Lo que realmente preocupa a los emprendedores cuando hablas de ciberseguridad

Por qué tu empresa es un objetivo (aunque creas que no)

Cuando pregunto a empresarios sobre ciberseguridad, la mayoría me responde lo mismo: "Yo no soy una multinacional, ¿quién va a atacarme?". Esta creencia es exactamente lo que los ciberdelincuentes aprovechan. No buscan grandes empresas con sistemas de seguridad robustos. Buscan el eslabón más débil: pequeñas y medianas empresas que creen estar fuera del radar.

La realidad es contundente. En 2025, las empresas enfrentan una media de **1.925 ciberataques semanales**, un incremento del 47% respecto al año anterior. Y España no está exenta. Desde universidades en Baleares hasta ING y Santander, pasando por El Corte Inglés y Mango, ningún sector ni tamaño de empresa queda fuera de esta amenaza creciente.

El correo que todos hemos recibido (y algunos han clicado)

"Hola, en ING queremos estar cerca de ti y poder ofrecerte un servicio cada día mejor. Para ello, es necesario que actualices tus datos personales..."

¿Te suena familiar? Este tipo de mensajes no son casuales. Son el resultado de operaciones de **phishing** cada vez más sofisticadas que estudian nuestro comportamiento, nuestras marcas de confianza y nuestros miedos.

El phishing sigue siendo la puerta de entrada más común a los sistemas empresariales. En 2025, los atacantes han incorporado inteligencia artificial para generar voces falsas y realizar estafas telefónicas (vishing) prácticamente indetectables. Ya no se trata solo de correos mal redactados con errores ortográficos. Ahora recibimos mensajes perfectamente elaborados, con el tono exacto de nuestra entidad bancaria, proveedor de servicios o incluso compañeros de trabajo.

Lo preocupante no es solo la técnica. Es que funcionan. Porque apelan a algo muy humano: la urgencia, el miedo a perder el acceso a algo importante, la confianza en marcas conocidas.

Cuando el ataque viene de donde menos lo esperas

Hablemos de algo que muchos emprendedores ni siquiera consideran: **los ataques a la cadena de suministro**. En marzo de 2025, El Corte Inglés sufrió una brecha de seguridad que expuso datos de clientes. Pero no fue un ataque directo a sus sistemas. El punto de entrada fue un proveedor externo con medidas de seguridad menos estrictas.

Esta es la nueva frontera de los ciberataques. Los delincuentes saben que atacar directamente a una gran empresa es complicado. Pero esa misma empresa trabaja con decenas de proveedores, subcontratas, sistemas externos... y solo hace falta que uno de ellos tenga una vulnerabilidad.

Para las pymes, esto tiene dos implicaciones críticas:

Primera: Tu empresa puede ser el vector de ataque hacia un cliente más grande. Imagina las consecuencias legales, reputacionales y económicas de ser identificado como el origen de una brecha de seguridad en uno de tus principales clientes.

Segunda: Tus propios proveedores pueden ser el punto débil. Esa aplicación de facturación que contratas, el sistema de nóminas en la nube, el CRM que usas... cada integración es una puerta potencial.

El secuestro digital que paraliza empresas enteras

Si hay una amenaza que realmente aterra a los empresarios cuando la comprenden, es el **ransomware**. Y con razón. El ransomware ha experimentado un aumento del 120% en 2025.

El escenario es simple y devastador: llegas un lunes por la mañana, enciendes tu ordenador, e intentas acceder a tus archivos. No puedes. Una pantalla te informa que toda tu información ha sido cifrada y que tienes 48 horas para pagar un rescate o perderás todo para siempre.

No hablamos de cantidades simbólicas. Las pérdidas para pymes oscilan entre 2.500 y 60.000 euros. Para grandes compañías, la media supera los 5,5 millones de euros. Pero el dinero no es lo único que se pierde. Está el tiempo de inactividad, los clientes que no puedes atender, la confianza deteriorada, los contratos incumplidos.

El Ayuntamiento de Badajoz lo sufrió en abril de 2025. Sistemas paralizados. Servicios ciudadanos interrumpidos. Caos operativo. Y la pregunta que todos los empresarios me hacen: "¿Hay que pagar el rescate?". La respuesta nunca es sencilla, pero la mejor estrategia siempre es la prevención.

Más allá del "instala un antivirus"

Cuando hablo con empresarios, muchos me dicen: "Ya tengo un antivirus". Y es un buen primer paso. Pero es como tener solo un candado en la puerta de casa cuando vives en una zona con índices de criminalidad crecientes.

La protección real en 2025 requiere un enfoque multicapa:

Formación continua del equipo. El 90% de los ciberataques exitosos empiezan con un error humano. Un clic en el enlace equivocado. Una contraseña compartida. Un empleado que trabaja desde una red wifi pública sin VPN. Capacitar a tu equipo no es un gasto, es la inversión más rentable en seguridad.

Actualización sistemática. Cada software desactualizado es una vulnerabilidad conocida y documentada. Los atacantes no necesitan ser genios. Simplemente escanean internet buscando sistemas sin actualizar y explotan fallos ya corregidos por los fabricantes.

Copias de seguridad reales. "Tengo copias de seguridad" es muy diferente a "He probado recuperar información desde mis copias de seguridad". He visto empresas con backups que llevan meses sin ejecutarse correctamente, o copias almacenadas en el mismo servidor que los datos originales, vulnerables al mismo ataque.

Evaluación de proveedores. Si trabajas con proveedores externos que acceden a tus sistemas, necesitas saber qué medidas de seguridad tienen. Un contrato firmado no protege tus datos si su infraestructura es vulnerable.

Las soluciones que realmente marcan la diferencia

Más allá de las medidas básicas, hay dos enfoques que están transformando la ciberseguridad empresarial en 2025:

Pentesting: Encuentra tus vulnerabilidades antes que los atacantes. El pentesting (test de penetración) consiste en contratar a expertos en seguridad para que intenten hackear tus sistemas de forma controlada. Es como contratar a un ladrón reformado para que te muestre todas las formas en las que podrían entrar a tu casa. Suena radical, pero es extraordinariamente efectivo. Identificas puntos débiles reales, no teóricos, y puedes corregirlos antes de que alguien los explote con malas intenciones.

DaaS (Device as a Service): Seguridad desde el hardware. El modelo DaaS centraliza la gestión de todos los dispositivos de la empresa. Cada portátil, cada móvil, cada tablet se gestiona, actualiza y protege desde una plataforma única. Si un empleado pierde un dispositivo, puedes borrarlo remotamente. Si detectas actividad sospechosa, puedes aislarlo de la red. Es seguridad integrada desde el primer día.

La conversación incómoda que debes tener

Hay una pregunta que ningún empresario quiere hacerse: "¿Qué pasaría si mañana perdemos acceso a todos nuestros sistemas?". Es incómoda porque las respuestas suelen ser alarmantes:

- ¿Cuánto tiempo podríamos seguir operando?
- ¿Qué clientes se verían afectados inmediatamente?
- ¿Tenemos los contactos y documentos críticos en formato físico o alternativo?
- ¿Cuál sería el impacto financiero del primer día? ¿De la primera semana?

Esta conversación incómoda es el primer paso hacia una estrategia de ciberseguridad real. Porque solo cuando comprendes lo vulnerable que es tu operación actual, empiezas a priorizar su protección.

El verdadero coste de no actuar

Un empresario me dijo una vez: "Es que la ciberseguridad es cara". Le respondí con una pregunta: "¿Más cara que perder tu negocio?".

Porque eso es lo que está en juego. No es solo el coste directo del rescate o la recuperación de sistemas. Es la pérdida de confianza de clientes que te confiaron sus datos. Es el impacto reputacional de aparecer en las noticias como la empresa que sufrió una brecha. Son las sanciones legales por incumplimiento de normativas de protección de datos. Es el tiempo que tú y tu equipo dedicaréis a gestionar la crisis en lugar de hacer crecer el negocio.

Las amenazas digitales son más sofisticadas y frecuentes cada año. La ciberseguridad no puede ser un "ya lo veremos". Debe ser parte del ADN operativo de cualquier empresa que quiera seguir siendo viable en los próximos años.

Por dónde empezar hoy mismo

No necesitas convertirte en un experto en ciberseguridad. Pero sí necesitas entender que es parte fundamental de tu responsabilidad como empresario. Igual que cuidas las finanzas, los recursos humanos o la calidad del producto, la seguridad digital requiere atención, recursos y estrategia.

Si hay algo que he aprendido formando a emprendedores y empresas en estos temas, es que la concienciación es el 80% del trabajo. El otro 20% son medidas técnicas que, una vez comprendes su importancia, son relativamente sencillas de implementar.

La pregunta no es si tu empresa será atacada. La pregunta es cuándo, y si estarás preparado cuando ocurra.

Isaac Ruiz Romero.