas) en aplicaciones con el SDK de Intune, sin importar la inscripción. En iOS, IntuneMAMAllowedAccountsOnly e IntuneMAMUPN limitan las cuentas; al actualizar una LOB de Android se necesita una directiva nueva.

5. Optimize endpoint operations by using automation, monitoring, and reporting

10–15%

Automate management tasks

- Intune se automatiza con Microsoft Graph y el SDK de Microsoft Graph PowerShell: Connect-MgGraph con -Scopes para acceso delegado o con ClientId, TenantId y certificado para acceso solo de aplicación. Leer dispositivos requiere DeviceManagementManagedDevices.Read.All, y acciones como syncDevice o wipe requieren PrivilegedOperations.All; todos los ámbitos de Intune exigen acceso de administrador.
- El agente de corrección de vulnerabilidades (Vulnerability Remediation Agent) usa datos de la Administración de vulnerabilidades de Microsoft Defender para listar y priorizar CVE de dispositivos Windows administrados, con impacto según la puntuación de exposición e instrucciones de corrección en Intune. Se ejecuta con una identidad agéntica, excluye Windows Server y no admite etiquetas de ámbito.
- Para analizar el rendimiento, Copilot en Intune genera KQL para la consulta de dispositivos a partir de lenguaje natural, compara un dispositivo sano con otro problemático y, con el complemento Windows 365, recomienda cambiar el tamaño de Cloud PC. El informe de rendimiento de recursos puntúa los picos de CPU y RAM, y Copilot respeta los roles RBAC y las etiquetas de ámbito.
- Las sugerencias del agente de corrección de vulnerabilidades se revisan en Intune: para el sistema operativo recomiendan directivas de actualizaciones de calidad y anillos de actualización, y para aplicaciones, versiones nuevas o perfiles. Mark as applied solo deja constancia con fecha; el agente no actúa en los dispositivos, no se puede pausar y quitarlo borra las sugerencias.
- El cumplimiento personalizado amplía las directivas de Intune con un script de detección (PowerShell en Windows) y un archivo JSON con reglas SettingName, Operator, DataType y Operand. El script se carga antes de crear la directiva, se ejecuta como System por defecto y debe terminar con ConvertTo-Json -Compress; el resultado cuenta para el acceso condicional.

Monitor and optimize health

- Los informes de Intune se agrupan en operativos, organizativos, históricos y de especialista, con búsqueda, filtros y exportación que conserva la búsqueda. Para datos propios, la configuración de diagnóstico envía registros como DeviceComplianceOrg a Log Analytics y libros de Azure Monitor, y la API exportJobs de Microsoft Graph exporta informes de forma asíncrona.
- El análisis de puntos de conexión recopila datos mediante Intune data collection policy y requiere el servicio DiagTrack activo. Ofrece puntuaciones de rendimiento de inicio, confiabilidad de aplicaciones y trabajo desde cualquier lugar, con líneas base propias y umbral de regresión; para actuar sobre sus conclusiones se asignan paquetes de Correcciones, como los integrados.
- Un paquete de Correcciones combina un script de detección y, opcionalmente, uno de corrección; este solo se ejecuta si la detección termina con exit 1. La programación se define al asignarlo (una vez, por hora o diaria, en hora local o UTC) y, si se exige la firma, se aplica la directiva de ejecución del dispositivo.
- La puntuación de inicio combina arranque e inicio de sesión, y la frecuencia de reinicios distingue apagados anómalos (errores de detención, botón de encendido) de normales; lo ideal es un reinicio de actualización al mes. La confiabilidad de cada aplicación se basa en el tiempo medio hasta el error y el uso total, con comparativas por versión de la aplicación y del SO.
- La página Estado del inquilino reúne los detalles del inquilino, el estado de los conectores (el peor estado resume cada tipo), el estado del servicio con las incidencias que afectan al inquilino y el centro de mensajes. Las preferencias de correo se configuran en el centro de administración de Microsoft 365, y los registros de auditoría muestran quién cambió qué.