

CHECKLIST DE VULNERABILIDAD EN REDES SOCIALES

¿Estás dejando un rastro digital que facilita el acoso, el robo de identidad o la extorsión?

Marca con X cada punto que aplique a tu situación actual. El documento tiene 20 ítems en total. Cuenta tus marcas al final y consulta la escala de resultado.

01 · CONFIGURACIÓN DE PRIVACIDAD

☐ Tu perfil principal es público (visible para cualquier persona sin cuenta)

Un perfil público permite a cualquier persona ver tu foto, nombre, red de contactos y publicaciones sin filtro alguno.

☐ No has revisado la configuración de privacidad en los últimos 6 meses

Las plataformas actualizan sus políticas con frecuencia. Lo que era privado hace seis meses puede haber dejado de serlo.

☐ Permites que buscadores externos indexen tu perfil

Facebook, LinkedIn e Instagram permiten desactivar la indexación por Google. Si está activada, tu perfil aparece en búsquedas públicas.

☐ Tus contactos o seguidores son visibles públicamente

La red de contactos visible revela información sobre tu entorno que puede ser explotada para ingeniería social o suplantación.

☐ Cualquier persona puede enviarte mensajes directos sin restricción

El acceso abierto a mensajería directa es el vector principal de phishing, extorsión y acoso.

02 · INFORMACIÓN PERSONAL EXPUESTA

☐ Tu domicilio o barrio aparece en tu perfil o en publicaciones

La dirección o zona de residencia permite localización física. Combinada con rutinas publicadas, facilita el seguimiento presencial.

☐ Has publicado fotos que revelan tu lugar de trabajo habitual

El lugar de trabajo es un punto de localización predecible. Fotos con fachada, uniforme o nombre de empresa lo exponen directamente.

☐ Tu número de teléfono o email personal está visible en el perfil

Los datos de contacto directos son el primer objetivo en intentos de phishing y acoso. Su exposición pública multiplica el riesgo.

☐ Has publicado documentos, carnés o datos oficiales, aunque sea parcialmente

Una foto parcial de un DNI o documento bancario puede ser suficiente para iniciar un proceso de suplantación de identidad.

☐**Tu fecha de nacimiento completa es visible públicamente**

La combinación nombre + fecha de nacimiento es suficiente para intentar recuperar contraseñas o acceder a servicios.

☐**Has compartido tu ubicación en tiempo real o has activado check-ins frecuentes**

Los check-ins en tiempo real permiten saber dónde estás y, por exclusión, cuándo no estás en tu domicilio.

03 · RUTINAS Y PATRONES DE COMPORTAMIENTO

☐**Publicas con regularidad desde los mismos lugares (gimnasio, cafetería, trabajo)**

La regularidad de publicaciones desde puntos fijos permite construir un mapa de rutinas sin necesidad de seguimiento físico.

☐**Has publicado fotos de tus hijos con nombre, colegio o actividades extraescolares**

La exposición de menores es un riesgo específico y grave. Nombre + colegio + foto es suficiente para aproximarse a un menor con engaño.

☐**Anuncias con antelación tus viajes o ausencias prolongadas del domicilio**

Publicar 'me voy de vacaciones' antes de salir equivale a anunciar que el domicilio estará desocupado durante un período determinado.

☐**Las fotos que publicas contienen metadatos de ubicación sin eliminar**

Las imágenes de smartphone incluyen coordenadas GPS por defecto. Muchas plataformas las eliminan, pero no todas.

☐**Participas en sorteos que solicitan datos personales para participar**

Los sorteos en redes sociales son un vector frecuente de recopilación de datos personales con fines comerciales o maliciosos.

04 · CONTRASEÑAS Y CONTROL DE ACCESOS

☐**Usas la misma contraseña en varias redes sociales o servicios**

Una sola brecha en cualquier plataforma compromete todos los servicios donde uses la misma contraseña.

☐**No tienes activada la verificación en dos pasos en tus cuentas principales**

La verificación en dos pasos bloquea el acceso no autorizado incluso cuando la contraseña ha sido comprometida.

☐**Has dado acceso a aplicaciones de terceros a tus cuentas de redes sociales**

Las aplicaciones con acceso pueden leer, y en algunos casos publicar, en tu nombre. Revisa qué aplicaciones tienen acceso activo.

☐**Tu pregunta de seguridad tiene respuesta deducible de tu perfil público**

Preguntas como 'nombre de tu mascota' o 'ciudad de nacimiento' son responsables por cualquiera que haya revisado tu perfil.

ESCALA DE RESULTADO

0 – 3 marcas	4 – 8 marcas	9 – 14 marcas	15 o más marcas
Exposición baja. Tu huella digital está razonablemente controlada. Revisa periódicamente.	Exposición moderada. Existen vulnerabilidades concretas. Corrégelas antes de que sean explotadas.	Exposición alta. Tu perfil digital representa un riesgo real. Actúa de forma inmediata.	Exposición crítica. Contacta con un profesional para una auditoría de huella digital.

Si tu resultado es alto o crítico, **Ineva Detectives** realiza auditorías de exposición digital para particulares y empresas. Descarga más recursos en www.inevadetectives.eu/docs o escríbenos a hola@inevadetectives.eu