

2026

EDICIÓN ESPECIAL

MICROSOFT 365 · OPTIMIZACIÓN & CIBERSEGURIDAD

# DOBLE AMENAZA, DOBLE OPORTUNIDAD.

Cómo neutralizar la subida de licencias de 2026 y blindar tu entorno con el **Baseline de Seguridad de Bullhost**.

DOCUMENTO

Dossier ejecutivo

AUDIENCIA

Dirección · IT · Finanzas

EDICIÓN

2026 · ES

PÁGINAS

9

# Hoja de ruta del dossier.

Siete capítulos que conectan el diagnóstico financiero con el blindaje técnico de tu tenant Microsoft 365.

- 
- 
- 01**    **Introducción — La falsa sensación de control en la nube**    **P. 03**  
El mito corporativo más caro: confundir suscripción con protección.
- 
- 02**    **El agujero financiero — ¿Por qué estás pagando de más?**    **P. 04**  
Tres sumideros que drenan tu presupuesto antes de la subida de 2026.
- 
- 03**    **Informe de riesgo — Las 5 vulnerabilidades críticas**    **P. 05**  
Las brechas silenciosas de un tenant "por defecto".
- 
- 04**    **El antídoto — Baseline de Seguridad Bullhost**    **P. 06**  
Qué es, qué no es, y los principios Zero Trust aplicados al tenant.
- 
- 05**    **La solución Bullhost — Optimización, blindaje y evolución**    **P. 07**  
Metodología en tres fases: FinOps, Hardening y Pulse.
- 
- 06**    **El "test del espejo" — Diagnóstico de madurez**    **P. 08**  
10 preguntas para conocer el estado real de tu Microsoft 365.
- 
- 07**    **Toma el control de tu tenant hoy mismo**    **P. 09**  
Primer paso, beneficios y contacto.
-

# La falsa sensación de control en la nube.

Existe un mito corporativo sumamente peligroso: asumir que pagar la suscripción mensual a Microsoft 365 equivale a estar automáticamente **optimizados y seguros**.

Este error no solo drena miles de euros al año en costes ocultos, sino que expone los datos más críticos de la compañía a ciberataques cada vez más sofisticados.

Por eso, en las siguientes páginas descubrirás cómo auditar tu entorno para detectar sobrecostes inmediatos, cerrar brechas de seguridad silenciosas y transformar Microsoft 365 en un ecosistema verdaderamente rentable y blindado.

## ⚡ TORMENTA PERFECTA

La subida de precios de **2026** amenaza el presupuesto IT. La escalada de ataques al **cloud** apunta directamente a las identidades de tus usuarios.

## 🔗 LA RAÍZ COMÚN

El riesgo **financiero** y el riesgo de **ciberseguridad** tienen la misma raíz: la falta de gobierno sobre el tenant de Microsoft. Una buena gestión resuelve ambos a la vez.

**01.07**   **100%**   **3+2**

Subida de tarifas Microsoft prevista para 2026.

Responsabilidad del cliente sobre identidades y accesos.

Sumideros financieros y vulnerabilidades clave revisadas en este informe.

# ¿Por qué estás pagando de más?

La subida de tarifas prevista para el **1 de julio de 2026** no es un simple ajuste de inflación: es un impacto directo a la línea de flotación de tu presupuesto tecnológico.

Sin embargo, el mayor sobrecoste no vendrá de esa subida sino de lo que **ya estás desperdiciando hoy**. Limpiar tu tenant antes de 2026 absorberá el impacto del cambio de precios y, en muchos casos, reducirá tu factura actual de Microsoft 365.

**01**

## Licencias “zombie”

El enemigo silencioso. Empleados que han dejado la compañía, cuentas genéricas olvidadas o entornos de prueba que siguen activos. Microsoft no te avisará: seguirá facturándolas mes tras mes.

**IMPACTO · ALTO****02**

## Sobredimensionamiento

Asignar licencias premium (E3 o E5) a usuarios cuya operativa se cubriría con planes más económicos (Business Basic o F3). Pagar por un Ferrari para ir a comprar el pan es un lujo inasumible.

**OVER-LICENSING****03**

## Solapamiento de software

¿Por qué pagar Zoom, Dropbox, Slack o Trello si tu licencia M365 ya incluye Teams, OneDrive, SharePoint y Planner con integración nativa? El “Shadow IT” duplica gasto a la sombra.

**SHADOW IT**

# Las 5 vulnerabilidades críticas de un tenant “por defecto”.

Según el Modelo de Responsabilidad Compartida, Microsoft protege sus centros de datos y la disponibilidad del servicio. La **configuración de acceso, las identidades y la protección del dato** son 100% responsabilidad tuya.

## RESPONSABILIDAD COMPARTIDA

Si operas con un M365 “por defecto”, te expones a cinco brechas silenciosas que detallamos a continuación.

### 01 Ausencia de MFA condicional

IDENTIDAD · PHISHING

Activar el autenticador no basta. Si no exiges un doble factor robusto basado en el **contexto** —rechazando accesos desde países no autorizados o dispositivos no corporativos— tus credenciales son vulnerables al phishing.

### 02 Protocolos heredados (Legacy Auth) abiertos

EMAIL · FUERZA BRUTA

Mantener habilitados protocolos antiguos como **IMAP o POP3** es dejar la puerta trasera abierta de par en par: son el vector número uno para ataques de fuerza bruta porque no soportan MFA.

### 03 Exceso de privilegios (Global Admins)

IDENTIDAD · TENANT

Cuantos más usuarios tengan el rol de “Administrador Global”, mayor es el riesgo de un secuestro total del tenant. **Un solo administrador comprometido** significa la pérdida de control de toda la empresa.

### 04 Descontrol en la compartición externa

SHAREPOINT · ONEDRIVE

Enlaces generados hace años que son públicos, no requieren contraseña y no tienen fecha de caducidad. Una **fuga de datos continua y silenciosa**.

### 05 Ceguera operativa (logs inactivos)

AUDITORÍA · FORENSE

La retención por defecto de los registros de auditoría es limitada. Si sufres una brecha hoy, ¿tienes los logs necesarios para saber qué descargó el atacante, desde dónde y cuándo entró? Si no, estás **ciego ante un incidente**.

# Baseline de Seguridad Bullhost.

No basta con “tener Microsoft 365”. Es necesario configurar, gobernar y operar correctamente las capacidades de seguridad, adaptándolas a la realidad de cada organización. A este enfoque lo llamamos **Baseline de Seguridad Bullhost**: configuraciones mínimas, buenas prácticas y controles que establecen un nivel de protección coherente, realista y sostenible.

## ✓ QUÉ SÍ ES

El resultado de aplicar correctamente los principios **Zero Trust** en tu tenant.

Una base coherente y sostenible para el nivel de licenciamiento y la madurez de cada organización.

Una palanca de cumplimiento que te acerca al **ENS** y al **RGPD**.

## 🔒 QUÉ NO ES

Un producto, ni una funcionalidad que se active con un solo clic.

Una garantía automática de cumplimiento normativo: depende del alcance, las licencias y el contexto.

Un proyecto puntual: requiere gobierno y revisión continua para mantenerse útil.

## PRINCIPIOS CLAVE



### Verificación estricta de identidades

MFA obligatorio, control de accesos por contexto y reducción del riesgo de phishing.



### Privilegio mínimo

Reducción drástica de cuentas con altos privilegios y control de roles administrativos.



### Superficie de ataque mínima

Bloqueo de protocolos heredados y revisión de accesos externos a datos y correo.



### Protección progresiva de la información

Cuando licencia y estrategia lo permiten, controles adicionales como clasificación de datos o DLP, dentro de un marco gobernado y asumible.

# Optimización, blindaje y evolución.

Abordar la optimización financiera y la ciberseguridad como proyectos separados es ineficiente. La magia ocurre en la intersección: al auditar y limpiar tu entorno de cuentas inactivas y herramientas duplicadas, no solo ahorras dinero, sino que **reduces drásticamente tu superficie de ataque.**

## FASE 01

**FinOps****Auditoría de  
licenciamiento**

Escaneamos tu tenant para identificar ineficiencias. Eliminamos licencias zombie, reasignamos perfiles sobredimensionados y consolidamos el Shadow IT para neutralizar la subida de precios y maximizar tu ROI.

## FASE 02

**Hardening****Activación del  
Baseline**

Cerramos las puertas traseras. Implementamos políticas de acceso condicional, reforzamos el MFA, bloqueamos protocolos heredados y establecemos alertas tempranas sin interrumpir el flujo de trabajo.

## FASE 03

**Pulse****Monitorización  
continua**

El trabajo no termina en la configuración. Pulse monitoriza la salud de tu tenant de forma continua, mide la madurez del entorno y prepara tu infraestructura para la llegada de Microsoft Copilot.

**ROI**

Limpieza de licencias, consolidación de herramientas y absorción del impacto 2026.

**RIESGO**

Cierre de brechas, gobierno de identidades y reducción de la superficie de ataque.

**EVOLUCIÓN**

Medición de madurez mes a mes y preparación para IA, Copilot y cumplimiento.

Bullhost no es un simple revendedor de licencias. No se trata de tener más tecnología, sino de gestionarla mejor. Aportamos **criterio, claridad y control** para que tu Microsoft 365 deje de ser una incógnita y pase a ser una plataforma fiable, optimizada y alineada con tu negocio.

## CAPÍTULO 06 · AUTODIAGNÓSTICO

# Diagnóstico de madurez y riesgo M365.

Responde con total sinceridad (sí o no) a las siguientes 10 preguntas sobre el estado actual de la infraestructura Microsoft 365 de tu compañía.

**01** ¿Tienes visibilidad exacta de cuántas licencias de M365 no han registrado actividad en los últimos **30 días**?

**02** ¿Tienes bloqueado a nivel de tenant el acceso desde países en los que tu empresa no tiene operaciones ni personal?

**03** ¿Tus usuarios tienen restringido el uso de protocolos de autenticación heredados (**IMAP**, **POP3**)?

**04** ¿Estás completamente seguro de que ningún empleado paga suscripciones a Zoom o Dropbox usando presupuestos departamentales?

**05** ¿Tu empresa cuenta con **menos de 3** usuarios con el rol de "Administrador Global" permanente?

**06** ¿Están configurados los enlaces de compartición externa para que caduquen automáticamente a los pocos días?

**07** ¿Exiges MFA de manera obligatoria a **todos los usuarios** sin excepción, incluidos los directivos?

**08** ¿Sabes qué porcentaje de empleados usa Teams para algo más que videollamadas (gestión de proyectos o SharePoint)?

**09** ¿Tienes políticas de **DLP** que eviten que se envíen tarjetas de crédito o DNI por correo electrónico?

**10** ¿Tienes un inventario en tiempo real de los dispositivos personales (**BYOD**) que acceden al correo corporativo?

## +2 NO

EL  
VEREDICTO

Si has respondido "NO" o "No lo sé" a más de **2 preguntas**, tu empresa está perdiendo dinero mes a mes y operando bajo un nivel de riesgo cibernético inaceptable. Tu tenant necesita una intervención urgente.

## CAPÍTULO 07 · LLAMADA A LA ACCIÓN

# Toma el control de tu tenant **hoy mismo.**

La inercia es el mayor enemigo de la rentabilidad y la seguridad en la nube. Esperar a julio de 2026 —o a sufrir un incidente— es una decisión que tu empresa no puede permitirse.

Nuestro compromiso va más allá del software: ponemos **orden real** en tu entorno cloud para reducir la incertidumbre y garantizar tu continuidad operativa.

- 01** Analizamos tu entorno y detectamos las **ineficiencias financieras** antes de la subida de 2026.
- 02** Activamos tu **Baseline de Seguridad** y cerramos las puertas traseras del tenant.
- 03** Te entregamos un **cuadro de mando vivo** con la madurez de tu Microsoft 365 mes a mes.

## VISITA

**bullhost.tech**

/servicios-m365

## ESCRÍBENOS

**hola@bullhost.tech**

Respuesta en menos de 24h

## LLÁMANOS

**+34 946 94 13 77**

Lunes a viernes, 9 — 18h

*Servicios gestionados Bullhost: Expertise Cloud y Seguridad. Protegiendo y optimizando entornos de trabajo modernos para empresas que no pueden permitirse fallar.*