Ransomware en 2026: cuando enciendes el ordenador y todo ha desaparecido

La doble extorsión que arrodilla a pymes: cómo funciona, por qué nadie está a salvo y qué puedes hacer hoy

Son las 8:47 de un lunes. Marta enciende el ordenador en su gestoría de Bilbao. Lleva doce años construyendo ese negocio: clientes de confianza, contratos bien guardados, facturas de los últimos tres ejercicios fiscales. En la pantalla aparece un fondo rojo que no reconoce. Hay un texto en inglés y una cuenta atrás. Todos sus archivos tienen una extensión nueva que no existía el viernes. No puede abrirlos. No puede trabajar. No puede llamar a sus clientes para decirles que su información está… ¿dónde?

Esto no es una historia inventada para asustar. Es la variación de algo que en 2026 ocurre en España y en el resto de Europa con una frecuencia que los informes de ciberseguridad ya no miden en casos al año, sino en incidentes por día.

El ransomware ha dejado de ser un problema de grandes corporaciones. Se ha democratizado, y no precisamente en el buen sentido.

¿Qué es exactamente el ransomware?

La palabra viene de *ransom*, que en inglés significa rescate. Un ransomware es un programa malicioso que, una vez dentro de tu sistema, cifra todos tus archivos. Los bloquea con una clave que solo tiene quien te atacó. A partir de ese momento, tus datos siguen estando ahí, en el disco duro, pero son completamente ilegibles. Es como si alguien hubiera cambiado todos los candados de tu archivo físico y se hubiera llevado las llaves.

El mensaje que aparece en pantalla es siempre una variación del mismo: paga una cantidad en criptomoneda antes de que expire el tiempo, y te devuelvo el acceso. No pagues, y pierdes todo para siempre.

Durante años, el debate era sencillo: ¿pago o no pago? Hoy esa pregunta ya no es suficiente, porque el ransomware de 2026 ha mutado hacia algo bastante más sofisticado y bastante más dañino.

La doble extorsión: el giro que lo cambia todo

Lo que convierte al ransomware moderno en una amenaza de otra dimensión no es solo el cifrado. Es lo que ocurre **antes** del cifrado.

Los grupos criminales que operan estos ataques, muchos de ellos organizados como empresas con estructura jerárquica, divisiones técnicas y hasta "atención al cliente", han incorporado una fase que los profesionales de ciberseguridad llaman **doble extorsión**. Antes de bloquear tus archivos, los copian. Los filtran hacia sus propios servidores. Con calma, en silencio, a veces durante semanas.

Cuando finalmente activan el cifrado y aparece la pantalla roja, ya tienen lo tuyo. Y entonces el mensaje no dice solo "paga o pierdes el acceso". Dice: **"Paga, o publicamos tus datos en Internet"**.

Para Marta, esto significa que sus clientes —personas con su información fiscal, sus nóminas, sus declaraciones de la renta— pueden ver esos datos expuestos públicamente. O peor, pueden ser utilizados para otros ataques. El daño ya no es solo operativo. Es reputacional, legal y humano.

La doble extorsión ha transformado el ransomware en algo mucho más parecido a una extorsión clásica que a un problema informático. Y eso lo hace incomparablemente más difícil de ignorar.

Cómo entra el ransomware en tu empresa

La pregunta que siempre surge es: ¿cómo llegan hasta ahí dentro? La respuesta suele ser decepcionantemente sencilla.

En la mayoría de los casos documentados en 2025 y 2026, el punto de entrada es un correo electrónico con un archivo adjunto. Una factura que alguien esperaba, un presupuesto, un documento de Word con "instrucciones para abrir". Basta con que una persona lo abra en el ordenador equivocado. A partir de ahí, el programa se instala solo, busca la manera de propagarse por la red interna y espera el momento para actuar.

En otros casos, el acceso llega a través de contraseñas comprometidas. Una persona reutiliza la misma contraseña en varios servicios; uno de esos servicios sufre una brecha; esa contraseña acaba a la venta en foros de la internet oscura; un atacante la compra y la usa para entrar al sistema de gestión de la empresa. Todo ello sin que nadie en la organización haya cometido un error evidente.

También ocurre a través de vulnerabilidades en programas sin actualizar. Un software de contabilidad antiguo, un sistema operativo que no ha recibido parches de seguridad en meses. Las empresas criminales tienen escáneres automáticos que rastrean internet buscando exactamente estas puertas abiertas.

Lo relevante aquí es que ninguno de estos vectores requiere que tú seas descuidado en el sentido tradicional. Requiere que seas humano, que tengas recursos limitados y que, como la mayoría de los negocios pequeños, no tengas un equipo de ciberseguridad dedicado.

Por qué las pymes son el objetivo preferido

Existe un error de percepción muy extendido: creer que los ataques de ransomware apuntan a grandes corporaciones porque ahí hay más dinero. La realidad del ecosistema criminal en 2026 es más matizada.

Las grandes empresas tienen equipos de respuesta a incidentes, sistemas de detección avanzados y procedimientos de recuperación. Son objetivos jugosos pero costosos de atacar. Las pequeñas y medianas empresas, en cambio, ofrecen algo que los atacantes valoran enormemente: **una relación favorable entre el esfuerzo invertido y el beneficio obtenido**.

Una pyme de diez empleados puede tener datos de cientos de clientes, contratos de alto valor, información financiera sensible, y probablemente ningún protocolo de seguridad definido. El rescate que puede pagar es menor que el de una multinacional, sí, pero el coste del ataque también es mucho menor. Y cuando operas a escala industrial, atacando decenas de empresas al día de forma automatizada, los números cuadran.

Además, las pymes tienen algo que los atacantes han aprendido a explotar: la dependencia crítica de sus datos. Para una consultoría, una clínica dental, una agencia de viajes o una gestoría, perder el acceso a los archivos durante 48 horas no es un inconveniente gestionable. Es el fin del negocio en el horizonte inmediato.

La respuesta real: las copias de seguridad como estrategia, no como tarea pendiente

Aquí es donde la mayoría de los artículos sobre ransomware cometen un error de comunicación. Mencionan las copias de seguridad como si fueran un consejo de higiene digital básico, algo que todos sabemos que deberíamos hacer y que pocos hacemos bien. Lo dicen, lo marcan en la lista y pasan al siguiente punto.

Pero si hay una sola idea que deberías llevarte de este artículo, es esta: **una copia de seguridad bien configurada es la única defensa real frente al ransomware**. No la única capa de protección, sino la única que, cuando todo lo demás ha fallado, te permite levantarte.

Y cuando digo bien configurada, hay tres condiciones que deben cumplirse:

Primera: la copia debe ser reciente. Una copia de seguridad de hace seis meses no es una solución; es perder seis meses de trabajo. Las copias deben realizarse con una frecuencia acorde al ritmo real del negocio. Para muchas empresas, eso significa diaria.

Segunda: la copia debe estar desconectada. Aquí está el error más común. Muchas empresas hacen copias de seguridad en un disco externo que está permanentemente conectado al ordenador, o en una unidad de red siempre accesible. Cuando el ransomware cifra el sistema, cifra también esas copias. La copia de seguridad útil es la que el ransomware no puede alcanzar: un disco que se conecta solo en el momento de la copia y luego se guarda en otro lugar, o un servicio de nube configurado con acceso restringido.

Tercera: la copia debe haberse probado. Una copia de seguridad que nunca se ha restaurado es una promesa sin verificar. El día que la necesitas no es el momento para descubrir que el proceso de recuperación falla, que faltan archivos o que el sistema no es compatible. Las copias deben probarse periódicamente.

Si Marta hubiera tenido una copia de seguridad de sus archivos de la semana anterior, almacenada en un disco externo no conectado habitualmente, la historia habría tenido otro final. No uno sin daño —el tiempo perdido, el estrés, la investigación posterior— pero sí sin el desastre total.

Lo que no te dice el rescate: pagar no garantiza nada

Es importante decirlo con claridad porque muchos negocios, en el pánico del momento, lo consideran: **pagar el rescate no garantiza recuperar los datos**. Los informes del sector indican que un porcentaje significativo de quienes pagan no reciben la clave de descifrado, o reciben una que no funciona correctamente, o recuperan los datos pero vuelven a ser atacados semanas después porque el acceso original nunca fue cerrado.

Además, pagar alimenta el modelo de negocio. Cada pago confirma a estos grupos que el ransomware funciona y merece la pena escalar. Es una decisión que tiene consecuencias que van más allá de la empresa individual.

Reflexión final: la ciberseguridad como cultura del negocio

El ransomware no es un problema técnico que se resuelve comprando software. Es un problema estructural que requiere una forma diferente de pensar sobre la información de tu negocio.

Los datos que gestionas —de tus clientes, de tus empleados, de tus procesos— tienen valor. Tienen valor para ti y, lamentablemente, tienen valor para otros. Tratarlos como el activo que son, con los mismos criterios con los que proteges el dinero en caja o los documentos en papel, es el cambio de mentalidad que marca la diferencia.

Esto no requiere ser experto en tecnología. Requiere entender qué información tienes, dónde está, quién puede acceder a ella y qué ocurriría si mañana no estuviera disponible. A partir de esa claridad, las decisiones prácticas —la copia de seguridad, la actualización del sistema, la formación de tu equipo— dejan de ser tareas pendientes y se convierten en parte natural de cómo gestionas tu negocio.

Marta, por cierto, tuvo que reconstruir tres meses de trabajo desde cero. Recuperó algunos documentos gracias a copias antiguas dispersas y a la memoria de sus empleados. El cliente más afectado tardó mucho tiempo en volver a confiar en ella plenamente. El coste real del ataque, calculando tiempo perdido, horas de consultoría técnica y el impacto reputacional, multiplicó por diez el rescate que le pedían.

No hace falta que eso le pase a tu negocio para tomar nota.

Si este artículo te ha hecho pensar en algo que tienes pendiente, ese pensamiento vale más que cualquier artículo. Compártelo con quien lleva un negocio, con quien gestiona la información de otros. Una persona informada toma mejores decisiones, y eso en ciberseguridad se traduce en daños que no ocurren. Visita el blog para acceder a más recursos gratuitos sobre seguridad digital aplicada.

Isaac Ruiz Romero.