CIBERSEGUROS

RESUMEN EJECUTIVO

# Ciberseguridad para la pyme verano 2026

*Por qué las vacaciones son la temporada alta del cibercrimen*

**La ciberseguridad ha dejado de ser un asunto de grandes corporaciones.** En España, donde más del 99 % del tejido empresarial son pymes, el problema afecta a casi todos los negocios. Y los datos confirman que la amenaza crece sin pausa: durante 2025, INCIBE gestionó 122.223 incidentes, un 26 % más que el año anterior.

Este resumen condensa las conclusiones del informe completo: cuál es el estado real de la amenaza, por qué el verano multiplica el riesgo, cómo la nueva regulación NIS2 puede afectar a su negocio y qué medidas concretas marcan la diferencia.

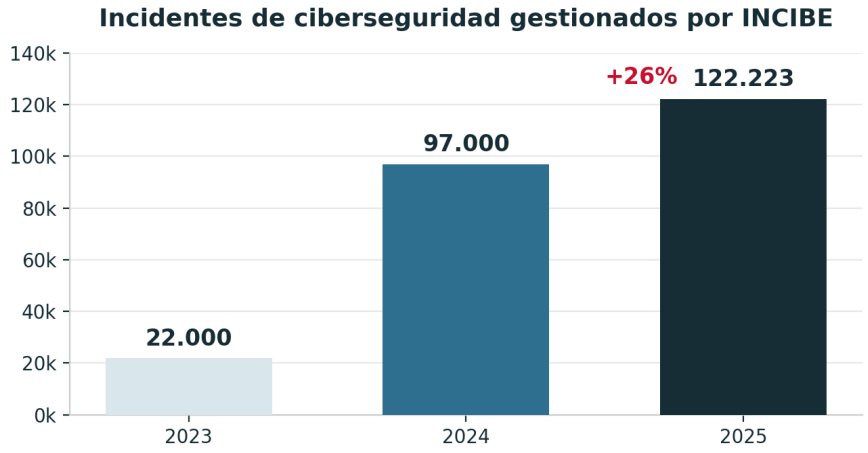
**+26 %**
más incidentes en 2025 (INCIBE)

**60 %**
de pymes atacadas cierran en 6 meses

**~30 %**
de los ataques se concentran en verano

## Una amenaza que se dispara cada año

El volumen de incidentes gestionados se ha multiplicado por más de cinco desde 2023. No es un pico puntual, sino una tendencia sostenida que ya forma parte del día a día de las empresas.




*Fuente: balances anuales de INCIBE.*

## El verano: cuando bajan las defensas

Existe una creencia tan extendida como falsa: que en verano «no pasa nada». Los ciberdelincuentes piensan lo contrario. **Para ellos, julio y agosto son temporada alta**, porque las defensas de las empresas bajan justo cuando ellos aprietan.

- **Plantillas reducidas:** menos personas vigilando los sistemas y detectando anomalías a tiempo.
- **Funciones críticas delegadas:** sustitutos con permisos elevados pero poca formación en seguridad.
- **Más trabajo en remoto:** conexiones desde redes wifi de hoteles o segundas residencias, a menudo inseguras.
- **Procesos relajados:** las verificaciones internas se saltan más fácilmente por las prisas y las ausencias.

> **El dato que lo resume todo**
>
> Entre las empresas atacadas en verano, el **62 % tardó más de tres días** en detectar la intrusión.
>
> Tres días en los que el atacante actúa con total libertad. Y el sector turístico concentró cerca del 70 % de los ataques del verano de 2025.

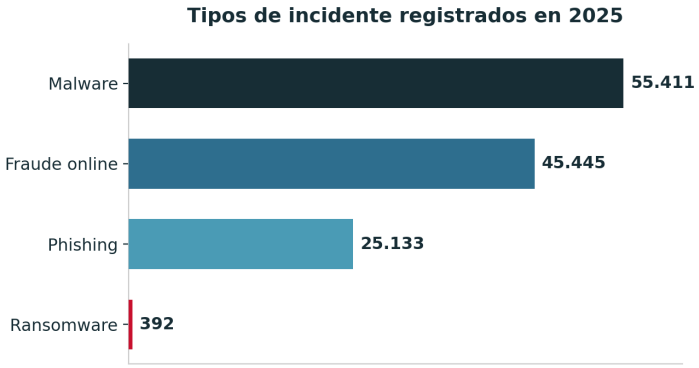
## NIS2: la seguridad ya es un requisito comercial

La nueva regulación europea de ciberseguridad (NIS2) obliga a las empresas grandes y medianas a **vigilar la seguridad de sus proveedores**. Aunque su pyme no esté directamente obligada, el efecto llega por la cadena de suministro.

> **Qué significa esto para su negocio**
>
> Cada vez más clientes exigen por contrato medidas de seguridad, cuestionarios y certificaciones como condición para seguir trabajando.
>
> Quien cumpla, **mantendrá y ganará contratos**; quien no, quedará fuera de concursos y licitaciones.

### No todos los ataques son iguales

El malware y el fraude online concentran la mayoría de los casos. El ransomware, mucho menos frecuente, es de los más destructivos: puede dejar una empresa sin acceso a su información durante días.




*Fuente: balance de ciberseguridad 2025 de INCIBE.*

## Protegerse es más fácil de lo que parece

La inmensa mayoría de los ataques se evitan con medidas sencillas y constancia. El informe desarrolla un decálogo práctico; estos son sus diez puntos:

1. Verificación en dos pasos
2. Forma a tu equipo
3. Ojo con correos sospechosos
4. Todo actualizado y legal
5. Contraseñas robustas
6. Permisos al mínimo
7. Copias de seguridad
8. Conexiones remotas seguras
9. Plan de respuesta
10. Revisa proveedores y NIS2

### Y cuatro básicos imprescindibles

La base sobre la que se construye todo lo demás. Ningún negocio debería operar sin ellos:

| | |
|---|---|
| 1 | **Software legal y actualizado.** Cada actualización cierra una puerta que los atacantes ya conocen. |
| 2 | **Copias de seguridad.** La única defensa que funciona con garantías frente al secuestro de datos. |
| 3 | **Herramienta antimalware.** Vigilancia permanente que bloquea las amenazas antes de que causen daño. |
| 4 | **Un ciberseguro.** La red de protección financiera cuando, pese a todo, algo falla. |