Lo que puede destruir tu Pyme este 2026

Si no cumples este mínimo de seguridad

José González - Desarrollo de negocio

zynco
Technology without limits

⚠ URGENTE

En 2026 no te atacan por ser grande. Te atacan por ser fácil.

Ataques automatizados y masivos

El cibercrimen hoy funciona como una industria: herramientas automatizadas que escanean millones de empresas buscando vulnerabilidades básicas.

Las Pymes son objetivo fácil

No te descartan por tamaño, te eligen por facilidad. Menos recursos de protección significan más probabilidad de éxito para los atacantes.

El riesgo real: continuidad del negocio

Un ataque exitoso no solo compromete datos: para la operación completa, impide facturar y puede cerrar tu empresa definitivamente.

Los ataques ya no son artesanales. Son industria, automatización y volumen.

Y en una Pyme, el impacto no es "tengo un virus"… el impacto es que se para el negocio.

Lo que realmente destruye una Pyme

Paro operativo total

No puedes facturar, no produces, los empleados no pueden trabajar. Cada día parado representa pérdidas irrecuperables.

Pérdida de datos críticos

Clientes, contabilidad, proyectos en curso. Información que ha costado años construir puede desaparecer en minutos.

Fraude por suplantación

Correos comprometidos permiten estafas a clientes y proveedores usando tu identidad. El daño va más allá de lo económico.

Reputación y confianza

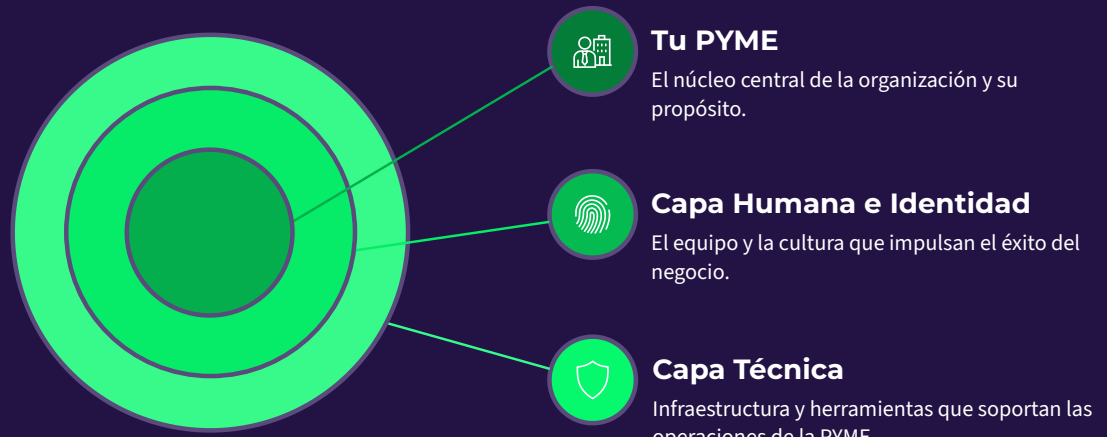
Los clientes dudan en seguir trabajando contigo. La recuperación de imagen puede llevar años o ser imposible.

RGPD y sanciones legales

Multas por incumplimiento del RGPD, costes legales, reclamaciones. El coste oculto puede superar el del propio ataque.

El ataque no te roba un ordenador… te roba días o semanas de vida del negocio. Y hay empresas que no sobreviven a eso.

La seguridad real es por capas



Tu PYME
El núcleo central de la organización y su propósito.

Capa Humana e Identidad
El equipo y la cultura que impulsan el éxito del negocio.

Capa Técnica
Infraestructura y herramientas que soportan las operaciones de la PYME.

El principio de defensa en profundidad

- No hay una herramienta mágica que te salve
- Si una capa falla, la siguiente sostiene el ataque
- Si te falta una capa crítica… caes en cascada

La clave: No es el ataque lo que destruye una Pyme. Es que todo falle a la vez cuando llega.

CAPA 1

Dispositivos protegidos: PCs y servidores

Los dispositivos son el punto donde la empresa trabaja. Si aquí entras, puedes parar la empresa completa. El mínimo empieza aquí:

01

Parches automatizados

Actualización constante de sistemas operativos y aplicaciones. Las vulnerabilidades conocidas son puertas abiertas para atacantes.

02

Inventario HW/SW completo

Control real de qué dispositivos y software tienes en tu red. No puedes proteger lo que no conoces.

03

EDR: Detección y Respuesta

Endpoint Detection and Response. La diferencia entre estar protegido y creer que lo estás.

04

Opcional según tamaño: DLP / XDR

Data Loss Prevention y Extended Detection and Response para empresas con mayores necesidades de protección.

Antivirus tradicional vs EDR: la diferencia crítica en 2026

❌ Antivirus tradicional

- Funciona por firma: solo detecta amenazas conocidas
- Reactivo: actúa cuando ya hay infección
- No detecta comportamientos anómalos
- Sin capacidad de respuesta automática

✅ EDR moderno

- Detecta patrones raros y comportamientos sospechosos
- Proactivo: identifica amenazas en tiempo real
- Contiene el ataque automáticamente
- Responde y mitiga antes de que se propague

Si no tienes EDR, lo peor no es estar desprotegido... lo peor es creer que estás protegido.

Los ataques modernos no entran como "virus clásico". Entran como comportamiento, como herramientas legítimas, como movimiento lateral. El antivirus te avisa de que tienes un problema. El EDR evita que el problema se convierta en cierre.

CAPA 2

Cloud protegido

El cloud ya no es solo un disco duro externo; es donde vive tu empresa. Si no está protegido, toda tu operación está en riesgo.

Email: puerta de entrada nº1

El correo electrónico es el vector de ataque más frecuente. Un solo clic erróneo puede comprometer toda tu red.

Advanced Email Security

Protección anti-phishing y anti-malware proactiva. Filtra las amenazas antes de que lleguen a la bandeja de entrada de tus empleados.

Backup de correo y datos cloud

Asegura la recuperación rápida de M365, Google Workspace y otros datos cloud. Un buen backup te permite volver a operar en minutos, no en días.

> **“El correo no es una herramienta: es tu empresa. Si lo pierdes, pierdes el control.”**

CAPA 3

Backup real (3-2-1-0)

El backup no es una opción, es la última línea de defensa de tu PYME. Pero no cualquier backup sirve. Necesitas una estrategia robusta que siga la regla de oro: la regla 3-2-1.

3 copias de tus datos

Una original y dos copias adicionales. Esto minimiza el riesgo de perder todos tus datos por un único punto de fallo.

2 soportes distintos

Almacena tus copias en al menos dos tipos de medios diferentes (ej: disco local y nube) para mayor resiliencia.

1 copia fuera de red / inmutable

Mantén al menos una copia completamente aislada de tu red (offline) o con características de inmutabilidad para protegerla de ransomware y eliminaciones accidentales.

0 errores al restaurar

Un backup solo es útil si puedes recuperarlo. Realiza pruebas de restauración regularmente para asegurar que tus datos son accesibles y utilizables.

> **“El ransomware va a por tus copias. Backup que no se restaura, no existe.”**

CAPA 4

Firewall perimetral gestionado

El firewall no solo bloquea amenazas, sino que gestiona el tráfico de tu red para garantizar un funcionamiento seguro y eficiente.

Primera línea de defensa

Actúa como la barrera inicial entre tu red interna y las amenazas externas de internet.

Filtrado inteligente

Bloquea accesos maliciosos y filtra tráfico no deseado, protegiéndote de intrusiones y ataques.

Menor superficie de ataque

Reduce los puntos vulnerables por donde los ciberdelincuentes podrían intentar acceder a tu empresa.

Reglas y monitorización

Mantenimiento continuo de reglas, actualizaciones de firmware y monitorización en tiempo real para una protección activa.

“El firewall no lo sustituye todo… pero evita que te entren por la puerta principal.”

CAPA 5

Personas: La Capa más Crítica

No importa cuán robusta sea tu tecnología, el eslabón más débil siempre puede ser el humano. Invertir en formación de tu equipo es la defensa más potente contra los ciberataques. No es culpa de nadie: es que el ataque está diseñado para engañar.

El Eslabón Humano

El 90% de los incidentes de ciberseguridad se originan por descuidos o falta de conocimiento del personal.

Formación Constante

Sesiones regulares y concisas que mantengan la ciberseguridad fresca en la mente de tus empleados.

Pruebas Prácticas

Entrena a tu equipo a reconocer y reportar intentos de phishing con ejercicios controlados y sin riesgos.

Cultura de Seguridad

Fomenta una mentalidad proactiva, donde cada empleado se siente parte activa de la protección de la empresa.

> **“La seguridad no se instala. Se entrena.”**

CAPA 6

Identidades y contraseñas

El control de accesos es la base de la ciberseguridad. En 2026, robar una contraseña no es solo un inconveniente; es un acceso directo a tu empresa.

Gestor Corporativo

Centraliza y organiza todas las credenciales, eliminando el caos de "post-its" y archivos inseguros (ya no más Excel con contraseña).

Contraseñas Robustas

Genera automáticamente claves únicas y complejas, minimizando el riesgo de ataques por fuerza bruta.

Compartición Segura

Permite compartir accesos de forma controlada y cifrada, sin exponer información sensible por canales no seguros.

Auditoría y Control

Supervisa quién tiene acceso a qué, asegurando que solo el personal autorizado maneje la información crítica.

> **“El ataque más rentable en 2026 sigue siendo robar credenciales.”**

Tu mínimo de seguridad 2026

Si te falta una sola capa, el ataque se convierte en una caída en cascada. Estos son los mínimos indispensables para proteger tu PYME este año:

Dispositivos EDR + parches	**Cloud** M365 o Google protegido
Backup Estrategia 3-2-1-0	**Firewall** Perimetral gestionado
Personas Formación y conciencia	**Identidades** Gestor de contraseñas

🎁 Autoevaluación rápida (5 min) Checklist Seguridad IT para PYMEs (2026)

En 5 minutos detectas si te falta alguna capa crítica en:

Endpoint · Cloud · Backup

Firewall · Usuarios · Contraseñas

Ideal si quieres revisarlo por tu cuenta, sin llamadas.

Descargar checklist GRATIS

🎯 Diagnóstico con experto (30 min) Auditoría Express de Seguridad IT

Te decimos exactamente:

✅ qué riesgo es urgente

✅ qué mínimo debes cerrar en 2026

✅ por dónde empezar sin malgastar presupuesto

Valorada en 99,50€ + IVA (Gratis solo asistentes del webinar hasta el 30/01/2026)

Reservar mi auditoría GRATIS

Si falla una capa, cae todo. Asegura el mínimo en 2026.