Claude Security para PYMEs: tu primera auditoría seria sin contratar una consultora

Subtítulo: Cómo saber exactamente qué vulnerabilidades tiene tu negocio hoy, sin gastar miles de euros ni necesitar un equipo técnico propio.

Hay una conversación que se repite constantemente en el mundo de la ciberseguridad para empresas. Va así: el responsable de una pyme sabe que debería revisar su seguridad. Lo ha oído, lo ha leído, incluso lo ha vivido de cerca cuando un cliente o proveedor ha sufrido un ataque. Pero cuando pide presupuesto a una consultora especializada, los números son desorbitados para su tamaño. Y así, la auditoría se convierte en algo que "ya haremos cuando tengamos más recursos".

El problema es que los atacantes no esperan.

En 2026, más del 60% de los ciberataques dirigidos tienen como objetivo empresas de menos de 250 empleados. No porque sean más rentables que un banco o una multinacional, sino porque son más accesibles. Tienen datos valiosos, manejan dinero real, están conectadas a cadenas de suministro de empresas más grandes, y casi ninguna ha hecho una revisión seria de su postura de seguridad. Son el eslabón más débil, y los actores maliciosos lo saben perfectamente.

La buena noticia —y es una noticia real, no un reclamo comercial— es que hoy existe una alternativa concreta. No perfecta, no sustituta de un equipo de seguridad dedicado, pero sí suficiente para conocer tu situación real y actuar con cabeza.

¿Qué empresa es candidata a hacer esto?

Antes de entrar en el cómo, es necesario ser honesto sobre el para quién.

Esta aproximación funciona bien si tu empresa cumple alguno de estos perfiles: tienes entre 5 y 150 empleados, manejas datos de clientes o información financiera, usas herramientas en la nube (correo, almacenamiento, software de gestión), has conectado sistemas propios a los de algún proveedor o cliente, o simplemente no tienes a nadie con dedicación exclusiva a ciberseguridad.

Si eres una empresa con regulación estricta del sector financiero o sanitario, o si manejas infraestructuras críticas, necesitarás ir más allá de lo que aquí se describe. Este proceso no es un sustituto de la normativa aplicable, ni de una auditoría formal para certificaciones. Es un punto de partida robusto para quien nunca ha tenido ninguno.

Qué obtienes con una auditoría asistida por IA

Lo primero es entender qué significa "auditoría" en este contexto. Una auditoría de ciberseguridad clásica implica que un equipo externo analiza tus sistemas, prueba tus defensas activamente e identifica vulnerabilidades técnicas concretas. Tiene un coste real porque requiere expertise, tiempo y responsabilidad profesional.

Lo que puedes hacer hoy con herramientas de IA como Claude no llega a ese nivel técnico, pero sí te proporciona algo que muchas pymes nunca han tenido: una visión estructurada de su superficie de ataque.

Concretamente, obtendrás un mapa de tus activos digitales críticos y quién tiene acceso a qué, una evaluación de tus políticas de contraseñas y gestión de accesos, una revisión de los vectores de entrada más comunes (correo, VPN, aplicaciones en la nube, proveedores), identificación de brechas en tus copias de seguridad y capacidad de recuperación, y un análisis de los riesgos de ingeniería social más probables para tu sector.

Lo que no obtendrás: análisis de vulnerabilidades técnicas en código propio, pruebas de penetración activas, certificación formal, ni garantías legales. Si alguno de esos puntos es imprescindible para ti, necesitas un profesional certificado. Si no, sigamos.

Mini protocolo de uso: cuándo escanear, cómo priorizar y cómo aplicar lo que encuentres

Fase 1: Inventario de activos (30–45 minutos)

El primer paso de cualquier análisis de seguridad es saber qué tienes. Suena obvio; muy pocas empresas lo han hecho de forma sistemática.

Crea una conversación con Claude y describe tu infraestructura: qué herramientas usáis, dónde está almacenada la información crítica, quién tiene acceso administrativo a qué sistemas, cuáles son vuestros proveedores digitales clave, y qué conexiones tenéis con sistemas externos (clientes, plataformas, integraciones). No necesitas saber los detalles técnicos. Describe el negocio como lo harías con un nuevo empleado.

A partir de esa descripción, puedes pedirle que identifique los activos de mayor riesgo y por qué. El resultado es sorprendente para la mayoría: hay conexiones, accesos y herramientas que se habían olvidado porque llevan meses funcionando "solos".

Fase 2: Análisis de vectores de entrada (45–60 minutos)

Los vectores de entrada son los caminos que un atacante podría usar para llegar a tu información. Los más frecuentes en pymes son el correo electrónico, las cuentas en servicios en la nube, las credenciales de empleados y extrabajadores, los accesos de proveedores, y los dispositivos personales que se usan para trabajar.

Para cada uno, puedes trabajar con Claude usando un esquema simple: ¿qué protección tienes actualmente? ¿Qué pasaría si fallara? ¿Cuánto tardaríais en detectarlo?

Este ejercicio no requiere conocimientos técnicos avanzados. Requiere honestidad. La mayoría de las vulnerabilidades que encontrarás no son técnicas; son organizativas. Accesos que no se han retirado. Contraseñas compartidas por comodidad. Empleados que no saben qué hacer si reciben un correo sospechoso.

Fase 3: Evaluación de exposición pública (15–20 minutos)

Hay información sobre tu empresa que está disponible públicamente y que puede ser usada por un atacante para preparar un engaño personalizado. Esto se llama OSINT (Open Source Intelligence), y los actores maliciosos lo usan de forma sistemática antes de lanzar cualquier ataque de ingeniería social.

Puedes pedirle a Claude que te ayude a mapear qué información tuya o de tu empresa es visible públicamente: cargos de empleados en LinkedIn, correos corporativos publicados en la web, nombres de herramientas que usáis, relaciones con clientes o proveedores que aparecen en notas de prensa o en redes sociales. El objetivo no es volverse paranoico; es conocer qué sabe ya un atacante antes de que os llame o os escriba.

Fase 4: Priorización y plan de acción (30 minutos)

Una vez tienes el mapa, el riesgo de paralizarse por abrumamiento es real. Hay demasiadas cosas que mejorar y no sabes por dónde empezar.

La forma correcta de priorizar en seguridad no es solucionar lo más fácil primero, sino lo que combina alta probabilidad de ocurrencia con alto impacto. Claude puede ayudarte a construir una matriz simple: para cada riesgo identificado, estimas la probabilidad (alta, media, baja) y el impacto si ocurre (crítico, significativo, menor). Lo que queda en la esquina de alta probabilidad y alto impacto es tu lista de prioridades reales.

En la práctica, para la mayoría de las pymes esta lista incluye: activar autenticación multifactor en correo y herramientas críticas, revisar y retirar accesos de exempicados y proveedores inactivos, establecer una política de copias de seguridad verificadas, y lanzar una sesión básica de concienciación con el equipo sobre phishing e ingeniería social.

Fase 5: Aplicación y seguimiento

El mayor error que cometen las empresas que hacen este tipo de revisiones es hacerlas una vez y no volver a ellas. La seguridad no es un estado que se alcanza; es un proceso que se mantiene.

Establece un ciclo regular: una revisión de este tipo cada trimestre, una revisión más ligera cada vez que incorporas un nuevo proveedor o herramienta, y una revisión específica si hay un incidente —aunque sea menor— o si un empleado abandona la empresa con acceso a sistemas críticos.

La ciberseguridad real no empieza en la tecnología

Hay una trampa conceptual en la que caen muchas empresas cuando empiezan a preocuparse por la seguridad digital: buscan una solución técnica para un problema que en gran parte es humano y organizativo.

Los ataques más eficaces contra pymes en 2026 no aprovechan vulnerabilidades técnicas sofisticadas. Aprovechan la confianza, la urgencia y la falta de protocolos internos. Un empleado que recibe un correo de "su proveedor habitual" pidiendo un cambio de cuenta bancaria. Una llamada a la recepción que parece del soporte técnico. Una factura que llega por el canal correcto pero con datos modificados.

Ninguna herramienta resuelve eso sola. Lo que sí funciona es que las personas de tu empresa entiendan el ecosistema en el que operan, sepan qué señales buscar y tengan un protocolo claro para verificar antes de actuar. Eso no requiere presupuesto. Requiere cultura.

Una auditoría asistida por IA es un buen primer paso porque te obliga a hacer explícito lo que suele ser implícito: quién tiene acceso a qué, qué pasaría si algo fallara, y cuánto tardaríais en saberlo. Ese ejercicio de claridad tiene valor independientemente de las herramientas que uses después.

Reflexión estratégica: el coste de no hacer nada

Cuando una empresa pequeña sufre un incidente de seguridad grave —un ransomware que bloquea sus sistemas, una brecha que expone datos de clientes, una transferencia fraudulenta que no se recupera— el daño raramente es solo económico. La pérdida de confianza de clientes, los plazos incumplidos, el tiempo del equipo absorbido por la gestión de la crisis y el coste reputacional se acumulan de formas que no siempre se monetizan fácilmente, pero que son muy reales.

El argumento de "somos muy pequeños para que nos ataquen" ha dejado de ser válido. El argumento de "no tenemos presupuesto para seguridad" se está erosionando rápidamente. Lo que queda es una decisión: actuar con lo que hay ahora, o esperar a que el coste de no haberlo hecho sea mucho mayor.

Una primera auditoría estructurada con herramientas de IA no te convierte en una empresa invulnerable. Pero sí te convierte en una empresa que conoce su situación, ha identificado sus riesgos más críticos y tiene un plan concreto para actuar. En el ecosistema digital de 2026, eso ya es una ventaja real.

Tu próximo paso

Esta semana puedes hacer algo concreto: reserva dos horas, reúne a las personas clave de tu empresa que gestionan herramientas digitales, y seguid las cinco fases de este protocolo. No necesitáis conocimientos técnicos. Necesitáis honestidad sobre cómo funcionáis realmente.

Si este artículo te ha dado un punto de partida, compártelo con alguien que lo necesite. Una pyme mejor preparada protege también a sus clientes y proveedores. Y eso, en la economía digital actual, importa a todos.

Visita el blog para acceder a más recursos gratuitos de ciberseguridad aplicada a empresas reales.

Isaac Ruiz Romero.