MANUAL MSP PARA

TRABAJAR DE FORMA INTELIGENTE,

NO MÁS DURA

HORNETSECURITY

AMY BABINCHAK

Amy Babinchak es una profesional de IT de primer nivel, empresaria y figura influyente con más de 20 años de experiencia en el sector tecnológico. Es propietaria de varias empresas de IT, entre las que destaca Harbor Computer Services, que llegó a ocupar el puesto 40 en el ranking de los 501 mejores MSP (proveedores de servicios gestionados) de Estados Unidos, antes de vender en 2023.

En la actualidad, Amy lidera Third Tier, donde se dedica a ofrecer servicios avanzados de soporte técnico a proveedores y consultores, con un enfoque especial en las tecnologías de Microsoft.

Su experiencia técnica es ampliamente reconocida en el sector. Ha sido distinguida como Microsoft Most Valuable Professional (MVP) durante 18 años, un reconocimiento que refleja su profundo conocimiento y las importantes aportaciones que ha realizado al ecosistema de Microsoft. Sus habilidades avanzadas en el diseño, gestión e implementación de redes le han valido el reconocimiento como una de las 100 mejores profesionales de IT según MSP Mentor. Además, Amy cuenta con varias certificaciones de Microsoft, incluida la de Administración de Identidad y Acceso.

PAUL SCHNACKENBURG

Paul comenzó su trayectoria en el mundo de la tecnología en los tiempos en los que el sistema operativo DOS y los procesadores 286 representaban la vanguardia de la innovación. Actualmente, está al frente de Expert IT Solutions, una consultoría de IT que presta servicios a pequeñas empresas en Sunshine Coast, Australia. Además, trabaja como profesor de IT en una academia certificada por Microsoft.

Es un autor reconocido en el sector tecnológico y un miembro muy activo de la comunidad. Escribe artículos técnicos sobre temas como Hyper-V, System Center, entornos de nube privada e híbrida, y tecnologías de nube pública como Office 365 y Azure. Entre sus certificaciones destacan MCSE, MCSA y MCT.

HORNETSECURITY

ÍNDICE

HORNETSECURITY

CAPÍTULO 1

INTRODUCCIÓN A LA MEJORA DE LA EFICIENCIA DE LOS MSP

Este eBook tiene como objetivo ofrecer a los MSP (Proveedores de Servicios Gestionados) estrategias para operar de manera más eficiente en distintas áreas del negocio y mantenerse competitivos en un sector que no para de evolucionar. A lo largo de estas páginas, descubrirás cómo trabajan los MSP más eficaces, aprenderás a mejorar tu rentabilidad y te prepararás para anticiparte a las demandas del mercado.

Hoy en día, los MSP se enfrentan a retos y oportunidades sin precedentes. Vamos a analizar cómo algunos de los más exitosos han sabido aprovechar herramientas de automatización para optimizar sus operaciones, reducir costes y, a la vez, conservar esa relación clave con sus clientes. Este eBook te proporcionará las estrategias esenciales para triunfar en este entorno tan dinámico.

COMPRENDER CÓMO HEMOS LLEGADO HASTA AQUÍ

El modelo de negocio que conocemos como Proveedor de Servicios Gestionados (MSP) apareció en una época en la que la infraestructura tecnológica se encontraba en las oficinas de los clientes y era propiedad de estos. Los servidores estaban por todas partes, los ordenadores eran aparatos fijos en los escritorios conectados mediante cables Ethernet, y el personal de oficina rara vez trabajaba los fines de semana. El objetivo del MSP era funcionar como el departamento de IT externalizado de la empresa, ofreciendo ahorros al distribuir su tiempo entre unos pocos clientes. Los equipos de los MSP eran altamente técnicos, especializados en configuración, despliegue y resolución de problemas de infraestructura.

Por aquel entonces, la mayor parte de las operaciones eran manuales y presenciales. Las herramientas eran bastante básicas: TechNet, Wireshark y comprobadores de cables, entre otras. Las jornadas de trabajo estaban acompañadas de montañas de pizza y litros de bebidas con cafeína, especialmente durante las actualizaciones de servidores, interminables llamadas con el soporte técnico de Microsoft y reuniones con grupos de usuarios.

Y entonces llegó la nube.

La nube cambió por completo el panorama y las habilidades necesarias. En lugar de centrarse en instalar servidores y configurar redes, los MSP tuvieron que aprender a gestionar aplicaciones de manera remota. Además, la creciente demanda de servicios más variados obligó a los MSP a ampliar sus equipos y distribuir su atención entre un mayor número de clientes para mantener la rentabilidad. Esto se debió, en parte, a que algunas fuentes de ingresos pasaron de proyectos de infraestructura muy rentables a modelos de suscripción de software con márgenes más ajustados y costes operativos constantes.

Luego llegaron los ciberdelincuentes.


AUTOMATIZA.
ESTANDARIZA.
GESTIONA.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

La nube ha incrementado el riesgo de que los ciberdelincuentes accedan a los datos corporativos, lo que les ha llevado a desarrollar herramientas mucho más sofisticadas. Así nacieron las amenazas con las que lidiamos hoy, como el ransomware y el phishing. Siempre había existido un trasfondo de piratería informática, pero a partir de 2013, con la llegada del ransomware, las interrupciones en los negocios empezaron a dispararse a una velocidad alarmante.

Entonces aparecieron el sector de los ciberseguros y las normas de cumplimiento.

Cuando las empresas comenzaron a pagar rescates, el ciberdelito se disparó, y con él surgió una sopa de letras interminable de requisitos de cumplimiento específicos para cada sector. Los MSP (Proveedores de Servicios Gestionados) se encontraron en primera línea de defensa sin las habilidades ni el modelo de precios adecuado para cubrir las necesidades de los clientes. Esto les obligó a reaccionar rápidamente y adaptarse a las nuevas exigencias del mercado. La mayoría apostó fuerte por herramientas de software cada vez más avanzadas para suplir la falta de competencias y automatizar tareas repetitivas. Actualmente, los MSP destinan más del 20% de sus ingresos a estas soluciones, lo que ha acabado generando una crisis marcada por la ineficiencia.

OPERAR COMO UN MSP EFICIENTE

El cambio en la industria de los MSP fue rápido, pero el modelo de negocio no ha evolucionado al mismo ritmo. Muchos proveedores están teniendo dificultades para mantener la rentabilidad en un sector que antes era conocido por sus altos márgenes de beneficio y sus empleos bien remunerados. La buena noticia es que las empresas tienen claro que necesitan a los MSP, y estos saben que deben modernizarse si quieren seguir siendo competitivos y rentables.

En este eBook vamos a analizar varias áreas clave de las operaciones de los MSP, identificando dónde se pueden lograr mejoras y ofreciendo sugerencias para conseguirlas. Nos centraremos especialmente en Microsoft 365 y la ciberseguridad, evaluando cómo los MSP que construyen sus estrategias en torno a estos productos pueden optimizar su rendimiento. No entraremos en soluciones técnicas excesivamente específicas ni abordaremos aspectos financieros, pero sí te daremos una visión global de cómo funciona un MSP eficiente.

El objetivo es que entiendas cómo este sector puede seguir generando buenos empleos, ofreciendo servicios esenciales y resolviendo problemas técnicos que no van a desaparecer, como la ciberseguridad y el cumplimiento normativo. Los MSP desempeñan un papel crucial en el éxito de las empresas de cualquier sector y en todas las economías del mundo. Cuando un MSP triunfa, todos ganamos.

¿Estás listo para transformar tu negocio MSP y alcanzar un nuevo nivel de eficiencia? Vamos a ello, empezando por la primera tarea que cualquier MSP afronta al trabajar con un cliente nuevo: el onboarding.

HORNETSECURITY

CAPÍTULO 2

EL ONBOARDING

El onboarding a menudo se percibe como un gasto y una carga para los recursos de la empresa. Sin embargo, este capítulo tiene como objetivo cambiar tu manera de verlo, destacando las ventajas de un proceso de onboarding bien gestionado y compartiendo consejos para hacerlo más eficiente.

DOS ENFOQUES DEL ONBOARDING

Entender cómo un cliente percibe el trabajo de un proveedor de servicios gestionados (MSP) puede resultar complicado. Los clientes, que a menudo no tienen un perfil técnico, se centran en la experiencia de trabajar contigo, mientras que los MSP se suelen centrar en los resultados. Esta diferencia de perspectivas convierte el proceso del onboarding en una oportunidad clave para causar una buena impresión y conquistar a los nuevos clientes.

¿Qué dejará impresionado al cliente? ¿Qué logrará conquistarle?

QUÉ IMPRESIONARÁ	QUÉ ENCANTARÁ
Profesionalidad	Personalización
Eficiencia	Capacidad de respuesta
Experiencia	Amabilidad
Fiabilidad	Atención al detalle

Figura 1 **Impresionar y encantar a los clientes**

¿Cuáles son los objetivos en los que se centra el proveedor de servicios gestionados (MSP)?

RESULTADO DEL ONBOARDING	
Unir dispositivos al sistema de gestión	Migrar a soluciones de Microsoft 365
Asegurar los dispositivos	Minimizar el tiempo de inactividad
Implementar aplicaciones	Desplegar las herramientas del MSP
Configurar requisitos de cumplimiento	Finalizar rápidamente

Figura 2 **Resultados en los que se centran los MSPs**


Facilita el onboarding, la gestión y el cumplimiento para los tenants de M365 de manera sencilla.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

EL ONBOARDING DESDE LA PERSPECTIVA DEL CLIENTE

Cada vez es más importante que el cliente valore tus habilidades interpersonales al elegirte. Al principio, probablemente piense que puede encontrar habilidades técnicas competentes en cualquier otro lugar. Sin embargo, fue tu proceso de ventas lo que le hizo decidirse por ti. Fue tu presentación, tu página web y la manera en la que transmitiste tu propuesta de valor lo que le convenció a la hora de optar por ti en lugar de por otros MSPs que había considerado. Si metemos la pata y rompemos esa "buena impresión" durante el onboarding, la relación con el cliente podría quedar dañada para siempre. Por eso, es crucial deslumbrarles desde el primer día del proceso de onboarding.

Basándonos en los dos gráficos anteriores, estas son las áreas clave en las que el personal del MSP debería centrarse:

1. PROFESIONALIDAD:

Comunicación clara: Mantén una comunicación constante y sencilla con el cliente durante todo el proceso de onboarding. Explica cada paso de forma clara y establece expectativas realistas. Una buena comunicación ayuda a que los clientes estén tranquilos y se sientan más confiados, ya que resuelve dudas y posibles problemas antes de que surjan.

Documentación accesible: Ofrece documentación clara y fácil de entender sobre todos los procesos y procedimientos. Esto permitirá al cliente comprender lo que se está haciendo y contar con una referencia para futuras consultas.

Buena apariencia: Todas las interacciones, ya sean cara a cara o virtuales, deben ser profesionales. Esto incluye vestir de manera adecuada y mantener una actitud amable y cercana.

2. EFICIENCIA:

Procesos optimizados: Aunque los clientes no siempre comprenden los aspectos técnicos, sí notan la eficiencia (o la falta de ella). Diseña un proceso de onboarding que sea replicable y asegúrate de incorporar las lecciones aprendidas de experiencias previas para mejorar continuamente.

Automatización: Automatiza procesos, como el onboarding en Intune, para facilitar la configuración inicial, garantizar el cumplimiento normativo, mejorar la seguridad y gestionar el despliegue de aplicaciones en dispositivos Windows y otros puntos finales.

Resolución rápida: Gestiona cualquier problema o inquietud de forma rápida y eficiente para minimizar tiempos muertos y garantizar una experiencia de onboarding fluida. Comunica cada paso al cliente y haz un seguimiento posterior para confirmar que su percepción de la resolución ha sido positiva.

3. EXPERIENCIA:

Compartir conocimientos: Prepara al cliente para el proceso de onboarding organizando una breve reunión en la que expliques, de forma clara y directa, los pasos a seguir. Después, comparte tus conocimientos con el cliente mediante sesiones de formación y recursos prácticos que les ayuden a comprender y sacar partido a los servicios que les estás ofreciendo.

Resolución de problemas: Pon en práctica tu experiencia resolviendo de forma eficaz cualquier problema técnico que pueda surgir durante el proceso de onboarding. No lo dejes para más tarde; los clientes suelen interpretar cualquier anomalía como un fallo en la ejecución.

Personalización: Adapta el proceso de onboarding a las necesidades y requisitos específicos de cada cliente. Detalles sencillos, como cargar su logo, el nombre de su empresa o una imagen de fondo personalizada, muestran que estás ofreciendo una solución completamente adaptada a ellos.

4. FIABILIDAD:

Rendimiento consistente: Es posible que algunos nuevos clientes hayan tenido malas experiencias con otros MSP. Por eso, es fundamental que todas las tareas y procesos se lleven a cabo con precisión y puntualidad. Así, generarás confianza y credibilidad desde el primer momento.

Seguimiento: Una vez finalizado el proceso de onboarding, haz un seguimiento con el cliente para resolver cualquier cuestión pendiente y garantizar su satisfacción. ¿Te has dado cuenta de que falta algún detalle? Soluciónalo de inmediato.

Soporte fiable: Ofrece un soporte fiable, no sólo durante el proceso de onboarding, sino también a lo largo de toda la relación con el cliente. Asegúrate de que se sientan respaldados y valorados en todo momento.

Si tu MSP cumple con cada uno de estos aspectos, la satisfacción de los clientes será una consecuencia natural. Al centrarte en la profesionalidad, la eficiencia, la experiencia y la fiabilidad, puedes crear un proceso de onboarding que no solo cumpla con las expectativas, sino que las supere.

Cuando hagas el seguimiento para conocer la opinión del cliente sobre su experiencia, deberías escuchar comentarios como amable, profesional, experto y conocedor. Es entonces cuando sabrás que has hecho un gran trabajo consolidando la relación con el cliente y ofreciendo una experiencia excepcional.

EL ONBOARDING DESDE LA PERSPECTIVA DEL MSP

Aunque sabemos qué considera el cliente como una experiencia de onboarding exitosa, es fundamental entender que, desde la perspectiva del MSP, gran parte del trabajo ocurre tras bambalinas para asegurar ese éxito.

En la **figura 2**, puede que te preguntes por qué "terminar rápido" está en la lista. Finalizar rápidamente es clave para mantener al cliente satisfecho, ya que asegura que la migración a tus servicios no se alargue ni interfiera en su negocio. Desde la perspectiva del MSP, terminar rápido significa dedicar únicamente las horas de trabajo necesarias al proyecto, optimizando así los recursos y la eficiencia.

EFICIENCIA EN EL ONBOARDING DE CLIENTES

El primer paso para mejorar la eficiencia en el onboarding de nuevos clientes es diseñar un proceso claro de recopilación de información. Por ejemplo, el MSP necesita obtener datos como licencias existentes, contraseñas de administrador, detalles sobre la transición de MFA (autenticación multifactor) y consolidar toda esa información en su sistema. En la práctica, gran parte de estos datos no estarán disponibles por parte del cliente ni del MSP anterior. En ese caso, será necesario contar con un método fiable para reunir esta información rápidamente.

La eficiencia en el onboarding se consigue gracias a la repetición y la automatización. Estos dos elementos no solo permiten que el MSP sea rentable, sino que también impresionan a los clientes con profesionalidad y una actitud impecable. Con una cuenta de partner de Microsoft, al adquirir Action Pack o planes superiores, tienes acceso a un tenant de demostración. Estos tenants son ideales para configurar tus ajustes estándar.

Sin embargo, un inconveniente de usar únicamente un tenant de demostración para configurar los ajustes es que no experimentas cómo funcionan esas configuraciones en un entorno real. Por ello, podrías considerar usar tu tenant de producción como un "canary ring". Es una práctica recomendada que el MSP viva con el nivel de seguridad más alto de su tenant y lo adopte como estándar de calidad. Este enfoque, conocido cariñosamente en la industria como dogfooding, implica probar primero las configuraciones en un grupo reducido de clientes con mayor tolerancia al cambio antes de un despliegue más amplio.

Siguiendo este proceso, cometerás menos errores y darás tiempo a tu equipo de marketing para preparar los mensajes sobre los nuevos ajustes, mientras el equipo de soporte ajusta sus procedimientos.

Facilita el onboarding, la gestión y el cumplimiento para los tenants de M365 de manera sencilla.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

COMPLETANDO NUESTRAS TAREAS

Para lograr la eficiencia en el onboarding, debes realizar estas cuatro tareas.

Figura 3 Tareas en el onboarding

Tus clientes podrán incorporarse de forma sencilla a un portal "todo en uno" gracias al **365 Multi-Tenant Manager para MSPs** de Hornetsecurity. Con esta herramienta, tienes la opción de seleccionar a todos tus clientes desde el portal de partners de Microsoft o elegir solo a algunos, tal y como se muestra en la **figura 1**.

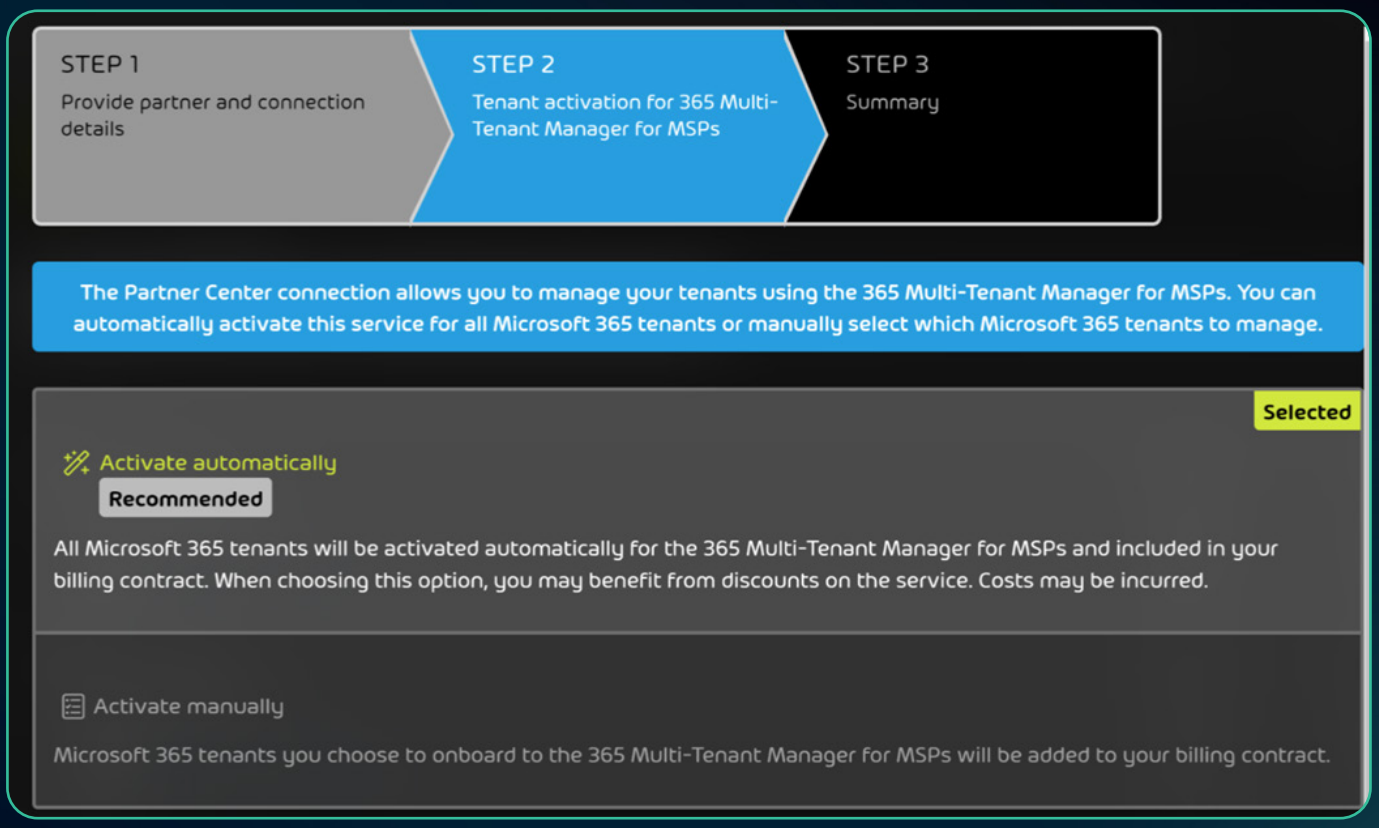


Figura 4 Usa el asistente para incorporar rápidamente a los tenants en el portal de administración

Una vez que tengas a tus tenants organizados, Microsoft ofrece varias herramientas para facilitar el onboarding de dispositivos, cada una diseñada para distintos escenarios de clientes:

- **Windows Autopilot** es perfecto para automatizar el registro y la configuración de dispositivos. Simplifica el proceso de unión a Microsoft Entra durante la Experiencia Fuera de la Caja (OOBE) de Windows, lo que permite desplegar dispositivos nuevos sin intervención manual.
- **Registro Masivo** está pensado para dispositivos ya existentes o en casos donde Autopilot no se pueda aplicar.
- **Registro en la Gestión de Dispositivos (MDM)** con Intune posibilita que los dispositivos se registren automáticamente en MDM al unirse a Microsoft Entra, lo que activa la gestión en cuanto se integran a tu organización.
- **Registro de Autoservicio** resulta útil para escenarios de dispositivos propios (BYOD). Los usuarios pueden añadir sus propios dispositivos desde la configuración de Windows o durante el OOBE.
- **PowerShell y Tareas** Programadas son una opción para dispositivos ya vinculados a Entra AD que necesitan registrarse en Intune. Se puede ejecutar un script de PowerShell que active deviceenroller.exe con los parámetros adecuados o configurar una tarea programada en el sistema que ejecute dicho script.

Después de incorporar los dispositivos mediante cualquiera de estos métodos, estarán listos para configurarse con Intune. Intune es tu herramienta clave para aplicar configuraciones de dispositivos y políticas de cumplimiento. Microsoft proporciona plantillas y bases de seguridad para ayudarte a definir tus estándares.

Un aspecto fundamental para trabajar con eficiencia es contar con un estándar documentado que incluya listas de verificación y procedimientos operativos estándar (SOPs). Así, todo tu equipo puede repetir el proceso de onboarding de nuevos clientes de forma consistente. Microsoft 365 no incluye ninguna herramienta automatizada para este propósito; en su lugar, puedes optar por herramientas del sector o algo tan sencillo como OneNote.

El siguiente paso para mejorar el onboarding de clientes es estandarizar la configuración del portal y los controles de seguridad. Estas tareas forman parte del proceso de onboarding y deben mantenerse en el tiempo. Microsoft proporciona herramientas útiles para la configuración inicial, como las líneas base de seguridad y la herramienta Desired State Configuration (DSC). No obstante, ambas tienen limitaciones. Las líneas base de seguridad suelen ser muy estrictas, lo que puede dificultar el trabajo diario de muchos usuarios. Tendrás que probarlas con cada cliente antes de implementarlas y adoptar las actualizaciones que Microsoft vaya publicando.

Una vez definido tu estándar, puedes crear una "imagen dorada" con la herramienta DSC. Esto te permitirá replicar esa configuración en otros tenants con los mismos ajustes. En la práctica, muchos proveedores de servicios gestionados (MSPs) consideran estas herramientas complicadas de usar. Por eso, pueden resultar más útiles soluciones de terceros, como el **365 Multi-Tenant Manager de Hornetsecurity para MSPs**. Esta herramienta te permite guardar una "imagen dorada" personalizada y usar tu propio conjunto de configuraciones para implementarlas en nuevos clientes de forma más sencilla durante el onboarding.

RESUMEN

En definitiva, lograr un onboarding eficiente de nuevos clientes es clave para mantener la rentabilidad y causar una buena impresión, destacando tanto por profesionalidad como por un trato impecable. Utilizando herramientas como Intune para configurar dispositivos y establecer ajustes de cumplimiento, junto con plantillas y directrices de seguridad de Microsoft, los proveedores de servicios gestionados (MSP) pueden desarrollar un proceso de onboarding estandarizado y replicable. No obstante, es imprescindible contar con estándares bien documentados, listas de verificación y procedimientos operativos claros (SOP) para garantizar la consistencia entre todos los miembros del equipo.

Estandarizar la configuración del portal y los controles de seguridad durante el proceso de onboarding, así como mantener esos estándares a lo largo del tiempo, resulta fundamental. Aunque Microsoft ofrece herramientas como guías de seguridad y la utilidad Desired State Configuration, los MSP podrían optar por soluciones de terceros, como el **365 Multi-Tenant Manager** de Hornetsecurity, que a menudo resultan más sencillas y eficaces para crear y desplegar "imágenes doradas" personalizadas. Estas soluciones, como se verá en capítulos posteriores, también son útiles para mantener y actualizar la postura de seguridad de la red.

Al priorizar la automatización, la estandarización y una documentación exhaustiva, los MSP pueden agilizar el proceso de onboarding, reducir los tiempos de inactividad y garantizar una transición sin contratiempos para los nuevos clientes. Este enfoque no solo mejora la eficiencia, sino que también refuerza la confianza y la seguridad en los servicios ofrecidos, logrando así una experiencia de onboarding satisfactoria y exitosa para los clientes.


Facilita el onboarding, la gestión y el cumplimiento para los tenants de M365 de manera sencilla.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

HORNETSECURITY

CAPÍTULO 3

SUPERVISIÓN Y MANTENIMIENTO

El núcleo del negocio de los proveedores de servicios gestionados (MSP) siempre ha sido la supervisión y el mantenimiento. El mantenimiento permite trabajar de forma proactiva, mientras que la supervisión automatizada nos mantiene al tanto de los cambios y amenazas. Con el aumento de las exigencias en ciberseguridad y cumplimiento normativo, estas tareas nunca han sido tan cruciales. Tampoco han requerido tanta concentración como ahora.

Lograr eficiencia en la supervisión y el mantenimiento no es tarea sencilla. Es tentador pensar que deberíamos automatizarlo todo, pero la realidad es que sigue siendo imprescindible el conocimiento y la capacidad de análisis humanos. Además, hay que considerar qué hacemos cuando la supervisión detecta un problema grave. Encontrar el equilibrio entre la necesidad de eficiencia y la intervención humana en la respuesta es el reto donde un MSP debe identificar el punto justo de rentabilidad. En cierto modo, nuestros trabajos son hoy más exigentes y complejos que nunca, lo que genera bastante estrés tanto para los propietarios de MSP como para sus equipos. Tener procedimientos y planes bien definidos es clave para mantener la eficiencia y gestionar la carga de trabajo de forma efectiva.

MANTENIMIENTO PROACTIVO

El mantenimiento proactivo es esencial para anticiparse a los problemas antes de que se conviertan en críticos. El software tradicional de monitorización y mantenimiento remoto (RMM) disponible en el mercado arrastra una notable deuda técnica. Su enfoque principal sigue siendo gestionar actualizaciones de software y detectar fallos a nivel de hardware. Aunque estas funciones siguen teniendo importancia, hoy en día han perdido algo de relevancia. Las actualizaciones de los sistemas operativos son ahora más seguras, y los usuarios han adquirido un mayor nivel de conocimiento. Muchas actualizaciones pueden programarse para instalarse automáticamente en el sistema operativo y las aplicaciones, lo que simplifica bastante el proceso.

Backblaze SSD Lifetime Annualized Failure Rates

Reporting period: 10/1/2018 to 06/30/2023 inclusive for active drive models as of 06/30/2023

MFG	Model	Size (GB)	Drive Count	Drive Days	Drive Failures	AFR	Confidence Interval	
Crucial	CT250MX500SSD1	250	598	205,743	9	1.60%	0.9%	3.3%
Dell	DELLBOSS VD	500	411	304,937	0	0.00%	0.0%	0.4%
Micron	MTFDDAV240TCB	250	88	83,259	9	3.95%	1.8%	7.5%
Seagate	SSDSCKKB240GZR	250	1	133	1	274.44%	0.0%	1012.4%
Seagate	ZA250CM10003	250	1,114	924,856	14	0.55%	0.3%	0.9%
Seagate	ZA500CM10003	500	3	1,125	0	0.00%	0.0%	119.7%
Seagate	ZA2000CM10002	2,000	3	5,538	1	6.59%	0.2%	36.7%
Seagate	ZA250CM10002	250	547	667,680	17	0.93%	0.5%	1.5%
Seagate	ZA500CM10002	500	18	29,739	0	0.00%	0.0%	4.5%
Seagate	ZA500GM10001	500	2	682	0	0.00%	0.0%	197.4%
Seagate	ZA250NM1002	250	80	15,523	0	0.00%	0.0%	8.7%
Seagate	SSD	250	106	151,465	3	0.72%	0.1%	2.1%
WDC	WD Blue SA510 2.5	250	65	3,716	4	39.29%	10.7%	100.6%
WDC	WDS250G2B0A	250	108	38,914	2	1.88%	0.6%	8.2%
		Totals	**3,144**	**2,433,310**	**60**	**0.90%**		

Backblaze

Figura 5 https://www.backblaze.com/blog/how-reliable-are-ssds/

Por otra parte, los fallos de hardware son cada vez menos comunes. La industria ha evolucionado hacia componentes más integrados y resistentes, alejándose de piezas intercambiables y de aquellos que requerían sistemas de refrigeración más complejos. Un estudio de Backblaze realizado durante cinco años con miles de unidades SSD mostró una tasa de fallos inferior al 1%, lo que refleja esta mejora.

La tendencia hacia los portátiles también ha tenido un papel importante. Durante un tiempo, renovar el hardware cada 3 o 4 años era la norma, pero hoy en día muchos proveedores de servicios gestionados (MSP) se dan cuenta de que equipos con 4, 5 e incluso 6 años de antigüedad siguen funcionando sin problemas.

¿Qué implica esto para el mantenimiento? Básicamente, significa que deberías enfocarte en automatizar todo lo que puedas y centrarte únicamente en las excepciones durante los despliegues. Las tareas de mantenimiento deberían disminuir, ya que el hardware actual es mucho más fiable.

SUPERVISIÓN AUTOMATIZADA

Aunque el tiempo necesario para el mantenimiento ha bajado, el dedicado a la supervisión ha aumentado, incluso con el apoyo de la automatización. Las alertas por problemas clásicos, como discos duros llenos, han disminuido gracias al uso del almacenamiento en la nube. Sin embargo, han aumentado las alertas relacionadas con phishing, gestión de identidades y aplicaciones. Esto ocurre porque la supervisión automatizada desempeña un papel esencial en la detección de posibles amenazas, abarcando tanto la continuidad del negocio como la ciberseguridad. Los proveedores de servicios gestionados necesitan soluciones de supervisión robustas e inteligentes para no quedarse atrás ante la avalancha de información que se genera constantemente, desde registros y cambios de configuración hasta indicadores de actividad maliciosa. Un buen programa de supervisión es la columna vertebral de cualquier plan eficaz de detección de amenazas.

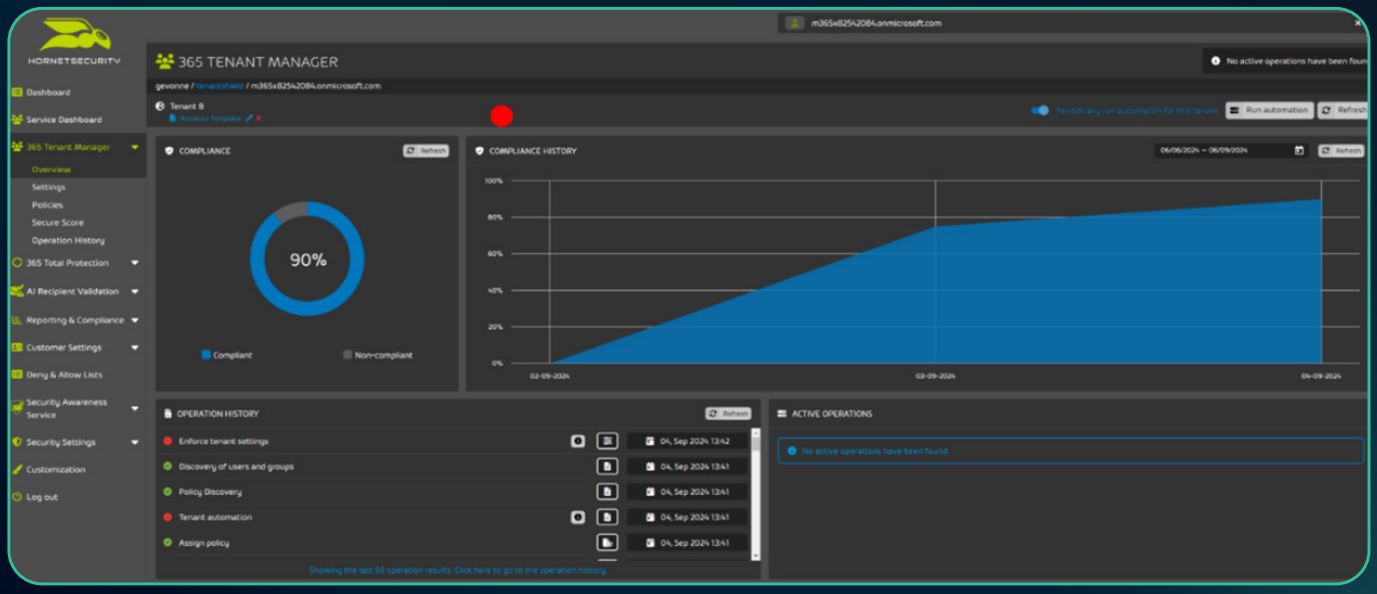


Figura 6 Vista general del tenant en Multi-Tenant Manager

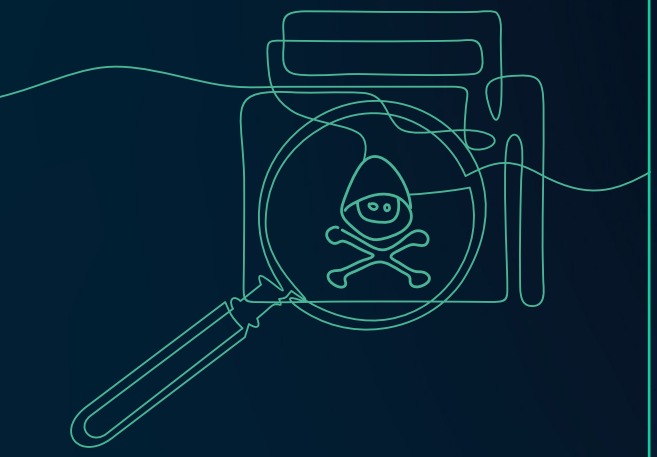
Un sistema de supervisión automatizado debe ser lo suficientemente inteligente como para identificar la gravedad tanto de un cambio aislado como de varios cambios en conjunto. La combinación de herramientas integradas de Microsoft, como Intune para supervisar dispositivos, Sentinel para gestionar alertas y Defender XDR para el seguimiento de incidentes, funciona de manera conjunta para ofrecer una solución inteligente. Este tipo de sistema puede tomar medidas automáticas, mapear actividad y enviar notificaciones cuando sea necesario. Por otro lado, soluciones de terceros como el **365 Multi-Tenant Manager de Hornetsecurity para MSPs**, junto con planes de protección empresarial, aprovechan la inteligencia artificial para ofrecer información y seguridad automatizada basada en la supervisión. Sea cual sea la herramienta que elijas, es fundamental que sea un conjunto integral capaz de trabajar en equipo, no solo para supervisar, sino también para actuar en tu lugar cuando las condiciones lo requieran.

RESPUESTA ANTE INCIDENTES Y RECUPERACIÓN ANTE DESASTRES

La complejidad de gestionar incidentes y recuperarse de desastres nunca ha sido tan grande. Con el aumento de las demandas de rescate por parte de ciberdelincuentes, las aseguradoras y los organismos reguladores han pasado a desempeñar un papel mucho más relevante en el proceso de recuperación. Esto implica que hoy no solo hay que lidiar con el componente técnico, sino también con requisitos de cumplimiento normativo y condiciones de seguros que deben integrarse en los planes de respuesta a incidentes y recuperación.

Mientras que muchos seguros cibernéticos emplean términos vagos como "tan pronto como sea posible" o "con prontitud", otros especifican plazos concretos, como 72 horas. La mayoría de los MSP quieren entrar directamente en modo recuperación para que la empresa retome su actividad lo antes posible. Sin embargo, los seguros cibernéticos suelen imponer requisitos que limitan las acciones inmediatas a una mera contención inicial. De hecho, el primer paso suele ser ponerse en contacto con la aseguradora para que sus expertos puedan intervenir en el proceso de recuperación. Por otro lado, las normativas de cumplimiento también suelen incluir requisitos específicos de notificación. Como si esto no fuera suficiente, muchas empresas siguen sin invertir lo necesario en prevención y planificación de recuperación. Las amenazas cibernéticas han hecho que el trabajo de los MSP sea cada vez más complicado y exigente.


Administra y supervisa tus tenants de M365 desde un único portal.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS



Un cliente mío, una pequeña PYME, sufrió una brecha de seguridad y, de manera apresurada, decidieron volver a poner en marcha los portátiles de los empleados reinstalando el sistema operativo sin más. Esto fue en contra de nuestra recomendación de dedicar el tiempo necesario para analizar cómo se produjo el acceso y qué datos se habían comprometido. Unos días después, los atacantes volvieron y desplegaron un nuevo ataque de ransomware. No fue hasta que esto se repitió por tercera vez cuando el cliente aceptó que trajéramos expertos en Respuesta a Incidentes de Informática Forense (DFIR). La investigación reveló la presencia de un rootkit implantado en el UEFI, que permitía a los atacantes mantener una puerta trasera incluso después de reinstalar los sistemas. La única solución fue reemplazar todos los equipos afectados por otros nuevos.

RECUPERACIÓN ANTE DESASTRES

Hoy en día, muchas personas, lamentablemente, han dejado de prestar atención a lo esencial: las copias de seguridad, ese recurso al que recurrir "por si todo falla". ¡Es como si se olvidaran de la recuperación del negocio en cuanto almacenan los datos en la nube! Pero ojo, la copia de seguridad nunca ha sido una función integrada. Siempre ha sido necesario complementarla con soluciones de un proveedor externo. Aunque la mayoría de los proveedores de servicios en la nube presumen de tener su propia función de copia de seguridad, esta está diseñada para protegerles a ellos mismos, no a ti como cliente ni al proveedor de servicios gestionados (MSP). Si sufren algún fallo, ellos pueden restaurar su servicio y tus datos, pero si buscas un verdadero plan de recuperación ante desastres, necesitas una solución de terceros que garantice una copia de seguridad completa y eficiente. Ahí es donde entra en juego Hornetsecurity con su **solución 365 Total Backup**. No solo protege los datos almacenados en Microsoft 365, sino que también incluye un componente de monitorización integral y la copia de seguridad de endpoints (dispositivos finales).

» **Multitenencia**
Gestiona y monitoriza todas las organizaciones de Microsoft 365 y las copias de seguridad de endpoints de Windows desde una consola centralizada y multitenente.

» **Panel de control intuitivo**
Supervisa de forma centralizada las actividades de copia de seguridad y restauración, el estado de las copias y el historial reciente. Configura notificaciones para estados exitosos, fallos o advertencias, además de alertas por correo electrónico o un resumen diario.

» **Copias de seguridad automáticas de Microsoft 365**
Las copias se realizan de forma automática varias veces al día. Para los endpoints, puedes programarlas con una frecuencia que va desde cada hora hasta una vez al día.

» **Copia de seguridad de endpoints locales y remotos**
Realiza copias de seguridad de dispositivos, estén en la oficina o en cualquier parte del mundo, sin necesidad de usar una VPN.

» **Políticas de copia de seguridad para endpoints**
Gestiona copias basadas en políticas específicas para ordenadores de sobremesa y portátiles con Windows. Configura fácilmente directorios, almacenamiento en la nube, frecuencia y retención para grandes grupos de dispositivos.

» **Respaldo en cualquier momento y lugar**
Haz copias de seguridad de usuarios específicos, grupos, MS Planner, bibliotecas de documentos de SharePoint y endpoints cuando lo necesites.

» **Proceso de aprobación con cuatro ojos**
Añade una capa adicional de seguridad para prevenir pérdidas de datos por errores o malas prácticas de los administradores. Cualquier acción sensible, como eliminar datos o modificar configuraciones, requiere la aprobación de un segundo administrador autorizado.

En el panorama actual de creciente cibercrimen, soluciones de este tipo, completas y enfocadas en la recuperación ante desastres, son imprescindibles. La probabilidad de necesitar restaurar datos se ha disparado en los últimos años, al mismo ritmo que aumentan los ataques cibernéticos.

RESPUESTA ANTE INCIDENTES

Aunque nos encantaría volver a los tiempos en los que restaurar desde una copia de seguridad era suficiente para gestionar un incidente, hoy en día eso ya no es viable. La complejidad de los sistemas actuales ha crecido tanto que los proveedores de servicios gestionados (MSP) necesitan un proceso claro y bien estructurado para abordar la respuesta ante incidentes. Aquí tienes una lista de las 6 áreas clave que forman parte de la respuesta ante incidentes en la actualidad. Es importante destacar que la recuperación ocupa el quinto lugar en esta jerarquía.

1. **Contención:** El primer paso es contener el incidente para evitar que cause más daños. Esto puede implicar aislar los sistemas afectados, desactivar cuentas comprometidas y detener procesos maliciosos. Idealmente, tu herramienta de monitorización debería haberte alertado sobre la amenaza, mientras que la solución de ciberseguridad que hayas implementado habría empezado a bloquear la cadena de ataque.

2. **Notificación:** El siguiente paso es notificar a cualquier organismo regulador que deba estar al tanto del incidente. Para las empresas más pequeñas, suele tratarse de la compañía de seguros de ciberseguridad; en el caso de entidades reguladas o públicas, será el departamento legal quien deba ser informado. Este equipo probablemente involucrará a expertos para coordinar el proceso de recuperación.

3. **Investigación:** En esta fase, los expertos llevan a cabo una investigación detallada para determinar la causa y el alcance de la brecha. Esto incluye analizar logs, identificar sistemas comprometidos y recopilar evidencias. El MSP puede jugar un papel crucial como asesor, aportando información al equipo de recuperación. Gracias a su conocimiento del negocio y de las personas clave dentro de la empresa, el MSP está en una posición privilegiada para cerrar cualquier brecha de comunicación y gestionar las expectativas.

4. **Erradicación:** Una vez contenida la amenaza, el MSP puede ser responsable de eliminar la causa del incidente. Esto podría incluir eliminar malware, cerrar vulnerabilidades y restablecer contraseñas comprometidas.

5. **Recuperación:** Si la red ha sufrido daños o hay áreas que no son seguras, el MSP deberá restaurar los sistemas y datos afectados utilizando copias de seguridad. También deberá asegurarse de que todos los sistemas vuelvan a estar plenamente operativos y sean seguros.

6. **Revisión post-incidente:** Finalmente, el MSP y cualquier otro equipo involucrado deben realizar una revisión del incidente. Esto implica elaborar un informe que documente lo ocurrido, identificar lecciones aprendidas y actualizar el plan de respuesta ante incidentes para mejorar futuras respuestas.

En este proceso, tanto la empresa como el MSP pueden aprender valiosas lecciones que fortalecerán la seguridad de la red a largo plazo. Es crucial recordar que el cliente a menudo no entiende los aspectos técnicos del incidente. Para él, se trata de una interrupción de su negocio, y buscará en el MSP no solo una solución técnica, sino también tranquilidad y explicaciones claras sobre las medidas adoptadas en cada fase. Este tipo de situaciones suelen ser momentos de gran estrés, tanto para el cliente como para el MSP. Una buena comunicación es fundamental para gestionar expectativas y evitar posibles malentendidos o descontentos.

Cuando el MSP lleva a cabo con éxito el plan de recuperación, la relación con el cliente no solo se recupera, sino que puede salir más fortalecida que nunca.


Administra y supervisa tus tenants de M365 desde un único portal.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

EQUILIBRAR LA EFICIENCIA Y LA EXPERIENCIA HUMANA

Gestionar todas estas actividades puede llevar mucho tiempo, pero por suerte, el aprendizaje automático y la inteligencia artificial están aquí para echarnos una mano. Con un conjunto de soluciones modernas que incluya automatización e IA, los MSP pueden aligerar la carga de trabajo de su personal de soporte técnico. Esto les permitirá afrontar situaciones de recuperación ante desastres sin descuidar las tareas diarias de despliegue, supervisión y generación de alertas. Encontrar el equilibrio ideal entre eficiencia y la experiencia humana es fundamental para un mantenimiento y monitoreo exitosos.

Muchos MSP han optado por contratar empleados con menos cualificación, mientras que los desarrolladores han trabajado en herramientas diseñadas para reducir su carga de trabajo. Estas herramientas, pensadas para simplificar las operaciones del día a día, hacen que ahora los MSP necesiten incorporar perfiles más especializados. Este personal cualificado debe contar con habilidades en gestión de la continuidad del negocio, ciberseguridad y recuperación ante desastres, además de entender bien la motivación empresarial y saber gestionar las comunicaciones. Por supuesto, sigue siendo necesario el personal con menor cualificación, pero su papel estará más orientado al manejo de herramientas y al servicio directo al cliente.

De hecho, este personal menos cualificado es el que suele interactuar más con los clientes. Son quienes responden al teléfono, hacen el triaje de los problemas y prestan la asistencia inicial de nivel uno. Por ello, es crucial prestar atención a estos puntos de contacto, ya que gran parte de la percepción del cliente sobre el servicio del MSP dependerá de cómo se sientan atendidos, especialmente en momentos de tensión.

RESUMEN

> En este capítulo hemos abordado los elementos clave para optimizar la eficiencia de los Proveedores de Servicios Gestionados (MSP) en tareas de monitorización y mantenimiento. Hemos analizado la importancia del mantenimiento proactivo, el impacto de la monitorización automatizada, la relevancia de los procedimientos de respuesta ante incidentes y la planificación para la recuperación ante desastres. También hemos destacado la necesidad de combinar la eficiencia con la experiencia humana. Implementando planes y procedimientos eficaces, los MSP pueden mejorar su rendimiento, reducir el estrés y alcanzar una mayor rentabilidad.


Administra y supervisa tus tenants de M365 desde un único portal.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

HORNETSECURITY

CAPÍTULO 4

PERSONALIZACIÓN

La personalización es un tema complejo. Aunque como MSP necesitamos estandarizar nuestros procesos, también es fundamental reconocer que cada cliente tiene necesidades específicas. Debemos evitar caer en la tentación de ofrecer soluciones genéricas que cualquier competidor podría replicar. La personalización es clave para diferenciarnos en el mercado.

La dificultad de la personalización radica en sus múltiples motivaciones, pero aquí nuestro objetivo es claro: personalizar de manera eficiente y centrándonos en aquellas áreas que realmente generan impacto. En este capítulo, trazaremos una línea entre lo que significa personalizar y lo que implica un despliegue personalizado, reflexionando sobre cuándo y por qué conviene llevar a cabo cada enfoque.

¿QUÉ ES LA PERSONALIZACIÓN?

Puede parecer una pregunta trivial, pero es fundamental comprenderla. ¿En qué se diferencia un despliegue personalizado de una personalización? Saberlo nos ayuda a mantener el foco en nuestro objetivo: operar de forma eficiente sin perder flexibilidad.

UNA SOLUCIÓN PARA IMPLEMENTAR UNA CONFIGURACIÓN PERSONALIZADA

Con el 365 Multi-Tenant Manager para MSPs de Hornetsecurity, podemos crear configuraciones personalizadas de forma ágil, basándonos en nuestros Procedimientos Operativos Estándar (SOP). Esta herramienta nos permite desplegar la configuración completa de un cliente en cuestión de minutos, asegurando que nuestras configuraciones se apliquen de inmediato a todos los clientes que gestionamos. Para cualquier MSP, contar con un despliegue personalizado que refleje sus estándares es esencial, siempre teniendo en cuenta las recomendaciones clave del sector.

A continuación, mostramos un ejemplo práctico de cómo hacerlo. Cada cliente de nuestra lista recibe una plantilla que representa nuestra configuración estándar para un perfil similar.

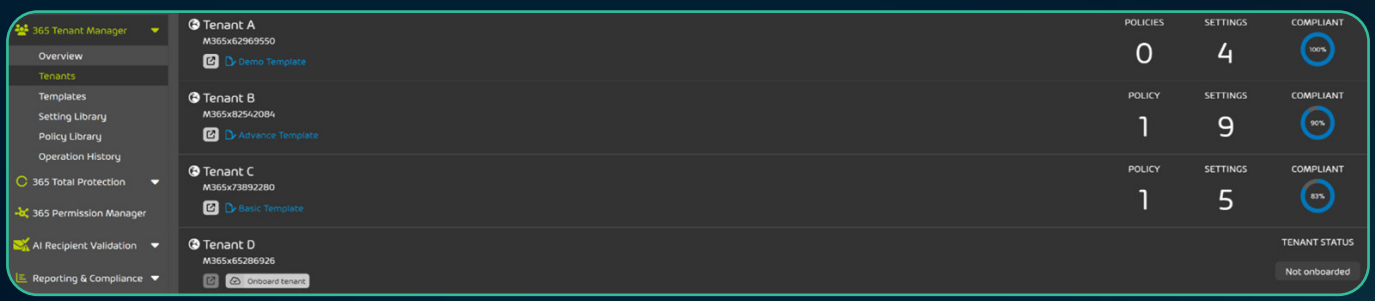


Figura 7 Multi-Tenant Manager de Hornetsecurity

Gracias al uso de plantillas, podemos mantener un alto nivel de personalización agrupando a los clientes según la plantilla que mejor se ajuste a sus necesidades. Al realizar modificaciones en una plantilla, los clientes asociados a ella se actualizan automáticamente. Este método nos permite desplegar configuraciones personalizadas de manera eficiente y efectiva, optimizando tanto tiempo como recursos.

DESPLEGAR PERSONALIZACIÓN DE FORMA EFICIENTE

La personalización es un paso fundamental que no podemos pasar por alto. En cada tenant de Microsoft 365 hay áreas que permiten realizar ajustes personalizados para que el cliente sepa que está operando dentro de su propia red, cumpliendo con las normativas y trabajando de forma segura. Es un poco como cuando antes instalabas un servidor de Microsoft y aplicabas tus propias configuraciones. Esa implementación personalizada y la presencia física del servidor eran lo que hacía que el cliente tuviera claro que era suyo. Ahora, esa presencia física se ha sustituido por la personalización.

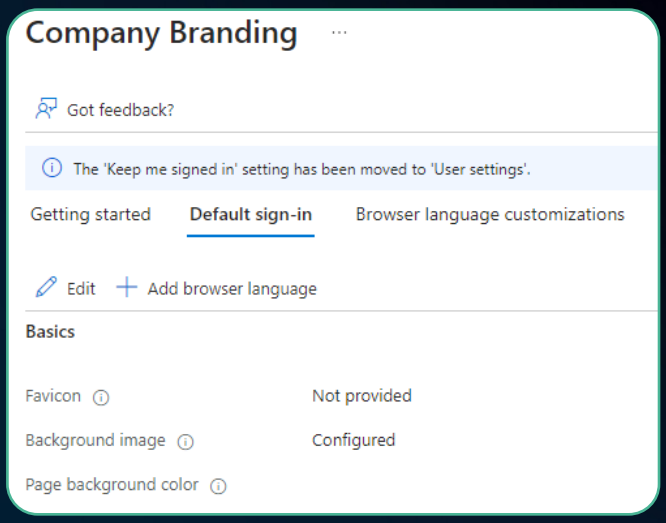


Figura 8 Personalización con imagen de fondo aprobada por la empresa en la pantalla de inicio de sesión

Aunque ya no tengamos un servidor físico, en una implementación de Microsoft 365 la personalización puede incluir detalles como el logotipo corporativo, el nombre de la empresa, el del proveedor de servicios gestionados (MSP) o la información de contacto. También se puede añadir una imagen de fondo en la pantalla de inicio de sesión. Estos elementos ayudan a los usuarios a reconocer fácilmente cuándo están trabajando dentro de su red corporativa. Además, para el MSP supone un valor añadido frente a quienes no se molestan en implementar estas personalizaciones.

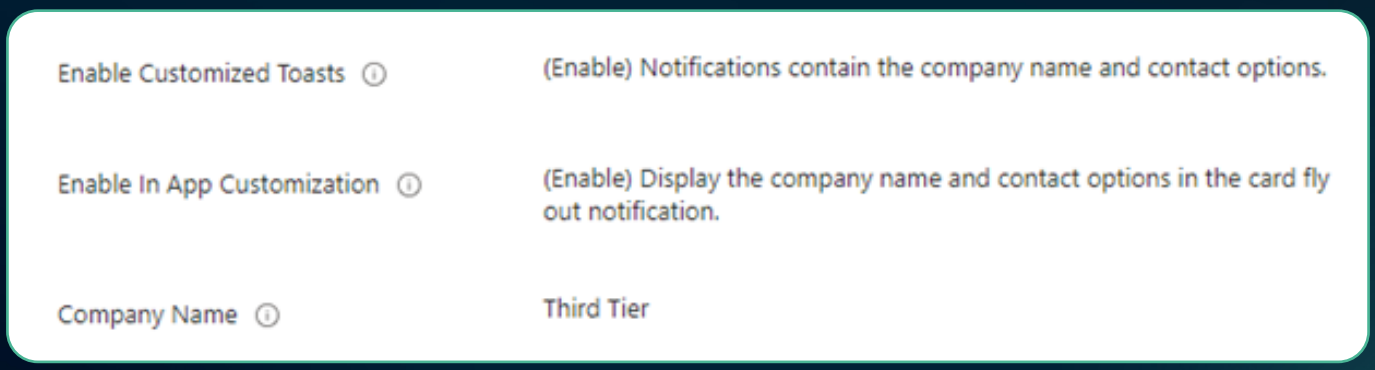


Figure 9 Personalización de pop-ups del sistema con el nombre de la empresa y la información de contacto

La personalización también puede incluir configuraciones estándar que sean útiles para varios clientes. Por ejemplo, puede que tengas clientes que procesan pagos con tarjeta de crédito y almacenan datos relacionados.

En este caso, todos necesitarán cumplir con la normativa PCI. Con la herramienta 365 Multi-Tenant Manager para MSPs de Hornetsecurity, puedes aplicar automáticamente esa política al tenant correspondiente cuando sea necesario. Igual que hemos hablado de crear plantillas para cada tipo de negocio, lo mismo hacemos con el cumplimiento normativo y las regulaciones que necesitan nuestros clientes, aplicando nuestras plantillas de configuración de forma eficiente.

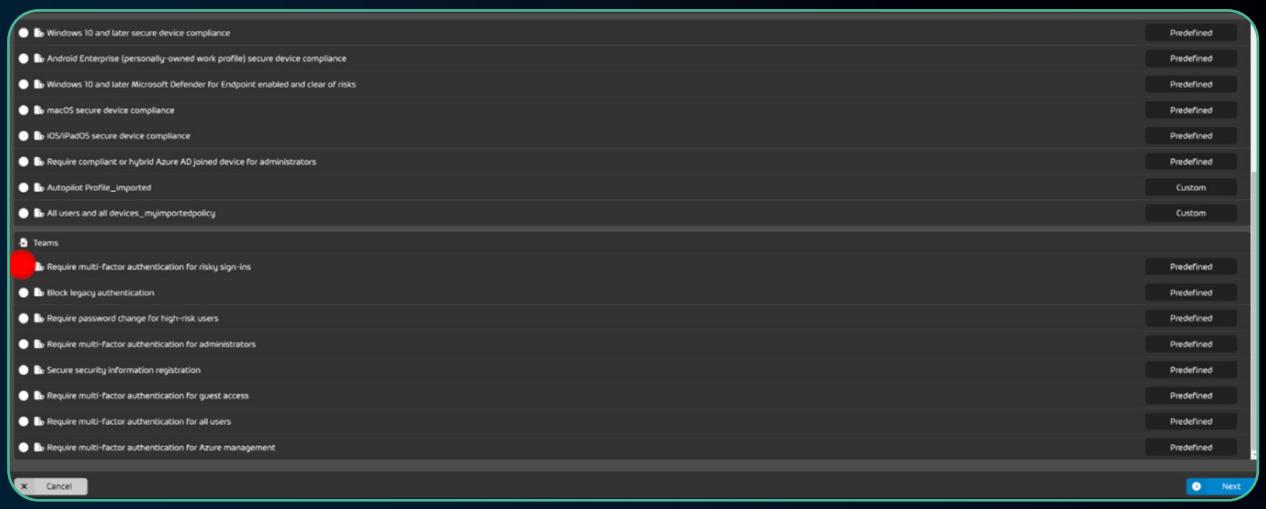


Figura 10 Plantillas de configuración de Multi-Tenant Manager

GESTIÓN DEL TIEMPO

La gestión del tiempo es esencial para la eficiencia de un MSP. Para ser efectivos, debemos:

- Configurar el despliegue inicial con el nombre de dominio y las entradas DNS.
- Implementar nuestra configuración personalizada para el tenant.
- Establecer las configuraciones de cumplimiento y normativas para los tenants adecuados.
- Adaptar personalizaciones específicas del negocio y experiencias de usuario.

El tiempo que dedicamos a cada tarea es clave. Un MSP eficiente debería invertir un 10% o menos de su tiempo en el despliegue de tenants y un 90% en la personalización, que incluye requisitos normativos y de cumplimiento. ¿Por qué desglosarlo de esta forma? Porque el despliegue estándar beneficia al MSP, pero la personalización aporta valor al cliente. Un MSP siempre debería priorizar dedicar la mayor parte de su tiempo a trabajar en beneficio del cliente.

Adapta la configuración de los tenants para cubrir las necesidades específicas de cada cliente en M365.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

Ten presente que la realidad del cliente suele ser muy distinta a la tuya. Ellos no entienden los detalles tecnológicos como tú. Un ejemplo clásico que me ha sucedido varias veces en mi negocio es este: dedico demasiado tiempo a buscar la solución más rentable para una necesidad empresarial, sabiendo que una solución más completa sería mejor a largo plazo, aunque más costosa. Sin embargo, al consultarlo con el cliente, su respuesta fue contundente: "No te pedí que me ahorraras dinero, te pedí la mejor solución". Así que, antes de seguir adelante, asegúrate de confirmar tus suposiciones con el cliente.

GESTIÓN DEL CAMBIO

El último aspecto que debemos dominar en nuestro trabajo de personalización es la gestión del cambio. Las herramientas pueden ayudarte a rastrear el historial de modificaciones, pero serán tus procedimientos operativos estándar (SOP) los que documenten el motivo de cada cambio. Casi todos los cambios que realices deberían aplicarse a un grupo existente de clientes que ya comparten una plantilla común. Es fundamental evitar reducir ajustes para adaptarte a un cliente específico dentro de esa plantilla. Una buena regla general es no crear políticas basadas en excepciones. Si un cliente necesita una excepción, lo más adecuado es asignarle su propia plantilla. Sin embargo, un proveedor de servicios gestionados (MSP) eficiente casi nunca hará esto; en lugar de eso, trabajará para que todos los clientes se alineen con un estándar superior.

RESUMEN

En definitiva, dominar el despliegue personalizado, la personalización y la gestión del cambio es crucial para que los MSP se diferencien en el mercado y ofrezcan valor real a sus clientes. Implementar configuraciones personalizadas de forma eficiente y mantener plantillas estandarizadas permite a los MSP satisfacer las necesidades únicas de sus clientes sin sacrificar la eficiencia operativa. Una gestión eficaz del tiempo, priorizando la personalización sobre el despliegue, permite a los MSP concentrarse en tareas orientadas al cliente. Esto se traduce en una mayor satisfacción del cliente y una propuesta de valor más sólida a la hora de competir en el mercado.

HORNETSECURITY

CAPÍTULO 5

CIBERSEGURIDAD

Hoy en día, pocos temas son tan relevantes para los MSP (Proveedores de Servicios Gestionados) y sus clientes como la ciberseguridad. De hecho, este asunto merece un eBook completo por sí solo. Mantenerse un paso por delante de los ciberdelincuentes y proteger a los clientes requiere un sinfín de configuraciones y un mantenimiento constante. Sin embargo, en este capítulo no nos centraremos tanto en configuraciones específicas, sino en cómo mantener la eficiencia y, con ello, la rentabilidad en un entorno de ciberseguridad que no deja de evolucionar.

Cuando nos planteamos cómo proteger las redes de las que somos responsables, es imprescindible aprovechar al máximo todas las herramientas que tenemos a nuestro alcance.

ENTENDIENDO LAS VULNERABILIDADES

Microsoft ofrece Informes de Analistas en la sección Threat Analytics de Defender, que contienen un gran volumen de información elaborada por expertos sobre el funcionamiento de amenazas específicas. Estos informes son detallados pero fáciles de entender, ya que comienzan con un resumen ejecutivo y profundizan en cómo opera cada amenaza.

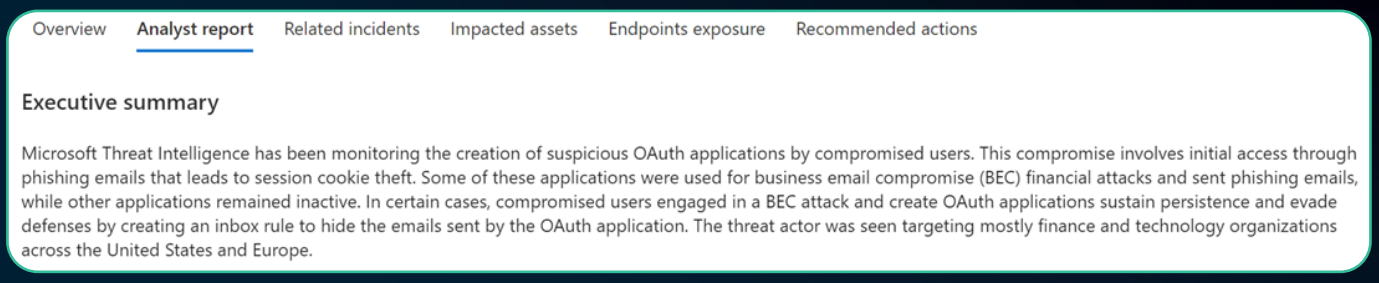


Figura 11 Resumen ejecutivo al inicio del informe detallado de amenazas

En las pestañas del informe encontrarás datos adicionales sobre cómo estas amenazas afectan específicamente a tu entorno y qué acciones puedes llevar a cabo para proteger tu red. Si haces clic en cada tarea pendiente, accederás directamente a las instrucciones necesarias para desplegar las protecciones correspondientes.

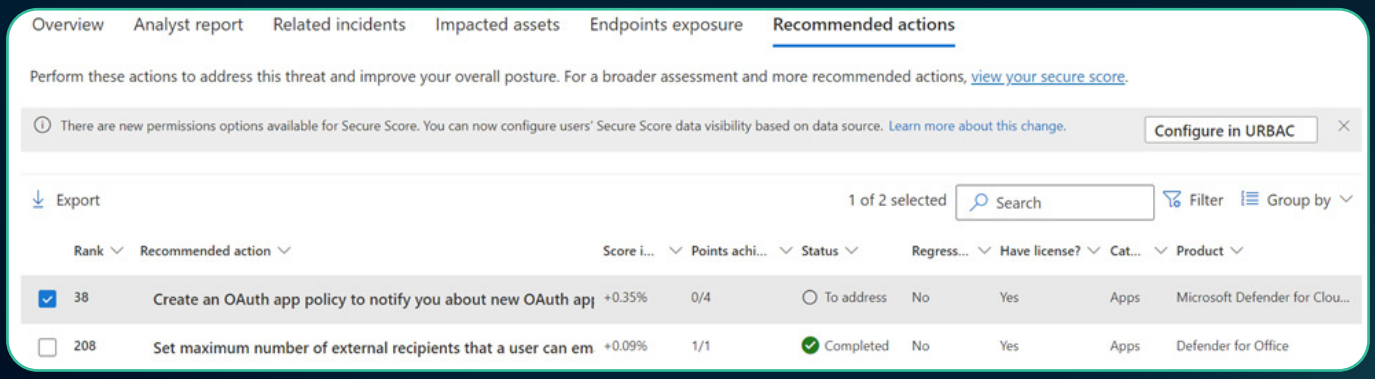


Figura 12 Lista de acciones que deberías realizar para proteger tu red

El portal de Microsoft Defender también enumera vulnerabilidades que no están directamente relacionadas con amenazas específicas. Hay muchísimas. Muchas de ellas son posibles teóricamente, pero no están siendo explotadas de forma activa. En la lista de recomendaciones de seguridad **(Figura 13)**, los iconos rojos indican vulnerabilidades activas, mientras que los iconos grises señalan las potenciales. Aunque esas vulnerabilidades activas quizá no hayan atacado aún tu red, están siendo utilizadas contra otras.

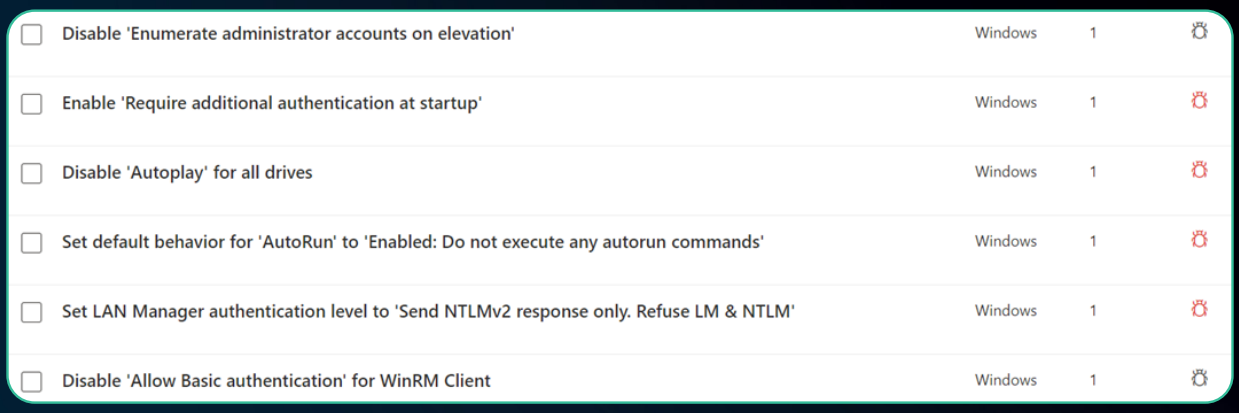


Figura 13 Recomendaciones de seguridad según la vulnerabilidad activa

Con estas dos herramientas, un MSP eficiente puede enfocar sus esfuerzos de mantenimiento en las vulnerabilidades que representan una mayor amenaza para sus clientes.

Cuando ves la cantidad de vulnerabilidades cibernéticas existentes y el número de ciberdelincuentes desarrollando nuevas formas de atacar redes, es fácil sentir que es una batalla perdida. Es una de esas situaciones en las que mucha gente se encoge de hombros y dice resignada: "bueno, no se puede hervir el océano". Es decir, nunca se puede estar completamente al día en ciberseguridad. Sin embargo, al utilizar las herramientas que hemos mencionado, puedes "hervir el agua para una taza de té" y centrarte en proteger las redes de tus clientes con una estrategia clara y efectiva.

BASES DE SEGURIDAD

Otra herramienta clave para mejorar la eficiencia en ciberseguridad son las bases de seguridad. Microsoft ofrece configuraciones de seguridad para Windows, Edge, Windows 365, Defender for Endpoints y las aplicaciones de Microsoft 365.

Figura 14 Security baselines

Puedes usar estas configuraciones como punto de partida, pero suelen ser muy estrictas y, en muchos casos, pueden resultar complicadas de implementar para las empresas. Por eso, lo más recomendable es revisar los parámetros de la configuración base y personalizarla según tus necesidades. Así, conseguirás un estándar propio que podrás aplicar en todos tus clientes.

Eso sí, para llevarlo a cabo necesitarás una herramienta externa, como el **365 Multi-Tenant Manager para MSPs** de Hornetsecurity. Esta herramienta facilita asignar tus estándares a las redes de las que te encargas, y su función de plantillas resulta especialmente práctica para este tipo de tareas.

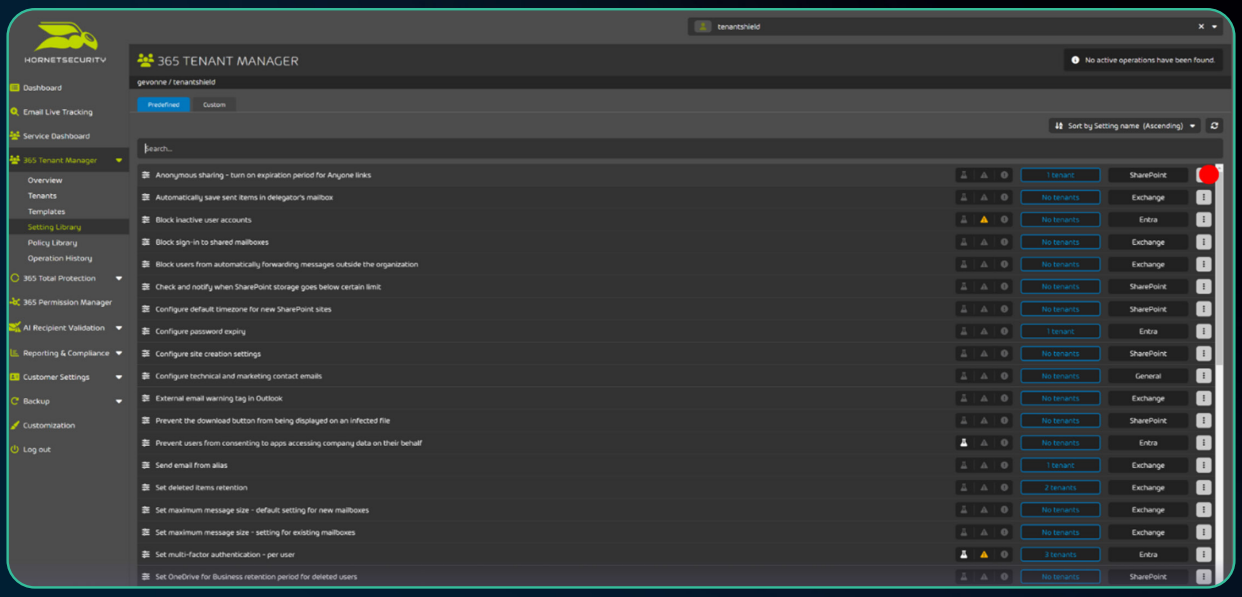


Figura 15 Biblioteca de configuración del Multi-Tenant Manager de Hornetsecurity

SEGURIDAD DEL CORREO ELECTRÓNICO

Sorprendentemente, no existe un estándar universal para garantizar la seguridad del correo electrónico. Con el alarmante aumento de los ataques de compromiso del correo electrónico empresarial (BEC) como medio para infiltrarse en redes, cabría pensar que ya habría uno establecido. Sin embargo, Microsoft ha dado un paso adelante al abordar este problema ofreciendo plantillas preconfiguradas de políticas de seguridad dentro de Defender for Business.

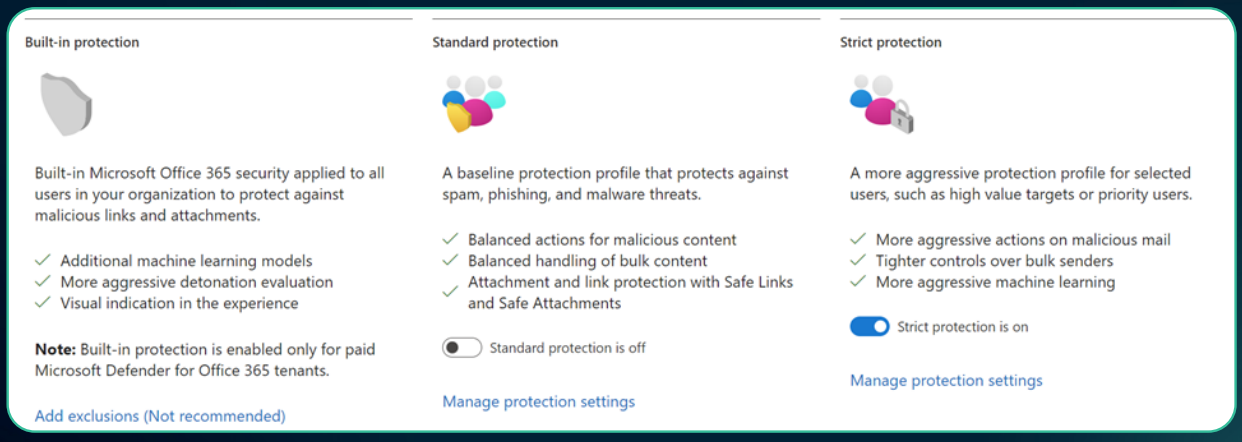


Figura 16 Políticas de seguridad preestablecidas para el correo electrónico

No hay una medida de ciberseguridad más crucial que disponer de una solución integral para proteger el correo electrónico. Los delincuentes emplean métodos como el phishing, el spear phishing y el phishing con códigos QR, además de otras técnicas de ingeniería social, para iniciar sus ataques. En el entorno actual, las empresas deben gestionar su correo electrónico con máxima precaución. La capacidad de suplantar identidades, redactar mensajes convincentes y de alta calidad, y hacer que enlaces fraudulentos parezcan legítimos está más avanzada que nunca. La única forma de combatir esto es implementando un programa completo de seguridad para el correo electrónico, aceptando incluso ciertos falsos positivos. Combinar las plantillas de Microsoft con la **solución 365 Total Protection de Hornetsecurity** es una estrategia eficaz para lograrlo.

INTUNE Y POLÍTICAS DE ACCESO CONDICIONAL

Intune, como mencionamos anteriormente en este eBook, es una herramienta fantástica para configurar y gestionar dispositivos en tu red. Permite desplegar configuraciones y aplicaciones en dispositivos de forma centralizada, proporcionando un control detallado que, en sí mismo, ya es una potente medida de ciberseguridad. Además, con las reglas de Acceso Condicional de Entra, puedes limitar el acceso a la red exclusivamente a los dispositivos registrados. ¿Te imaginas a un ciberdelincuente intentando acceder a tu dominio desde el portátil que usa para sus ataques? Puedes establecer políticas de Acceso Condicional que obliguen a esos dispositivos a unirse al dominio antes de obtener acceso. Y, claro, ¿de verdad van a hacerlo? Otra medida efectiva consiste en limitar el acceso a plataformas compatibles. Por ejemplo, si no utilizas Linux, Mac o versiones antiguas de Windows en tu red, puedes bloquearlas directamente. La idea es poner todos los obstáculos posibles para frustrar sus intentos.

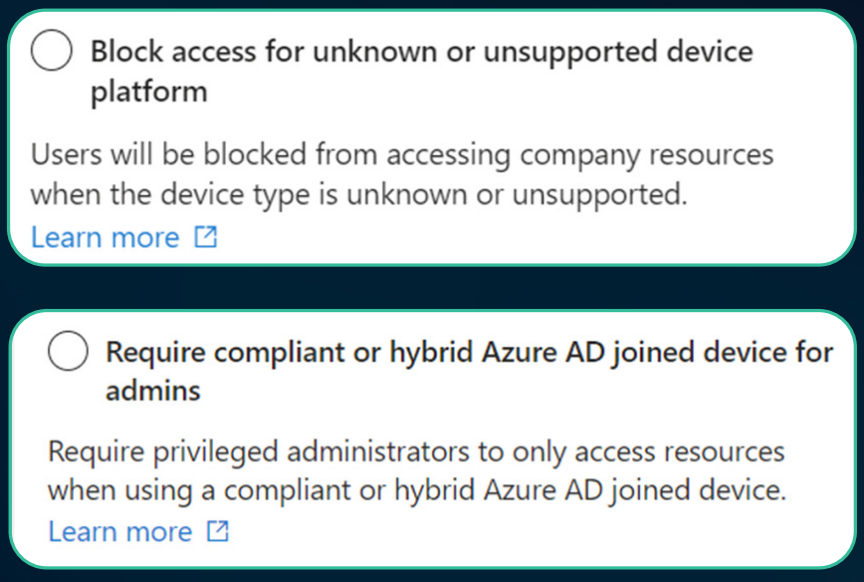


Figura 17 Reglas de acceso condicional de Microsoft Entra

Los paquetes avanzados de licencias de Microsoft 365 también ofrecen funcionalidades como Usuario en Riesgo, Inicio de Sesión en Riesgo y Dispositivo en Riesgo que se pueden integrar en tus políticas para garantizar que solo usuarios y dispositivos seguros accedan a la red.

La gestión de estas políticas de Acceso Condicional (CA) en múltiples tenants de clientes es clave, pero hacerlo manualmente puede ser una tarea titánica. Aquí es donde entra en juego el **365 Multi-Tenant Manager para MSPs** de Hornetsecurity, que simplifica la personalización y despliegue de políticas CA a gran escala.

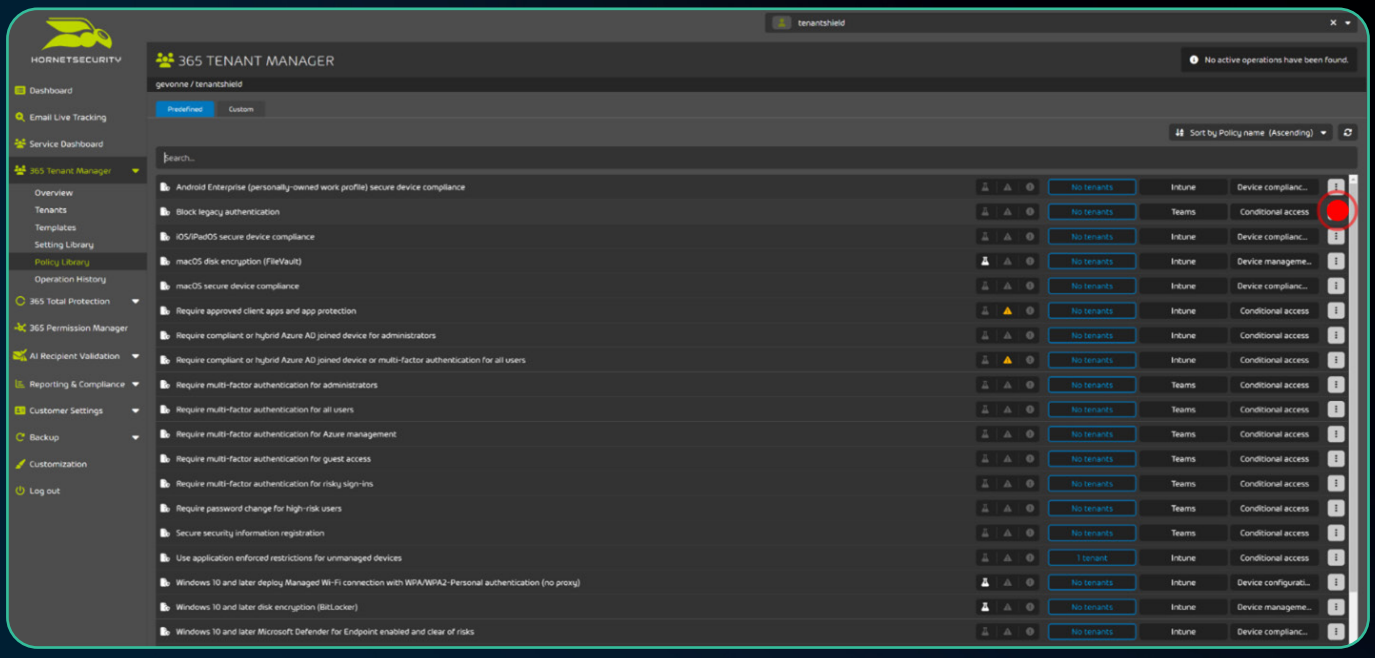


Figura 18 Biblioteca de Políticas de Acceso Condicional en Multi-Tenant Manager

AUTOPILOT, LIGHTHOUSE Y COPIAS DE SEGURIDAD

Además de las herramientas diseñadas para descubrir y configurar ajustes de seguridad, es crucial incluir Autopilot, Lighthouse y una solución de copias de seguridad como parte de tu estrategia de ciberseguridad. Autopilot te permite identificar con precisión los dispositivos que pertenecen a tu dominio y tomar el control desde el momento en que se desembalan. Por otro lado, Lighthouse facilita la gestión de ciertos ajustes directamente a través de los clientes, especialmente si no estás utilizando un servicio de terceros para esa función. Finalmente, las copias de seguridad garantizan la continuidad del negocio en caso de que todo lo demás falle.

Como se mencionó anteriormente, la continuidad del negocio parece ser un aspecto que muchos proveedores de servicios gestionados (MSPs) pasan por alto. Contar con un panel de control claro y fácil de leer que muestre el estado de las copias de seguridad de todos tus tenants es una forma eficaz de supervisar esta tarea tan crítica.

Garantiza que todos los tenants sean seguros, compatibles y uniformes.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

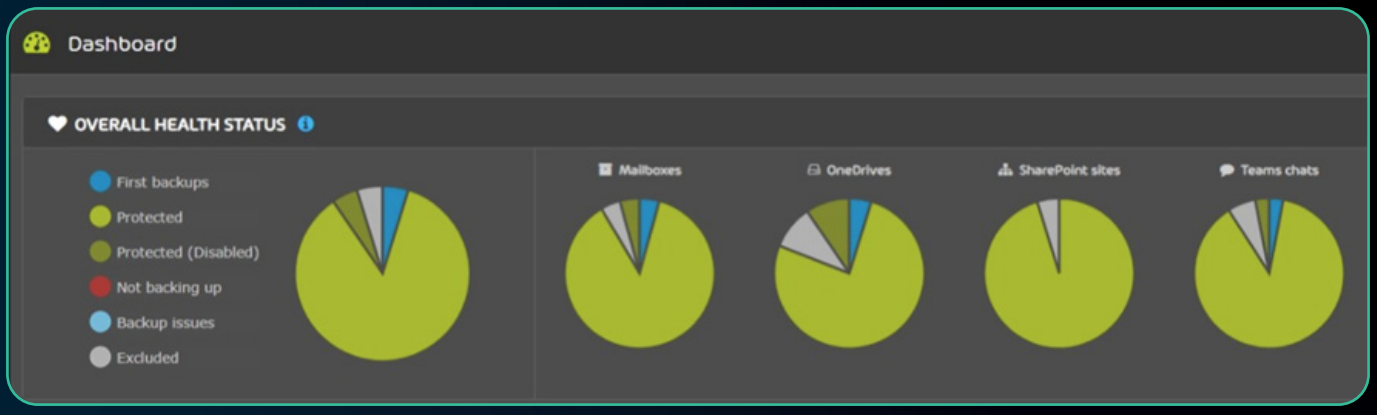


Figura 19 Panel de estado de las copias de seguridad de Hornetsecurity Total Backup

Para cerrar el círculo en términos de continuidad del negocio, los MSPs deberían realizar pruebas de restauración al menos una vez por trimestre para verificar que las copias de seguridad se pueden recuperar sin problemas. Las copias de seguridad no tienen valor si no son restaurables. Es curioso, pero hay una verdad universal en el mundo de la informática: las impresoras y las copias de seguridad siempre fallan cuando menos lo esperas. Ignorarlas o no revisarlas regularmente es una mala idea.

La visibilidad es esencial para gestionar la ciberseguridad de tus clientes. Con un sistema bien configurado, como Microsoft Sentinel (que utilizo con todos mis clientes), puedes identificar en cuestión de minutos si alguien ha creado una nueva política de acceso condicional, añadido un método de autenticación multifactor (MFA) a su cuenta o sido víctima de un ataque de fatiga de MFA (recibiendo tantas solicitudes que acaba aceptándolas para que cesen). Esta capacidad de supervisión casi en tiempo real me ha permitido contener incidentes menores antes de que se conviertan en brechas de seguridad importantes.

RESUMEN

Para concluir este capítulo sobre ciberseguridad, es fundamental entender que el panorama de amenazas está en constante evolución. Los profesionales de IT que trabajan con pequeñas empresas deben ser vigilantes y proactivos en su enfoque. Aprovechando herramientas y estrategias como las mostradas aquí, es posible proteger redes y datos de forma eficaz, manteniendo al mismo tiempo la eficiencia y la rentabilidad. Recuerda: la ciberseguridad no es un esfuerzo puntual, sino un proceso continuo que requiere aprendizaje, adaptación y compromiso constantes. Mantente informado, preparado y seguro.

CAPÍTULO 6

GESTIÓN DE PROVEEDORES

Cuando gestionas un MSP (Proveedor de Servicios Gestionados), hay varias maneras de abordar la relación con los proveedores. ¿Deberíamos optar por trabajar con varios proveedores líderes en su categoría o quedarnos con uno sólo? A primera vista, la elección parece obvia: decidir entre un único proveedor o múltiples. Pero la realidad es más compleja. Si la eficiencia es nuestra prioridad, hay muchos aspectos a tener en cuenta. Debemos encontrar un equilibrio entre ser eficientes y ofrecer a nuestros clientes una solución sobresaliente. Ante decisiones complicadas, herramientas como una tabla comparativa o un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades) pueden ser de gran ayuda. En este capítulo, exploraremos ambos enfoques.

EL ENFOQUE DE LA TABLA DE DECISIONES

Hace años, antes de que la ciberseguridad se volviera tan intrincada y nuestras necesidades de defensa fueran tan amplias, solía decantarme por los proveedores líderes en su categoría. En aquel entonces, esta decisión implicaba trabajar sólo con dos proveedores, lo que era manejable. Sin embargo, con el tiempo, mi perspectiva cambió a medida que el panorama de la ciberseguridad se transformaba. Hoy en día, trabajar con una selección de los mejores proveedores implica coordinar a muchos más actores, y las diferencias entre las soluciones han disminuido conforme los proveedores han ido madurando.

FACTOR	ENFOQUE DE UN SOLO PROVEEDOR	ENFOQUE BEST-OF-BREED
Complejidad de gestión	Simplificada	Compleja
Coste	Económico	Costes más altos
Integración	Sin fisuras	Desafiante
Innovación	Limitada	Alta
Dependencia del proveedor	Alta	Baja

Figura 20 Tabla de decisión

Tomar esta decisión nunca fue sencillo, ya que siempre conlleva concesiones. Entre los factores a considerar están la complejidad de la gestión, los costes, la integración, la innovación y, cada vez más, la dependencia de los proveedores.

El enfoque de Best-of-Breed (mejores en su categoría) tiene sus inconvenientes. La gestión se complica al tener que supervisar varios portales, lidiar con múltiples pagos y asumir un incremento de los costes operativos. La integración, en el mejor de los casos, resulta un desafío, y muchas veces es directamente imposible. Por si fuera poco, los contratos con los proveedores suelen incluir condiciones que dificultan el cambio, con cláusulas largas y complejas.


Optimiza tus recursos y maximiza los resultados.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

Otro problema que surge es el de los "huecos" entre las soluciones que implementamos. Al usar productos de distintos proveedores, a menudo desconocemos dónde termina la cobertura de uno y empieza la del otro, lo que puede dejar brechas sin cubrir. Estos vacíos representan riesgos importantes que debemos gestionar con cuidado.

ENFOQUE DAFO

El análisis DAFO es un método sencillo que analiza fortalezas, debilidades, oportunidades y amenazas. Es una herramienta muy útil para la toma de decisiones en diversos contextos. Aplicar el análisis DAFO nos permite examinar dos enfoques principales para gestionar proveedores en ciberseguridad.

DAFO DE UN ÚNICO PROVEEDOR

- **Fortalezas:** Gestión simplificada, menos complejidad, experiencia de usuario consistente, posible ahorro de costes.
- **Debilidades:** Falta de flexibilidad, dependencia del proveedor (vendor lock-in), menor innovación.
- **Oportunidades:** Operaciones más optimizadas, soporte técnico más sencillo.
- **Amenazas:** Dependencia excesiva de un único proveedor, riesgo de brechas de seguridad.

DAFO DEL ENFOQUE BEST-OF-BREED

- **Fortalezas:** Mayor especialización, flexibilidad, menor dependencia de un solo proveedor.
- **Debilidades:** Gestión más complicada, costes más altos, posibles problemas de integración.
- **Oportunidades:** Acceso a tecnologías avanzadas, soluciones personalizadas.
- **Amenazas:** Complejidad añadida, riesgos de incompatibilidades entre proveedores.

Una revisión de la información sobre el uso de proveedores en los MSP (Proveedores de Servicios Gestionados) reveló que los MSP más grandes trabajan con hasta 70 proveedores, mientras que los MSP promedio suelen tener en torno a 7. No obstante, se ha detectado una tendencia hacia la consolidación de proveedores. Esto se debe, en parte, a la dinámica general del mercado, pero también a la necesidad de lograr una mayor eficiencia operativa. Como MSP, es complicado gestionar un número elevado de proveedores o formar al personal en una variedad tan amplia de soluciones.

La creciente complejidad de la ciberseguridad nos obliga a consolidar esfuerzos y tomar decisiones más estratégicas. Aunque depender de un solo proveedor no es una solución viable, adoptar dos como estándar puede ser una estrategia razonable. Uno de estos proveedores podría ser Microsoft, que ha realizado importantes inversiones en seguridad y ha integrado sus soluciones dentro de las suites de Microsoft 365. Sin embargo, este enfoque está diseñado en gran medida para equipos de seguridad especializados, mientras que los MSP típicos suelen ser pequeños y cuentan con generalistas que necesitan abarcar un amplio rango de conocimientos en ciberseguridad. Por ello, es necesario contar con un segundo proveedor que complemente las carencias de Microsoft. Eso sí, es fundamental elegir un **conjunto de herramientas de seguridad** que estén bien integradas para reducir los problemas derivados de gestionar soluciones aisladas.

GESTIÓN MULTITENANT CON MÚLTIPLES PROVEEDORES

Un proveedor como Hornetsecurity puede ser clave para cubrir los huecos que deja Microsoft. Por ejemplo, Microsoft no ofrece una solución completa de copias de seguridad para Microsoft 365. Aunque cada vez quedan menos áreas por cubrir, la gestión multitenant sigue siendo una necesidad que los proveedores pueden abordar.

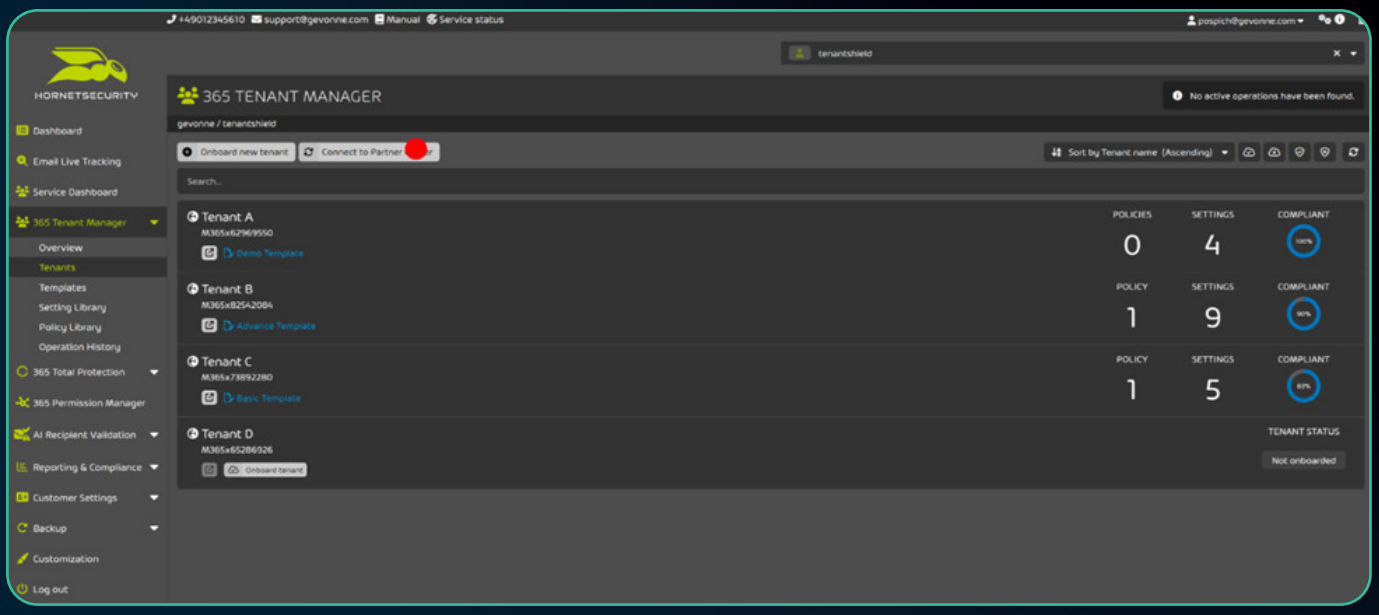


Figura 21 Onboarding de tenants en Multi-Tenant Manager de Hornetsecurity

Últimamente, Microsoft ha comenzado a incorporar funciones de gestión multitenant en algunos de sus productos, como Defender XDR. Sin embargo, estas funciones vienen acompañadas de limitaciones que, aunque a primera vista parecen arbitrarias, tienen sentido desde su perspectiva. Al desarrollar soluciones pensadas para grandes empresas, han establecido un límite de 50 tenants en el portal multitenant de Defender. Esto puede ser razonable si eres una gran organización con varios tenants internos. Muchas empresas tienen tenants separados para diferentes líneas de negocio o como resultado de adquisiciones. Sin embargo, para un MSP (Proveedor de Servicios Gestionados), 50 tenants se quedan cortos. Algunos de nuestros clientes también cuentan con múltiples tenants adquiridos a través de fusiones y adquisiciones. En mi MSP, que somos un equipo de 7 personas, gestionábamos 80 clientes, superando de lejos el límite de 50 tenants que permite la solución multitenant de Defender. Por eso, aunque preferimos usar Defender XDR como solución de seguridad, necesitamos un sistema de gestión distinto. La sugerencia de Microsoft de priorizar a ciertos clientes por encima de otros nos resulta inaceptable. Para garantizar eficiencia y ofrecer un servicio de calidad igual para todos los tenants, recurrimos a alternativas como el **365 Multi-Tenant Manager para MSPs** de Hornetsecurity.

CONSIDERACIONES ADICIONALES

Simplificar la gestión de proveedores permite a los MSP centrarse en servicios de mayor valor, como asumir roles virtuales de Director de Información (CIO) o Director de Seguridad de la Información (CISO). Este cambio facilita que los MSP ofrezcan orientación estratégica, alineen las iniciativas de ciberseguridad con los objetivos del negocio y obtengan ventajas competitivas. Los clientes valoran más los resultados visibles y concretos, como la mejora en la seguridad, el cumplimiento normativo o la reducción de riesgos, lo que incrementa su satisfacción y lealtad. Avanzar hacia una ciberseguridad más profesionalizada no solo mejora la propuesta de valor, sino que también abre la puerta a nuevos ingresos y a relaciones más sólidas con los clientes. Al centrarse en servicios estratégicos, los MSP pueden impulsar un crecimiento sostenible mientras responden a las demandas del mercado, que cada vez exige soluciones más avanzadas.

RESUMEN

En definitiva, gestionar proveedores en un entorno MSP implica encontrar el equilibrio adecuado entre eficiencia y calidad en las soluciones ofrecidas. Decidir entre un único proveedor o un enfoque basado en los mejores especialistas de cada categoría no es sencillo, ya que requiere evaluar factores como la complejidad, los costes, la integración, la innovación y la dependencia de terceros. Optar por un único proveedor puede simplificar la gestión y reducir costes, pero también puede llevar a una dependencia excesiva y limitar la innovación. En cambio, el enfoque de "best-of-breed" aporta especialización y flexibilidad, aunque conlleva una mayor complejidad y costes de gestión. La elección depende de las necesidades y objetivos concretos del MSP. Un proceso reflexivo, como una tabla de decisiones o un análisis DAFO, puede ser de gran ayuda para tomar la mejor decisión. Al gestionar eficazmente las relaciones con los proveedores, los MSP pueden centrarse en servicios estratégicos y lograr un crecimiento sostenible para su negocio.

Estos aspectos, que a menudo pasan desapercibidos, aportan un gran valor tanto para el cliente como para el MSP, subrayando la importancia de gestionar de forma eficiente las relaciones con los proveedores.


Optimiza tus recursos y maximiza los resultados.
365 MULTI-TENANT MANAGER FOR MSPs
DESCUBRE MÁS

HORNETSECURITY

CAPÍTULO 7

CONCLUSIÓN

En este eBook hemos analizado cinco factores clave que impulsan una operación eficiente de un MSP (Proveedor de Servicios Gestionados): onboarding de clientes, supervisión y mantenimiento, personalización, gestión de la ciberseguridad y de proveedores. Hemos revisado estas áreas esenciales de las operaciones de los MSP, identificando dónde se pueden optimizar los procesos y proponiendo formas prácticas de hacerlo.

Esto es lo que hemos aprendido:

ONBOARDING EFICIENTE

Para lograr un onboarding eficiente, es necesario realizar las siguientes cuatro tareas:

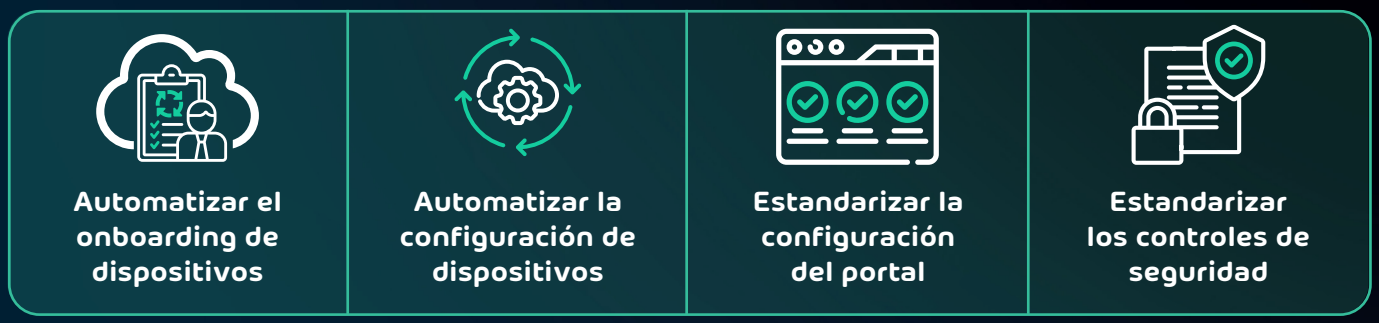


Figura 22 Onboarding eficiente

Es crucial usar herramientas internas y de terceros para minimizar el tiempo requerido en estas tareas, pero siempre equilibrándolo con las expectativas del cliente y garantizando una experiencia excelente. Encontrar este equilibrio puede ser muy beneficioso a largo plazo en la relación con el cliente. En nuestra reunión con los interesados, desglosamos las diferencias entre las perspectivas del cliente y del MSP, destacando que estas diferencias no solo surgen en esta fase, sino que están presentes a lo largo de toda la relación.

SUPERVISIÓN Y MANTENIMIENTO

En el ámbito de la supervisión y el mantenimiento, hemos analizado cómo los MSP pueden trabajar de forma más eficiente sin sacrificar la calidad del servicio. Destacamos la importancia del mantenimiento proactivo como una estrategia clave para prevenir problemas antes de que ocurran, así como el papel crucial de la monitorización automatizada para detectar y resolver incidencias de manera más ágil.También abordamos la relevancia de contar con procedimientos bien definidos para responder a incidentes, así como la planificación para la recuperación ante desastres, lo que asegura una respuesta rápida y efectiva ante posibles interrupciones. Sin embargo, aunque la automatización es una herramienta esencial para ganar eficiencia, no puede implementarse a costa de descuidar la relación humana con el cliente. Una parte importante del valor que aporta un MSP reside en la interacción entre el equipo de soporte y el cliente. Aunque gran parte del trabajo rutinario pasa desapercibido, el trato cercano y profesional deja una impresión duradera.

Al establecer procedimientos efectivos y planes sólidos, los MSP no solo mejoran su rendimiento, sino que también logran un mejor equilibrio entre productividad, satisfacción del cliente y rentabilidad.

PERSONALIZACIÓN

Dominar la personalización y la gestión del cambio es clave para que los MSP (proveedores de servicios gestionados) se diferencien en el mercado y aporten verdadero valor a sus clientes. Al implementar configuraciones personalizadas de manera eficiente y mantener plantillas estandarizadas, los MSP pueden atender las necesidades específicas de sus clientes sin perder de vista la eficiencia operativa. Una gestión del tiempo bien enfocada, priorizando la personalización sobre el despliegue técnico, permite que los MSP dediquen más esfuerzo a tareas orientadas al cliente, lo que se traduce en una mayor satisfacción y una posición más sólida en el mercado. Además, optimizar este aspecto puede abrir la puerta a que los MSP se especialicen en sectores concretos o en el cumplimiento de normativas específicas, mejorando tanto su eficiencia como su rentabilidad.

GESTIÓN DE LA CIBERSEGURIDAD

Es fundamental tener en cuenta que el panorama de las amenazas cibernéticas está en constante evolución. Los profesionales de ITque trabajan con pequeñas empresas deben mantenerse alerta y adoptar un enfoque proactivo hacia la ciberseguridad. Aprovechando las herramientas y estrategias descritas en este capítulo, pueden proteger eficazmente las redes y los datos de sus clientes, manteniendo al mismo tiempo la eficiencia y la rentabilidad.

La ciberseguridad no es una tarea puntual, sino un proceso continuo que exige aprendizaje y adaptación constantes. En este sentido, gestionar la ciberseguridad no dista mucho de tareas como la supervisión o el mantenimiento, en cuanto a la necesidad de eficiencia, y puede ser un motor para establecer nuevos estándares. Para ello, los MSP deben contar con equipos altamente cualificados, capaces de mantenerse al día con las últimas tendencias, estar preparados y, sobre todo, garantizar la seguridad.

GESTIÓN DE PROVEEDORES

En un entorno empresarial que cambia a gran velocidad, muchos MSP han añadido nuevos proveedores sin un plan claro, resultando en una gestión desordenada y poco eficiente. Revisar estas decisiones desde una perspectiva de eficiencia es una tarea crucial. En este contexto, herramientas como el análisis DAFO o una tabla comparativa pueden ser de gran ayuda.

Simplificar la gestión de proveedores permite a los MSP centrarse en servicios más estratégicos, como los roles de CIO o CISO virtuales. Este cambio no solo refuerza su propuesta de valor, sino que también les permite ofrecer asesoramiento estratégico, alinear las estrategias de ciberseguridad con los objetivos de negocio y garantizar una ventaja competitiva. Los clientes valoran más los resultados tangibles, como el fortalecimiento de la seguridad, el cumplimiento normativo y la mitigación de riesgos. Estos beneficios se traducen en mayor satisfacción y fidelización. Avanzar hacia servicios de mayor nivel en ciberseguridad implica no solo un incremento en los beneficios, sino también relaciones más profundas y valiosas con los clientes. Este enfoque estratégico permite a los MSP un crecimiento empresarial sostenible mientras aprovechan las tendencias del mercado.

ÚLTIMAS PALABRAS

Si los responsables de un MSP y su equipo técnico logran dominar las cinco áreas analizadas, el éxito está garantizado. Los MSP desempeñan un papel esencial en el funcionamiento de empresas de todo tipo, especialmente aquellas que no cuentan con un departamento de IT propio con las capacidades que un MSP puede aportar. El mercado potencial para un MSP eficiente es inmenso, y las oportunidades son prácticamente ilimitadas. Cuando un MSP tiene éxito, todos ganan, y la eficiencia es el factor clave para alcanzar ese éxito.

AI POWERED

HORNETSECURITY

365 MULTI-TENANT MANAGER FOR MSPs

AUTOMATIZAR ESTANDARIZAR CONTROLAR

La gestión de los tenants de M365 es una tarea que consume muchos recursos, y los proveedores de servicios pasan varias horas intentando gestionar varios portales de administración para configurar a sus clientes. Configurar tenents de M365 es una tarea muy detallada y compleja, y no basta con saber cómo configurarlos: los proveedores de servicios también deben mantener una seguridad estricta y mantener a raya los riesgos. Si se multiplica todo esto por las diversas necesidades de los tenants para diferentes clientes, el problema se convierte rápidamente en una montaña que puede resultar abrumadora.

LA GESTIÓN DE TENANTS DE MICROSOFT 365 MÁS FÁCIL QUE NUNCA

¿Qué se ve afectado?	¿Cómo le ayuda 365 Multi-Tenant Manager para MSP?			¿Qué mejora?
Todos los tenants de Microsoft 365	Automatizar	Estandarizar	Controlar	Gestión, gobernanza y cumplimiento sin esfuerzo para todos los tenants de M365.
	Detección automática de tenants M365 aprovechando la conexión con Microsoft Partner Center.	Plantillas, ajustes y políticas listas para usar con la flexibilidad necesaria para personalizar sus propias configuraciones.	Cuadro de mandos detallado para un análisis exhaustivo y una llamada a la acción para todos los tenants gestionados.	

HORNETSECURITY

365 MULTI-TENANT MANAGER FOR MSPs

365 MULTI-TENANT MANAGER PARA MSPS CARACTERÍSTICAS

Descubrimiento automático de tenants M365 aprovechando la conexión con Microsoft Partner Center, para facilitar el aprovisionamiento y la racionalización de los servicios.

Eliminación de la gestión de varios portales de Microsoft. Con 365 Multi-Tenant Manager para MSP, **se puede gestionar un tenant desde una solución consolidada a través de un único panel.**

Simplificación y estandarización de los complejos flujos de trabajo y dependencias entre portales en la administración de Microsoft Azure/M365.

Asistentes/wizards fáciles de usar que guían a los proveedores de servicios desde la incorporación del inquilino hasta su configuración, personalización y supervisión de las tareas automatizadas.

Configuraciones, políticas y plantillas listas para usar que todas las organizaciones pueden adoptar rápidamente.

Compatibilidad con herramientas integradas para la creación de configuraciones y políticas personalizadas y la importación de políticas de tenants, lo que garantiza que los MSP puedan satisfacer las necesidades exclusivas de cada cliente dentro de su tenant M365.

Corrección y aplicación automáticas cuando se detecta un incumplimiento.

Amplios cuadros de mando para la supervisión y la elaboración de informes.

Paneles de control detallados para **un análisis exhaustivo y una llamada a la acción** de todos los tenants gestionados y sus estados de cumplimiento.

AUTOMATIZA.
ESTANDARIZA.
GESTIONA.

365 MULTI-TENANT MANAGER FOR MSPs

DESCUBRE MÁS

www.hornetsecurity.com | info@hornetsecurity.com | +34 93 470 07 78