



OCTUBRE | MES DE LA CIBERSEGURIDAD

Ciberamenazas en la empresa: cómo reconocerlas y reducir su impacto

Un entorno digital con más puntos de exposición

Las empresas dependen de **más aplicaciones, servicios en la nube, dispositivos e identidades digitales**. Cada conexión facilita el trabajo, pero también puede abrir una vía de ataque si no se gestiona adecuadamente.

Los métodos conocidos siguen presentes: engañar a una persona, aprovechar un fallo o utilizar una cuenta comprometida. Lo que ha cambiado es la **capacidad para combinar técnicas, automatizar ataques y crear mensajes más convincentes con ayuda de la IA**. Por eso, protegerse exige conocer tanto las formas de acceso como sus posibles consecuencias.

Señales de alerta en tu entorno digital



Una petición que rompe la rutina

Alguien solicita con urgencia una transferencia, una contraseña o un cambio en los datos de pago.



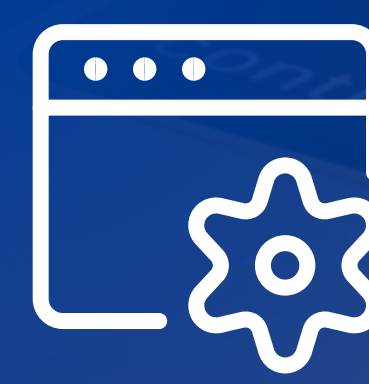
Un acceso que no reconoces

Aparece un inicio de sesión, un dispositivo nuevo o actividad inesperada en una cuenta.



Un servicio que cambia de comportamiento

Una aplicación deja de responder, se vuelve muy lenta o los archivos dejan de estar disponibles.



Un sistema expuesto sin protección actualizada

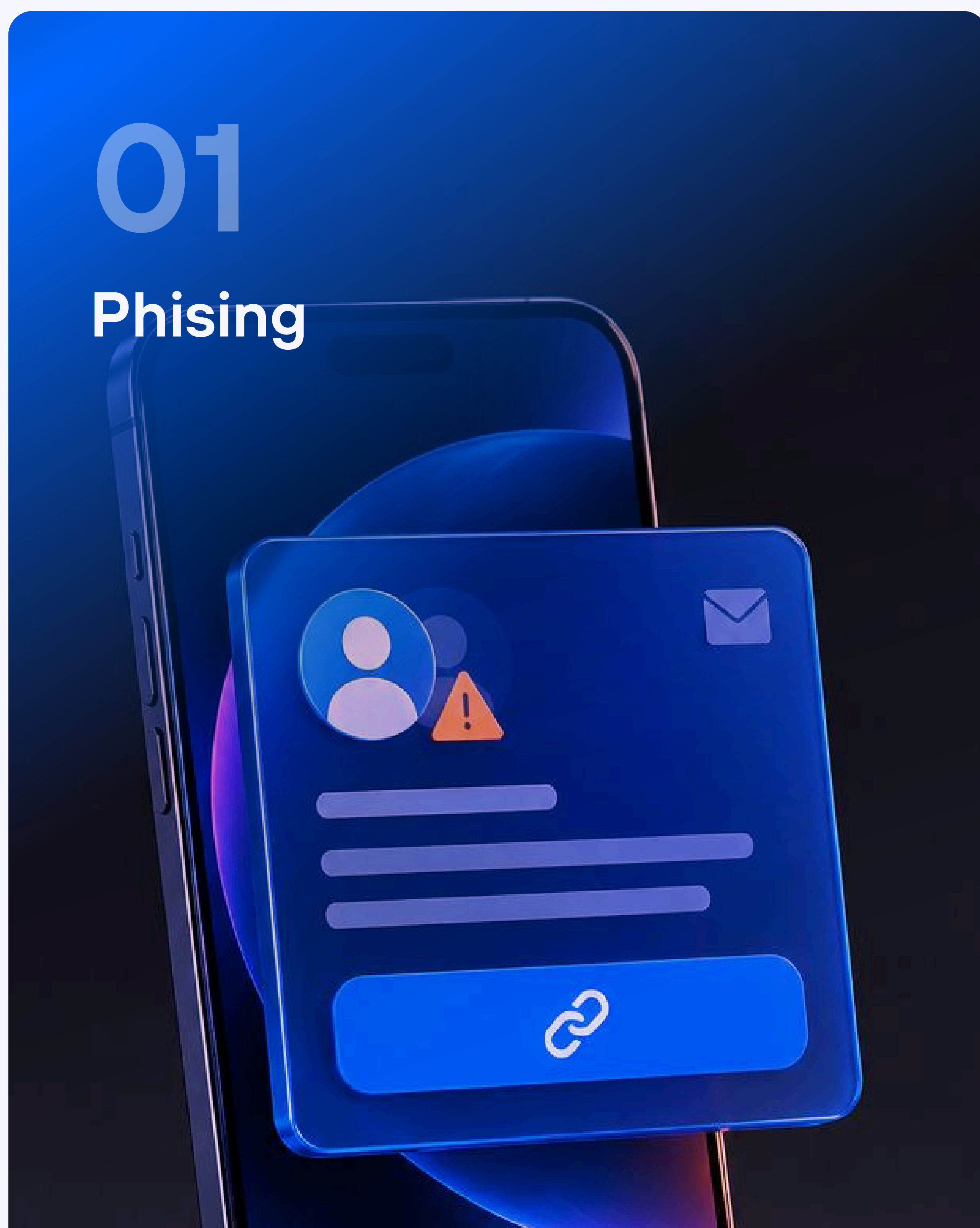
Hay aplicaciones sin soporte, parches pendientes o servicios accesibles desde internet que no se supervisan.

Estas señales no identifican por sí solas el tipo de ataque. Algunas amenazas tampoco ofrecen avisos evidentes antes del incidente. La clave es comprobar lo anómalo y comunicarlo a tiempo.

Las 5 ciberamenazas que tu empresa debe conocer

01

Phishing



- **¿En qué consiste?**

Un atacante se hace pasar por una persona u organización de confianza para conseguir información, acceso o un pago.

- **¿Cómo suele manifestarse?**

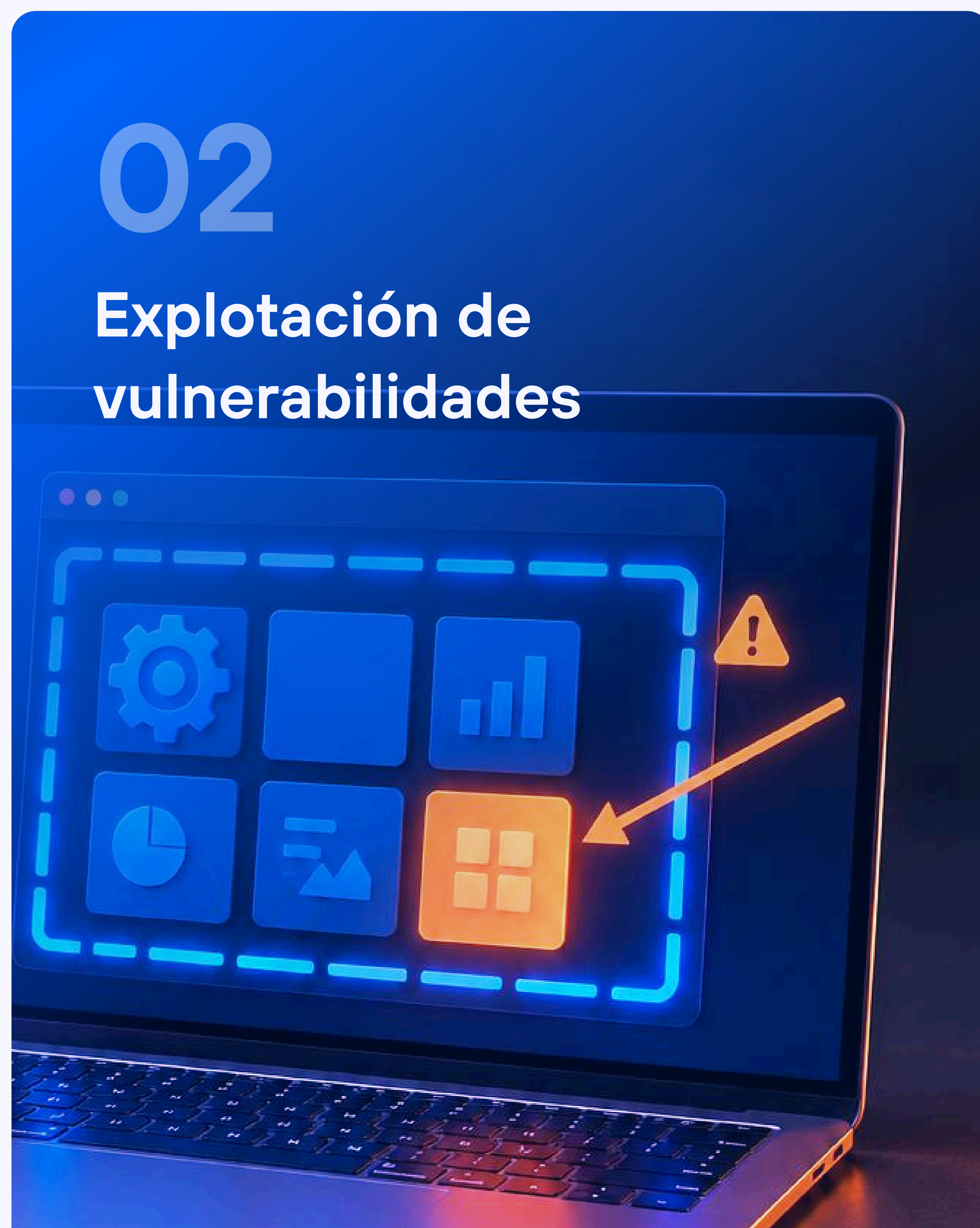
Un correo que pide abrir una factura, un SMS con un enlace o una llamada que solicita una transferencia urgente. Puede llegar por un canal habitual y parecer convincente.

- **¿Cómo suele manifestarse?**

Confirma las peticiones inesperadas por un canal distinto al que se utilizó para contactarte. Accede a los servicios desde sus direcciones oficiales.

02

Explotación de vulnerabilidades



- **¿En qué consiste?**

Se aprovecha un fallo en una aplicación, un dispositivo o un sistema para acceder a él o ejecutar acciones no autorizadas

- **¿Cómo suele manifestarse?**

Un servicio accesible desde internet permanece sin actualizar o utiliza una versión que ya no recibe soporte. No hace falta que una persona abra un mensaje sospechoso.

- **¿Cómo suele manifestarse?**

Identifica los activos expuestos y prioriza la corrección de los fallos que afectan a servicios críticos o que ya están siendo explotados.

03

Robo de credenciales



- **¿En qué consiste?**

Una contraseña, una sesión u otro dato de acceso comprometido permite al atacante entrar como si fuera un usuario legítimo.

- **¿Cómo suele manifestarse?**

Aparecen accesos desde dispositivos desconocidos o actividad fuera de lo habitual. Las credenciales pueden proceder de un engaño, una filtración o un programa malicioso.

- **¿Cómo suele manifestarse?**

Activa la autenticación multifactor, evita reutilizar contraseñas, limita los permisos y revisa las alertas de acceso.

04

Ransomware



- **¿En qué consiste?**

Los atacantes cifran sistemas o roban información para exigir un pago. El incidente puede comprometer los datos y detener la actividad.

- **¿Cómo suele manifestarse?**

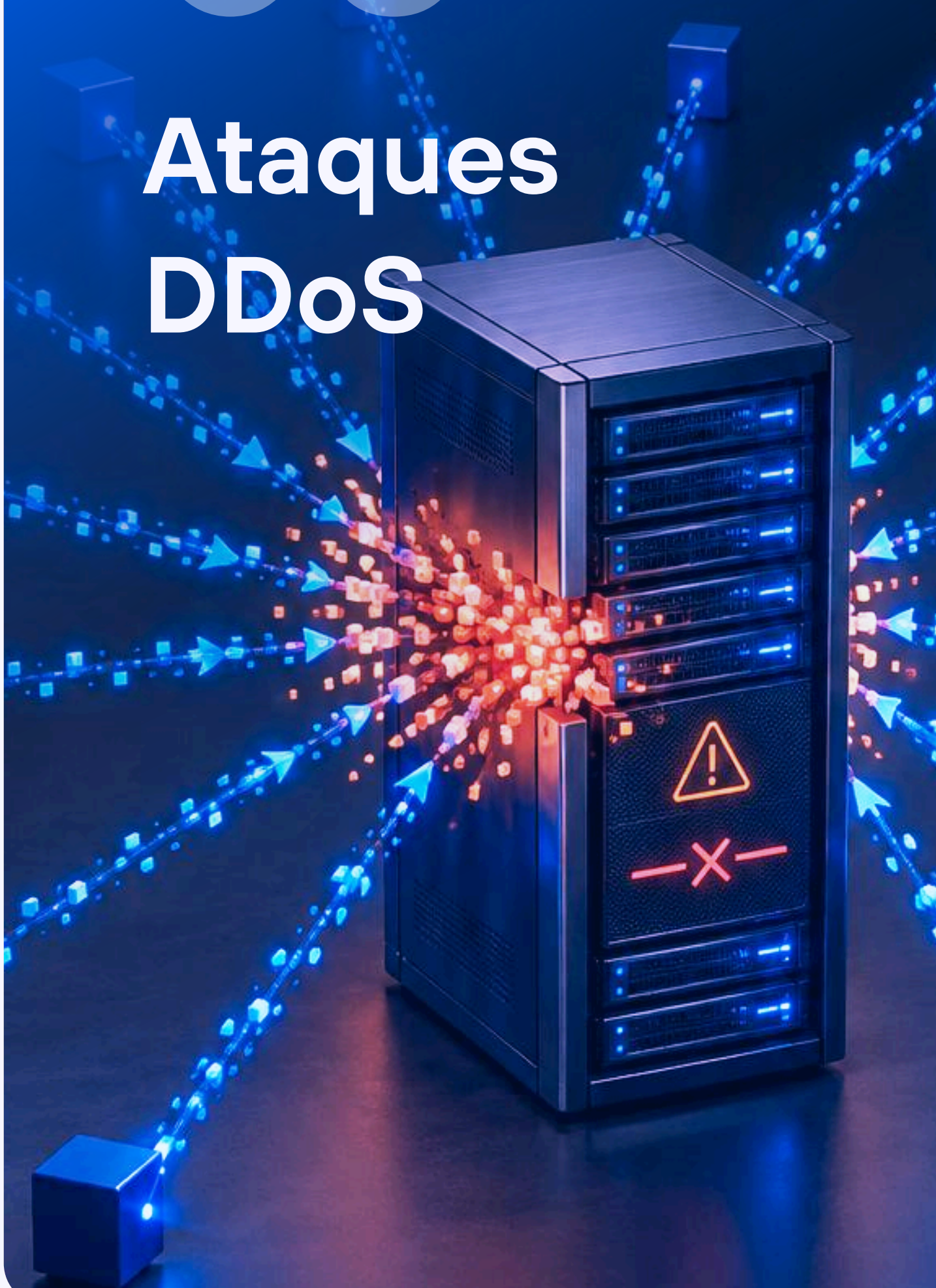
Archivos inaccesibles, sistemas interrumpidos o amenazas de publicar información. El acceso inicial puede haberse producido antes mediante una cuenta comprometida o una vulnerabilidad.

- **¿Cómo suele manifestarse?**

Protege y prueba las copias de seguridad, limita la propagación entre sistemas y ensaya la respuesta y la recuperación.

05

Ataques DDoS



- **¿En qué consiste?**

Múltiples fuentes envían tráfico o peticiones para saturar una web, aplicación o servicio digital.

- **¿Cómo suele manifestarse?**

El servicio responde muy lentamente o deja de estar disponible para muchos usuarios a la vez. El atacante puede buscar la interrupción sin acceder a los datos.

- **¿Cómo suele manifestarse?**

Prepara medidas de mitigación con tus proveedores y define cómo mantener o recuperar los servicios esenciales.



La IA también potencia los ataques

Los atacantes pueden utilizarla para automatizar tareas, personalizar campañas y crear mensajes, voces o vídeos falsos más convincentes. Ante una petición de acceso, información sensible o dinero, verifica la identidad por un canal independiente, aunque parezca auténtica.

¿Por qué Telefónica Tech?

Telefónica asume el reto indiscutible de convertirse en la mejor vía de acceso de empresas e instituciones a las tecnologías digitales.

Combinamos especialistas en ciberseguridad con servicios gestionados para proteger identidades, identificar vulnerabilidades y detectar y responder a incidentes.

Desde nuestro Digital Operations Center y nuestra red global de SOCs, te ayudamos a priorizar riesgos y a actuar para reducir el impacto sobre tu negocio.

