

ANUNCIA-TE

Visibilidad, privacidad y confianza digital

Cómo permitir que nos encuentren sin exponer innecesariamente
nuestros datos

**«Que te encuentren cuando te necesiten.
Que tus datos no estén a disposición de cualquiera.»**

Documento de reflexión y propuesta práctica para usuarios,
profesionales y empresas.

Introducción. La contradicción que debemos resolver

Queremos ser visibles para nuestros posibles clientes, pero no queremos ser vulnerables ante quienes buscan aprovecharse de nosotros. Un profesional necesita que lo encuentren; un autónomo quiere recibir encargos; una empresa necesita nuevos clientes. Ninguno debería tener que aceptar como precio inevitable de esa visibilidad que sus datos circulen sin control, se recopilen para otros fines o se utilicen para intentar engañarle.

La solución no consiste en desaparecer de Internet ni en confiar ciegamente en las empresas. Consiste en separar la visibilidad comercial de la exposición innecesaria de datos, y dar al usuario control real sobre cómo se produce el contacto.

Para Anuncia-te, esta reflexión puede convertirse en una propuesta de valor: no solo ayudar a que te encuentren, sino hacerlo con transparencia sobre qué información se publica, para qué sirve y quién puede utilizarla.

1. ¿Qué información necesitamos hacer pública?

No todos los datos tienen el mismo valor ni entrañan el mismo riesgo. Conviene distinguir tres categorías:

Categoría	Ejemplos	Criterio recomendado
A. Información comercial	Actividad profesional, productos, servicios, zona de trabajo, horario, fotografías de trabajos y precios publicados voluntariamente.	Hacerla visible cuando ayude al cliente a entender la oferta. No incluir datos personales que no sean necesarios.
B. Información de contacto	Teléfono profesional, correo comercial, formulario de contacto, mensajería o dirección de un establecimiento.	Permitir que el titular decida qué canal mostrar. En algunos casos puede bastar un formulario o canal profesional.
C. Información que debe protegerse	Contraseñas, códigos de verificación, credenciales bancarias, números completos de tarjetas y documentos de identidad.	No publicarla en un anuncio ordinario. Si una operación legítima exige verificar identidad o pagar, usar un procedimiento adecuado y protegido.

Idea clave: un dato no tiene que ser secreto para merecer protección. Un teléfono, un correo o el nombre de un profesional pueden utilizarse para suplantaciones, phishing o engaños dirigidos. El riesgo también depende de cómo se combinan los datos y de quién los utiliza.

Como muchos datos ya están distribuidos por Internet, la pregunta útil no es «¿cómo consigo que mis datos no existan en la red?», sino: ¿cómo permito que me encuentre quien tiene un interés legítimo en lo que ofrezco, sin facilitar innecesariamente el trabajo a quien pretende perjudicarme?

2. Como empresa: cómo generar confianza de verdad

La privacidad debería ser una característica de la forma de trabajar de Anuncia-te, no solo una frase publicitaria escondida en las condiciones legales. El Reglamento General de Protección de Datos

(RGPD) recoge principios como transparencia, limitación de la finalidad, minimización de datos y seguridad, además de protección de datos desde el diseño y por defecto.

1. El usuario decide qué muestra

Permitir que cada profesional elija qué información hace pública: actividad, descripción, fotografías, localidad, teléfono comercial, correo o formulario. No todo debe estar visible por defecto.

2. Cada dato tiene una finalidad concreta

Si un correo se proporciona para recibir consultas sobre anuncios, no debe utilizarse automáticamente para publicidad ajena ni venderse a terceros. Cada uso necesita una base jurídica válida y una explicación clara.

3. Los datos privados no se mezclan con los anuncios

Separar la información pública de la necesaria para administrar cuentas, gestionar pagos o prestar servicios, con permisos de acceso diferenciados.

4. El usuario sabe quién gestiona su espacio

Si el usuario delega tareas en un gestor de contenidos o Comercial GTC Asociado, deben estar claras la autorización, las funciones permitidas y el alcance del acceso. El gestor solo debe acceder a lo imprescindible.

5. Control real y salida sencilla

Facilitar la corrección de datos, el ejercicio de derechos, la gestión de preferencias y las solicitudes de supresión cuando proceda. Explicar también qué información puede conservarse por obligación legal.

6. Seguridad técnica y respuesta ante incidentes

Aplicar contraseñas almacenadas de forma segura, autenticación reforzada para cuentas privilegiadas, copias protegidas, actualizaciones, registros de acceso y procedimientos de respuesta.

7. Demostrar lo que se promete

Explicar qué datos se recogen, para qué, durante cuánto tiempo, quién accede y cómo contactar con el responsable de privacidad. Revisar periódicamente proveedores, permisos y prácticas reales.

Importante: estas medidas son una propuesta de diseño y gestión, no una afirmación de que Anuncia-te ya disponga de todas ellas. Antes de anunciar garantías concretas, debe revisarse cómo está construida y configurada actualmente la plataforma.

3. Una posible solución: el contacto bajo control

Imaginemos que una persona busca un fontanero en su localidad. En lugar de consultar un directorio lleno de teléfonos personales, podría encontrar los servicios publicados por profesionales y enviar una solicitud mediante Anuncia-te. El profesional recibiría la consulta y decidiría cómo responder, sin necesidad de mostrar públicamente su teléfono personal.

1. EL CLIENTE BUSCA	Un profesional disponible en su zona.
2. ANUNCIA-TE MUESTRA	Profesionales, servicios, zonas de trabajo y condiciones publicadas.
3. EL CLIENTE SOLICITA CONTACTO	La consulta llega al profesional a través de un canal de contacto.

4. EL PROFESIONAL DECIDE

Puede responder por el canal disponible y compartir datos adicionales si lo considera necesario.

Esta funcionalidad debe desarrollarse o comprobarse para saber si ya existe en parte. También requiere proteger la mensajería y evitar que los formularios se conviertan en una vía de spam o fraude.

Límite que debe explicarse con honestidad: si un profesional publica voluntariamente su teléfono, cualquier persona que pueda verlo podría copiarlo. La plataforma puede reducir la exposición innecesaria, pero no garantizar que un dato público nunca se recopile o se utilice indebidamente.

Propuesta de posicionamiento: «Tu actividad, visible. Tus datos, bajo tu control».

No prometer anonimato absoluto ni riesgo cero. Prometer decisiones claras, acceso limitado, transparencia y medidas verificables.

4. Como usuario: cómo evaluar la confianza en una empresa

Conviene distinguir dos cuestiones: que una empresa sea legítima —que exista realmente y no sea una identidad ficticia— y que trate correctamente los datos. Una empresa auténtica puede gestionar mal la privacidad. Un candado HTTPS cifra la conexión, pero no certifica la honradez de quien está al otro lado.

- Identidad comprobable. ¿Puedo identificar la razón social, el NIF cuando corresponda y una vía de contacto verificable?
- Política comprensible. ¿Explica qué datos recoge, para qué, durante cuánto tiempo y quién puede recibirlos?
- Control sobre mis datos. ¿Puedo acceder, corregir, oponerme a determinados usos o solicitar la supresión cuando proceda?
- Solo lo necesario. ¿Me solicita únicamente los datos razonables para el servicio que ofrece?
- Consentimientos claros. ¿Distingue la información necesaria para contratar de la autorización opcional para publicidad?
- Seguridad y reputación. ¿Ofrece canales de atención y tiene referencias independientes que puedo contrastar?
- Condiciones y responsabilidades. ¿Puedo saber quién presta el servicio, cómo reclamar y qué ocurre si hay un problema?

Recursos públicos útiles

- Agencia Española de Protección de Datos (AEPD): www.aepd.es/derechos-y-deberes — información sobre derechos y deberes en protección de datos.
- Instituto Nacional de Ciberseguridad (INCIBE): www.incibe.es/ciudadania — guías para prevenir fraudes digitales.
- INCIBE 017: línea de ayuda en ciberseguridad en España.

No conviene confiar únicamente en testimonios publicados en la propia web. Busca referencias independientes, comprueba que los datos de contacto coinciden y verifica las solicitudes extraordinarias mediante un canal oficial conocido.

5. Errores que debemos evitar

- Confundir visibilidad con consentimiento universal. Publicar un anuncio no autoriza automáticamente a utilizar todos los datos para cualquier fin.
- Creer que los datos no sensibles carecen de riesgo. Un teléfono y un nombre pueden servir para preparar un engaño personalizado.
- Confundir cumplimiento legal con seguridad absoluta. La normativa no elimina la posibilidad de un ataque, un error humano o una filtración.
- Prometer protección total. Una empresa responsable explica las medidas que realmente aplica y los riesgos que no puede eliminar.

Como usuarios, debemos desconfiar de comunicaciones que, aunque conozcan nuestro nombre o actividad, nos pidan contraseñas, códigos de verificación o pagos inesperados. La identidad de quien nos contacta debe verificarse por otro canal, no deducirse de los datos que conoce.

6. Propuesta de compromiso público para Anuncia-te

La privacidad puede diferenciar a la plataforma, siempre que las promesas comerciales vayan acompañadas de medidas técnicas y organizativas reales. Se propone desarrollar un compromiso público basado en cinco principios:

Tú decides qué muestras

La información comercial visible debe responder a una decisión informada del usuario.

Tus datos tienen una finalidad

Explicamos qué información necesitamos y para qué la utilizamos.

No pedimos lo que no necesitamos

Reducimos la información recogida y los accesos a ella.

Sabes quién gestiona tu espacio

El usuario conoce quién está autorizado para administrar su información y con qué alcance.

La confianza se demuestra

Publicamos nuestras prácticas, facilitamos el ejercicio de derechos y revisamos la seguridad.

Antes de publicarlo como garantía, conviene revisar la plataforma: formularios de registro, campos obligatorios, datos visibles, accesos de los GTC, proveedores tecnológicos, política de privacidad, conservación de datos y medidas de seguridad. Esa revisión permitirá preparar un plan de mejoras y comprobar qué compromisos son ya ciertos.

7. Plan de actuación recomendado

1. Revisar

Inventariar los datos recogidos, dónde se guardan, quién accede y con qué finalidad.

2. Reducir

Eliminar campos innecesarios y limitar los permisos de usuarios, colaboradores y proveedores.

3. Dar opciones

Separar datos públicos, datos de cuenta y datos de contacto; ofrecer alternativas cuando sea viable.

4. Informar

Redactar una explicación clara y coherente con el tratamiento real de los datos.

5. Proteger

Comprobar controles técnicos, copias de seguridad, accesos, actualizaciones y respuesta ante incidentes.

6. Verificar

Revisar periódicamente que la práctica coincide con las promesas y corregir las carencias detectadas.

Conclusión. La confianza debe formar parte del producto

Anuncia-te no necesita prometer que Internet es seguro. Necesita ayudar a que el usuario se exponga comercialmente de una manera consciente, proporcionada y controlada.

ANUNCIA-TE

**Que te encuentren cuando te necesiten.
Que tus datos no estén a disposición de cualquiera.**

Que la visibilidad sea una decisión. Que la privacidad sea una responsabilidad. Y que la confianza no dependa solo de lo que decimos, sino de lo que podemos demostrar.

No tenemos que elegir entre existir comercialmente en Internet y renunciar a nuestra privacidad. Podemos decidir qué mostrar, limitar lo que compartimos y exigir que las empresas justifiquen el uso que hacen de nuestros datos.

Nota: este documento es una exposición informativa y una propuesta estratégica general. No sustituye una auditoría técnica ni asesoramiento jurídico específico. Las obligaciones aplicables deben valorarse según el funcionamiento real de la plataforma y los tratamientos efectuados.