



OB Technology M365 Audit · VERSIÓN 0.3.6

Hoja de Producto

Qué es, a quién sirve y qué entrega

Producto	OB Technology M365 Audit
Documento	Hoja de Producto
Versión	0.3.6
Fecha	2026-10-03
Destinatarios	Clientes y partners
Emite	OB Technologies (Eduardo Ortega Busutil)

OB Technologies

Eduardo Ortega Busutil · empresario individual (autónomo) · nombre comercial OB Technologies

Índice

En una frase	3
El problema	3
La propuesta	3
A quién sirve	3
Qué recibe el cliente.....	4
Lo que lo distingue	4
Los datos del cliente	4
Los tramos	4
Los dos niveles: Radar y completa.....	5
Cómo funciona, de cara al cliente	6
Cómo encaja en la suite OBT	6
Requisitos	6
Novedades de la versión 0.3.6 (octubre de 2026).....	7
Estado y madurez	7

En una frase

Revisamos el Microsoft 365 de un cliente con 58 controles repartidos en doce áreas, y le entregamos una nota de 0 a 100 con la lista de lo que hay que arreglar, por orden de importancia.

El problema

Un tenant de Microsoft 365 lleva años creciendo sin que nadie lo mire entero. Usuarios sin doble factor. Enlaces compartidos con «cualquiera» y sin caducidad. Sitios sin propietario. Aplicaciones registradas con secretos caducados. Reglas de reenvío de correo que nadie recuerda haber creado. Licencias que se pagan y no se usan.

Nada de eso avisa. Aparece el día de la auditoría del ciberseguro, de la fusión o del incidente. Una auditoría lo pone en una lista, con prioridad, antes de ese día.

La propuesta

Doce áreas, una nota y un plan.

- **Se conecta al tenant en modo lectura** y extrae la configuración: usuarios, licencias, buzones, sitios, compartición, grupos, aplicaciones, protección de datos, almacenamiento y cumplimiento.
- **La contrasta con 58 controles** y clasifica cada hallazgo por severidad.
- **Calcula una nota de salud** de 0 a 100 y un plan de acción ordenado por riesgo, coste y plazo.
- **Entrega un informe** en Excel con el detalle y un JSON que sirve de línea base para comparar la siguiente auditoría.
- **Donde Graph no llega** (versionado de bibliotecas, papelera de segunda etapa, herencia de permisos rota, reglas de transporte, políticas DLP) hay seis scripts de PowerShell que se ejecutan en una sesión con el administrador del cliente.
- **Lo que no se puede comprobar no se convierte en un hallazgo.** Si falta una licencia (por ejemplo, Entra ID P1), un permiso, o Microsoft no expone el dato, el control aparece en «Alcance no cubierto» como «no comprobado» o «no verificable», con el motivo. Nunca como un problema del cliente.

No lee el contenido de documentos ni de buzones. Solo configuración. La lista completa de permisos, con el motivo de cada uno, se entrega antes de registrar nada. Los permisos de Microsoft Graph son todos de lectura; para lo que Graph no da hay tres vías, y la que se usa por defecto pide permisos delegados con nombre de control total, limitados a la sesión del administrador del cliente. Está explicado en Permisos y registro.

A quién sirve

- **Consultora que entra en un cliente nuevo** y necesita saber en qué estado está su tenant antes de proponer nada.
- **Responsable de IT** que tiene que justificar ante dirección qué hay que arreglar y por qué.
- **Empresa que renueva el ciberseguro** o prepara una auditoría externa y necesita evidencia.

Qué recibe el cliente

Entrega	Qué es
Informe en Excel	Resumen ejecutivo con nota y semáforo, la checklist de controles, el plan de acción priorizado y el detalle de usuarios, sitios, licencias y compartición
Informe en PDF	El documento de lectura para dirección, con cada hallazgo explicado y cómo se arregla
Fichero JSON	Todos los datos en bruto. Es la línea base con la que se compara la siguiente auditoría
Sesión de lectura	Se repasa el resultado con el cliente, entre una y dos horas según el tramo

Lo que lo distingue

Baja al detalle. Secure Score da un número y recomendaciones genéricas. Esta auditoría va usuario a usuario, sitio a sitio y enlace a enlace, y ordena qué arreglar primero según riesgo, coste y plazo.

Mide la mejora. Cada ejecución deja un fichero con el estado del tenant. La siguiente lo carga y muestra cómo ha cambiado la nota, qué se resolvió y qué es nuevo. Es la prueba, ante dirección o ante el ciberseguro, de que la postura de seguridad mejora.

Llega donde Graph no llega. Los seis scripts complementarios cubren lo que una aplicación de Graph no puede leer, y se ejecutan con las credenciales del administrador del cliente, a la vista, sin dejar ningún permiso de administración concedido.

No instala nada en los servidores del cliente. Es una aplicación de escritorio que se instala en el equipo del auditor y habla con el tenant por HTTPS.

Los datos del cliente

- **La foto del tenant se guarda cifrada** en el equipo del auditor (con la clave de Windows del usuario) y **se borra sola a los 12 meses**, que es lo que dura como línea base de la renovación. Si el cliente lo pide, se borra antes.
- **Al aprobar el informe final se cierra la entrega:** se borran las credenciales de acceso a su tenant que guardaba la aplicación, los ficheros de los scripts de IT y la caché del texto de la IA. Los informes entregados se conservan los mismos 12 meses.
- **Cada borrado queda apuntado** en un registro, sin datos de la auditoría: es la base del certificado de borrado.
- **La redacción con IA es opcional.** Si se usa, el modelo recibe un resumen **pseudonimizado** (nombres de personas, sitios, dominios y correos sustituidos por marcadores) en el servicio Azure OpenAI de OBT, con un despliegue de zona de datos de la **Unión Europea**. Las cifras nunca las escribe la IA, y un consultor revisa y aprueba el texto. Sin IA, el informe sale igual con texto de plantilla.

Los tramos

El tramo lo marca el número de usuarios del tenant. Auditoría inicial de entrega única.

Tramo	Usuarios	Precio	Entrega
Nivel Radar	Cualquiera	290 €	48 horas
Starter	Hasta 25	1.290 €	48 horas
Business	De 26 a 100	2.450 €	5 días laborables
Corporate	De 101 a 350	4.200 €	10 días laborables
Enterprise	Más de 350	Desde 7.500 €	A medida

Corporate añade los scripts complementarios y la sesión con el administrador. Enterprise cubre varios tenants o regiones, entrega en inglés e integración con el centro de excelencia del cliente.

Auditoría recurrente, a partir de la segunda: cuesta la mitad, porque el registro y la línea base ya están hechos. Semestral o trimestral, esta última con un 15 % de descuento y recomendada en sectores regulados. Si pasan más de doce meses sin auditar, la siguiente vuelve a ser inicial.

Precios sin IVA. El plazo cuenta desde que la aplicación está registrada en el tenant.

Los dos niveles: Radar y completa

OBT M365 Audit es un solo producto con dos niveles de entrega. El **nivel Radar** (290 €) es la puerta de entrada, para el cliente que todavía no conoce a OBT y no va a aprobar 1.290 € sin haber visto nada. Mismo nombre, mismo título de informe, misma nota: cambia lo que se entrega.

El mensaje de venta, en una línea: el Radar responde a «¿estamos expuestos?»; la auditoría completa responde a «¿qué hacemos, en qué orden y cuánto cuesta?».

El valor añadido se enseña con el caso del cliente, no con adjetivos. La última página del Radar es una tabla «Este informe / Auditoría completa» con las cifras de ese tenant: cuántos hallazgos describe cada nivel (p. ej. «5 de 22»), cuántos controles correctos quedarían documentados como evidencia y cuántos elementos concretos (sitios, bibliotecas, permisos) lleva el detalle. Todo sale del mismo análisis.

El plan de acción va destacado debajo de la tabla, porque es lo que más distingue a la completa: se enseña su forma, no su contenido. Por ejemplo: «La auditoría completa le entrega un plan de acción con 21 acciones: 2 esta semana, 8 en las dos semanas siguientes y 11 en uno a tres meses. Cada una con su coste y su esfuerzo». Deliberadamente **no** dice cuántas son «sin inversión»: esa cifra cuenta como gratis lo que no tiene coste estimado y sale inflada (20 de 21 en un tenant de pruebas) hasta revisar los costes del catálogo.

	Nivel Radar	Auditoría completa
Precio	290 €	Desde 1.290 € (por tramos)
Extracción y análisis	Los mismos	Los mismos
Nota de salud y nota por área	Sí	Sí
Hallazgos detallados	Los cinco principales, con por qué importa, qué hacer, coste y esfuerzo	Todos
Resto de puntos abiertos	Contados por área, sin describir	Descritos uno a uno
Plan de acción	No	Completo, con coste y plazo
Excel de comprobación y anexos	No	Sí
Alcance no cubierto	Sí	Sí
Sesión de lectura	No	Sí

El Radar no es otra auditoría: es el primer nivel de la misma. La nota del Radar y la de la auditoría completa son idénticas porque salen del mismo análisis. Por eso el paso de uno a otro no exige volver a conectarse al tenant: se regenera el informe sobre la misma foto de datos.

La oferta de conversión: si el cliente amplía a la auditoría completa en los 60 días siguientes, se descuentan los 290 € del Radar. El informe le dice **el precio de su tramo**, calculado con las cuentas activas del tenant (un «desde 1.290 €» a una empresa de 300 usuarios sería engañoso); solo sin datos de cuentas (modo Solo SharePoint) dice «desde». Precios, tramos y plazo viven en `src/src/report/radar.ts` (RADAR_OFERTA, TRAMOS_AUDITORIA): si cambian en la web, se cambian ahí.

Cómo se hace:

- **Web o escritorio:** casilla «Nivel Radar» al lanzar la auditoría. En la revisión, el botón «Ampliar a auditoría completa» genera el informe completo como borrador.
- **Ficheros:** Informe_Auditoria_<cliente>_<fecha>_Radar.pdf; la referencia termina en -RAD.
- **Terminal:** `obt-audit run ... --radar`, y para convertirlo `obt-audit report --from <audit_raw.json> --edicion completa`.

Al cambiar de edición, el texto revisado y la aprobación anteriores se apartan (se renombran con la edición y la fecha): el nuevo informe nace como borrador y hay que revisarlo.

Venta a través de un aliado. Una opción hace que el Radar no enseñe precios de OBT: ni el de la auditoría completa, ni el tramo, ni el descuento. En su lugar dice «para el presupuesto y las condiciones, consulte a su proveedor». Se marca al lanzar la auditoría (casilla «Venta a través de un aliado») o con `--sin-precio`, y queda guardada en la propia auditoría: las regeneraciones la mantienen. Por defecto, el Radar enseña los precios públicos de la web.

Cómo funciona, de cara al cliente

1. **Registro.** Se da de alta una aplicación en su Entra ID. Antes de empezar recibe la lista de permisos que pide y para qué sirve cada uno.
2. **Ejecución.** La extracción tarda entre veinte minutos y unas horas según el tamaño del tenant. En Corporate se añade una sesión con su administrador para lo que exige sus credenciales.
3. **Entrega.** Recibe el informe y el Excel, y se revisan con él.

Cómo encaja en la suite OBT

Es la **fase 1, Diagnosticar**, del [ciclo de vida de Microsoft 365](#) de OBT. El diagnóstico es el primer paso, no el último:

Producto	Qué aporta después
OBT IA Crawler	La auditoría mira la configuración; el Crawler mira el contenido: qué sobra, qué está duplicado y qué es delicado
OBT Migrator	Si el plan de acción pasa por mover contenido a SharePoint, se migra solo lo que merece la pena
OBT CoE SharePoint	Para que lo arreglado no se vuelva a estropear: vigilancia diaria y nota de la A a la F

Requisitos

- Un equipo con Windows 10 u 11 con la aplicación OBT M365 Audit instalada. No hace falta instalar nada en el cliente.

- Una aplicación registrada en el Entra ID del cliente («OB M365 Audit (solo lectura)») con permisos de solo lectura de Graph.
- Para los scripts complementarios: PowerShell 7 con los módulos de PnP y Exchange Online, y una sesión con el administrador del cliente.

Novedades de la versión 0.3.6 (octubre de 2026)

- **Se actualiza sola.** Al abrirla busca la versión nueva, la descarga y la instala al cerrar. Solo acepta instaladores firmados por OBTechnologies.
- **Más segura en el equipo del auditor.** El programa solo atiende a la propia aplicación: ninguna web abierta en el navegador puede darle órdenes ni leer una auditoría.
- **Informes más claros y accesibles.** La nota sale con el mismo color en pantalla, Word y Excel; los textos tienen el contraste mínimo de accesibilidad y los logotipos llevan descripción para lectores de pantalla.
- **Más fiable en empresas grandes.** Si Microsoft 365 va saturado, cada consulta se reintenta sola, y los límites de revisión se pueden ampliar para tenants muy grandes.
- **Más rigurosa.** Lo que no se pudo comprobar, como los invitados de un grupo, aparece como «no comprobado» y nunca como correcto.

Estado y madurez

Versión 0.3.6. Usado en clientes reales. La aplicación de escritorio y el modo de terminal funcionan de punta a punta: preflight, extracción, análisis, informes y scripts complementarios. El estado actualizado de lo que está probado y lo que no está en el diario del proyecto.