

# La guía definitiva para proveedores de servicios de TI sobre ofertas de seguridad

Los ciberataques no se están frenando. Al contrario, se aceleran, y la inteligencia artificial (IA) está ayudando a los ciberdelincuentes a moverse más rápido y parecer más convincentes que nunca.

- Correos de phishing generados con IA que parecen venir del CEO del cliente
- Kits de Ransomware-as-a-Service (RaaS) que permiten lanzar campañas en minutos
- Audios deepfake usados para suplantar ejecutivos en llamadas telefónicas

No es sorpresa que los clientes estén preocupados y busquen un proveedor de servicios de TI en quien confiar para mantener seguro su negocio. Los que asumen ese rol tienen mucho que ganar.

Esta checklist ofrece pasos simples para pasar de ser un proveedor de soporte de TI tradicional a un experto confiable en seguridad gestionada.



---

## La seguridad ya no es un lujo, es una expectativa

Más allá de eso, significa que tu negocio puede volverse altamente rentable, con retornos constantes y crecimiento sostenido.

Según la Encuesta Benchmark 2025, los proveedores de servicios de TI con márgenes netos de 15% o más ubicaron los servicios de seguridad mejorada entre sus tres principales fuentes de ingresos. En contraste, quienes tenían márgenes más bajos no lo hicieron.

Esto no es coincidencia. La seguridad es una de las formas más confiables de aumentar ingresos y proteger la rentabilidad.

El Reporte Datto State of IT Services 2024 concluyó lo mismo: los proveedores de servicios de TI de mejor desempeño lideran con ciberseguridad. Servicios como EDR, seguridad de correo y MDR/SOC no son extras, sino potentes motores de retención y diferenciadores comerciales.

# Tus clientes esperan seguridad

## Paso 1: Define el tipo de soluciones que necesitas

### Pregúntate:

Qué ofrecen los proveedores de servicios de seguridad de TI que yo no?

Qué amenazas preocupan más a mis clientes?

### Un stack moderno de seguridad va más allá del antivirus y los firewalls e incluye:

Detección y respuesta en endpoints (EDR)

Detección y respuesta gestionada (MDR) o SOC gestionado

Seguridad avanzada de correo y protección contra phishing

Monitoreo y respuesta 24/7 a amenazas

Gestión de parches y protección contra zero-day



### Principales amenazas (Reporte Datto 2024):

64% Phishing por correo electrónico

61% Compromiso de correo empresarial

59% Malware y virus

56% Contraseñas comprometidas

51% Amenazas en endpoints

## Paso 2: Encuentra al proveedor de seguridad adecuado

**No tienes que construir tu stack de seguridad desde cero, pero sí necesitas un proveedor confiable que te ayude a hacerlo de manera accesible.**

### Busca proveedores que ofrezcan:

Herramientas multicitente diseñadas para flujos de trabajo de servicios de TI

Servicios SOC 24/7 para escalar tu capacidad de respuesta

Integraciones probadas con tu stack actual (RMM, PSA, etc.)

Precios accesibles que permitan crecimiento de margen

Capacitación continua y soporte confiable

## Paso 3: Capacita a tu equipo

### Antes de lanzar servicios a los clientes, asegúrate de que tu equipo esté listo:

Capacitación de productos con tu proveedor

SOPs internos para onboarding y respuesta

Certificación de técnicos, especialmente en herramientas SOC

Alinear al equipo en cómo posicionar y dar soporte a cada nuevo servicio

## Paso 4: Promociona tus nuevas capacidades

**Si no lo cuentas, nadie lo sabrá. Y si lo cuentas solo una vez, probablemente lo olviden. Necesitas promocionar tus servicios de seguridad de manera consistente en los canales que tus clientes ya usan.**

### Formas fáciles de difundir:

- Agregar una página de Servicios de Seguridad a tu sitio web
- Incluir la oferta en materiales de onboarding y presentaciones
- Anunciar nuevos servicios en newsletters y correos
- Escribir blogs sobre riesgos comunes y buenas prácticas
- Compartir tips en LinkedIn o Facebook (ej. cómo detectar un phishing)
- Crear un video explicando cómo reduces ransomware, downtime o pérdida de datos
- Organizar un webinar o campañas dirigidas para prospectos

## Paso 5: Construye confianza

**La credibilidad genera confianza, y la confianza impulsa el crecimiento. Una vez que los clientes vean valor:**

- Pide testimonios a clientes satisfechos
- Crea casos de éxito cortos con resultados reales
- Usa citas en presentaciones, emails y en tu sitio web

## La seguridad es el movimiento más inteligente ahora

Los proveedores de servicios de TI que más crecen son los que han agregado seguridad a su oferta principal. No es solo un movimiento estratégico, es esencial para cumplir expectativas y ser competitivo.