Descubre las 5 amenazas tecnológicas que más impactan a las pymes gallegas y cómo protegerte hoy mismo

Guía práctica de ciberseguridad sin rodeos ni tecnicismos absurdos para empresas que quieren dormir tranquilas.

Informe de Consultoría Técnica y Estratégica
Año 2026

Introducción: El día a día de una PYME en Galicia

¡Buenas! Si estás leyendo esto, probablemente seas el dueño, gerente o el que se encarga de que todo funcione en una pyme aquí, en Galicia. Y seamos sinceros: bastantes dolores de cabeza tienes ya con sacar el trabajo adelante, lidiar con los proveedores, pagar las facturas a tiempo y cruzar los dedos para que la campaña del mes salga bien como para que encima venga un listo a hablarte de términos raros en inglés sobre 'ciberseguridad'.

Pero aquí está el problema: los malos ya no solo atacan a las multinacionales de Wall Street o a los ministerios en Madrid. Van a por la gestoría de Santiago, el taller de Vigo, la bodega de las Rías Baixas o la fábrica de muebles de la provincia de Lugo. ¿Por qué? Porque saben que las pymes gallegas suelen estar tan centradas en producir que dejan la puerta digital abierta de par en par.

Como experto en ciberseguridad, mi trabajo no es meterte miedo ni venderte soluciones millonarias que no necesitas. Mi trabajo es hablarte claro, 'en cristiano'. En este documento vamos a repasar, sin rodeos, los 5 agujeros negros de seguridad que más empresas se están llevando por delante en nuestra tierra y cómo puedes taparlos hoy mismo sin dejarte el presupuesto de todo el año.

1. Ciberataques de ransomware dirigidos a pymes

Imagínate llegar a la oficina un lunes por la mañana, encender el ordenador para repasar los pedidos de la semana y encontrarte con que todos tus archivos tienen un icono raro y no abren. En su lugar, aparece una pantalla en rojo con un texto que dice algo así como: 'Hemos cifrado todos tus datos. Si quieres recuperarlos, páganos 20.000 euros en Bitcoins antes de 48 horas. Si avisas a la policía, los borramos para siempre'.

Eso, amigo mío, es el ransomware. Es el equivalente digital a que entren en tu local de noche, metan todos tus papeles, facturas, planos y ficheros de clientes en una caja fuerte blindada que han traído ellos, le echen la llave y te cobren un rescate por darte la combinación.

¿Por qué te afecta a ti?

Los ciberdelincuentes usan sistemas automáticos que rastrean internet buscando cualquier red desprotegida. No es que tengan algo personal contra tu empresa; simplemente han visto una debilidad y se han colado. Si caes en esto, tu negocio se detiene al 100%. No puedes facturar, no puedes consultar los datos de los clientes, ni siquiera puedes saber qué tienes en el almacén.

> 🛠️ **Tu Plan de Acción Inmediato:**
> • Sentido común con el email: El 90% del ransomware entra por un correo electrónico falso (phishing). Si te llega una factura de un proveedor que no te cuadra, o un aviso urgente de Correos con un archivo adjunto raro... ¡No hagas clic!
> • Desconfía por defecto: Confirma las cosas por teléfono con el proveedor si el correo te huele un poco raro. Vale más perder un minuto llamando que una semana con la empresa parada.

2. Pérdida de datos sin backup en la nube

Siguiendo el hilo de lo anterior... ¿sabes cuál es la única forma real y 100% efectiva de mandar a paseo a un extorsionador de ransomware? Decirle: 'Quédate con los archivos, que tengo una copia de seguridad impecable hecha de anoche'. El problema es que la mayoría de pymes gallegas cree que tiene copias de seguridad, pero en realidad tiene 'simulacros'.

Tener un disco duro portátil de 50 euros enchufado todo el día por USB al servidor de la oficina NO es una copia de seguridad segura. Si entra un virus en el servidor, lo primero que va a hacer es saltar por ese cable USB y romper también el disco de copia. Y si hay un incendio, una inundación o roban en la oficina, te quedas sin ordenador y sin disco duro.

La importancia del backup 'en la nube' y desconectado

Una copia de seguridad moderna debe seguir la regla del 3-2-1: tres copias de tus datos, en dos soportes diferentes, y al menos una de ellas fuera de tu oficina (en la nube). El almacenamiento en la nube hoy en día es baratísimo y automático. Se hace por la noche mientras duermes y, lo más importante, está aislada de lo que ocurra físicamente en tu local.

> 🛠️ **Tu Plan de Acción Inmediato:**
> • Contrata un servicio de backup gestionado en la nube: Asegúrate de que los datos se guarden de forma cifrada en la nube.
> • Haz la prueba del algodón: Una vez al mes, pídele a tu informático que recupere un archivo aleatorio de hace dos semanas. Sorprende la cantidad de empresas que descubren que su sistema de copia fallaba justo el día que lo necesitan.

3. Redes WiFi corporativas sin segmentación

Imagínate esta escena que pasa todos los días en Galicia: llega un cliente o un proveedor a visitarte a la oficina, se sienta contigo a tomar un café y te dice: 'Oye, ¿me das la clave de la WiFi para mirar una cosilla del móvil?'. Y tú, con toda la amabilidad del mundo, le señalas un posit pegado en la pantalla del ordenador donde pone 'Galicia2026*'.

Felicidades, le acabas de dar la llave de tu casa al cartero. Al meter a un invitado en tu misma red WiFi corporativa, ese móvil (que vete tú a saber qué virus o aplicaciones sospechosas tiene instaladas) ahora puede 'ver' y conectarse con los ordenadores de administración, el ordenador donde se hacen las facturas y el servidor central de la empresa.

¿Qué es la segmentación de red?

No se trata de prohibirle internet a las visitas, sino de separar los caminos. Segmentar la red es tan simple como configurar tu router para que emita dos señales WiFi diferentes. Una llamada 'MiEmpresa_Interna' (oculta, súper protegida y solo para tus equipos informáticos) y otra llamada 'MiEmpresa_Invitados' (para clientes, que solo sirve para navegar por internet pero bloquea por completo el acceso a tus ordenadores internos).

> 🛠️ **Tu Plan de Acción Inmediato:**
> • Llama a tu proveedor de internet o técnico informático: Pídeles que activen de inmediato la 'Red de Invitados' en el router.
> • Separa el trabajo del ocio: No dejes que los teléfonos personales de los empleados se conecten a la misma WiFi donde guardas las nóminas y las cuentas.

4. Software sin licencia y sin actualizaciones

Lo sé, las licencias de software a veces son caras y da rabia pagar todos los meses por programas que usas de forma secundaria. Es muy tentador bajarse una versión 'pirata' o 'crackeada' de internet, o simplemente dejar ese Windows 7 antiguo funcionando en el ordenador del almacén porque 'mientras no falle, para qué lo vamos a tocar'.

Esto es el equivalente a dejar las persianas de tu negocio de madera vieja y medio podridas. Los fabricantes de software (como Microsoft, Adobe, etc.) descubren constantemente fallos y debilidades en sus programas. Cuando se dan cuenta, sacan un parche (una actualización) que tapa ese agujero. Si tu software es pirata o es tan viejo que ya no tiene soporte, el agujero se queda ahí para siempre.

El peligro oculto de los 'cracks'

Nadie regala nada en internet. Esos programas que te bajas gratis y que vienen con un 'activador' para saltarse la licencia suelen traer un regalo envenenado dentro. El activador abre las puertas de tu sistema a los delincuentes a cambio de ahorrarte unos pocos euros en la licencia oficial. A la larga, sale infinitamente más caro.

> 🛠️ **Tu Plan de Acción Inmediato:**
> • Activa las actualizaciones automáticas: En todos los Windows y aplicaciones de la oficina. Que se actualicen por la noche.
> • Pásate al modelo de suscripción si es necesario: Herramientas como Microsoft 365 o Google Workspace garantizan que siempre uses la última versión segura sin que tengas que estar pendiente de comprar licencias nuevas cada pocos años.

5. Falta de plan de recuperación ante desastres

Llegamos al último punto y el más estratégico. Si sufres un ataque informático grave o un desastre físico en tus instalaciones, la pregunta clave no es solo '¿tengo copia de seguridad?', sino: **¿Cuánto tiempo tardo en volver a levantar la persiana y seguir vendiendo?**

Muchas empresas asumen que si pasa algo, llaman al técnico de confianza, este reinstala todo y en un par de horas están funcionando. Siento decirte que, en el mundo real, no funciona así. Si no hay una estrategia definida por escrito (un Plan de Recuperación ante Desastres), reinstalar los sistemas, recuperar los gigas y gigas de datos de la nube, volver a configurar los correos y las contraseñas puede llevarte **días enteros o incluso semanas**.

¿Qué es un Plan de Recuperación (DRP)?

No hace falta que sea un manual de 300 páginas. Para una pyme gallega, basta con un documento sencillo de dos hojas que responda claramente a tres preguntas en un momento de pánico generalizado:

1. ¿Quién hace qué si la red se cae por completo?
2. ¿Qué sistemas son prioritarios para que el negocio siga facturando (ej: primero el TPV o la web de pedidos, luego el correo interno)?
3. ¿Dónde están guardadas las contraseñas maestras y las copias de seguridad?

> 🛠️ **Tu Plan de Acción Inmediato:**
> • Redacta tu 'Guía de Emergencia': Escribe en un documento básico los teléfonos del soporte informático, los números de póliza del seguro de ciberriesgo (si tienes) y los pasos clave para restaurar el negocio.
> • Guarda una copia impresa: Sí, en papel, guardada en un cajón bajo llave. Si los ordenadores se rompen, no podrás leer un PDF guardado en el escritorio del ordenador central.

Conclusión: Tu seguridad empieza hoy mismo

Como habrás visto, proteger tu negocio aquí en Galicia no requiere que te conviertas en un ingeniero de la NASA ni que inviertas miles de euros al mes. La ciberseguridad profesional es, en un 80%, pura rutina, sentido común y orden organizativo.

Aplica estos cinco puntos paso a paso. No intentes cambiarlos todos esta tarde; empieza esta semana llamando a tu informático para revisar la WiFi y las actualizaciones, y la semana que viene te pones con las copias de seguridad en la nube. Tu tranquilidad de cara al futuro y la continuidad de tu pyme bien valen ese pequeño esfuerzo.

¿Quieres que seamos tu informático de confianza?

Si prefieres centrarte en hacer crecer tu negocio y dejar la seguridad de tus sistemas en manos de profesionales expertos y cercanos, en IAFIDI Informática estamos listos para ayudarte. Contáctanos hoy mismo y blindemos tu pyme juntos.

IAFIDI Informática

Galerías Verxeles 3-5, Viveiro (Lugo)

+34 982 56 25 29 | +34 670 03 56 36

iafidi@iafidi.com