

# Protección de Privacidad



Llamamos privacidad al espacio de la vida personal de cada persona, que se desarrolla en un espacio reservado y debe mantenerse en la intimidad.

Como se ha mencionado con anterioridad, con esta nueva sociedad de la información y la expansión de las telecomunicaciones, la privacidad se encuentra amenazada y es por eso que hoy hablamos de temas como el que ahora nos compete como lo es “La Protección de la Privacidad”.

<https://www.cloudseguro.co/wp-content/uploads/2015/05/k.jpg>

Según las Declaraciones Universales, dentro de la Declaración Universal de los Derechos Humanos, se establece que el derecho a la privacidad es:

*“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.*

Derecho a la privacidad

Todo el mundo tiene derecho a una vida privada en la que nadie debe interponerse. Todos tenemos derecho a que se nos respeten las actuaciones y los sucesos de nuestra vida, es decir, todos tenemos derecho a la privacidad<sup>1</sup>, algunas de las formas de violar este derecho son:

- Intervenir en la vida privada de una persona (lo que incluye su derecho a establecer relaciones y a disfrutar de su libertad sexual).
- Impedir la vida familiar (lo que incluye el derecho a casarse y a fundar una familia).
- Destruir la casa de una persona, o impedir a una persona que viva en su casa.
- Intervenir la correspondencia privada.

Como ciudadanos del mundo tenemos derecho a la protección del honor, la intimidad personal, familiar y la propia imagen de los usuarios.

---

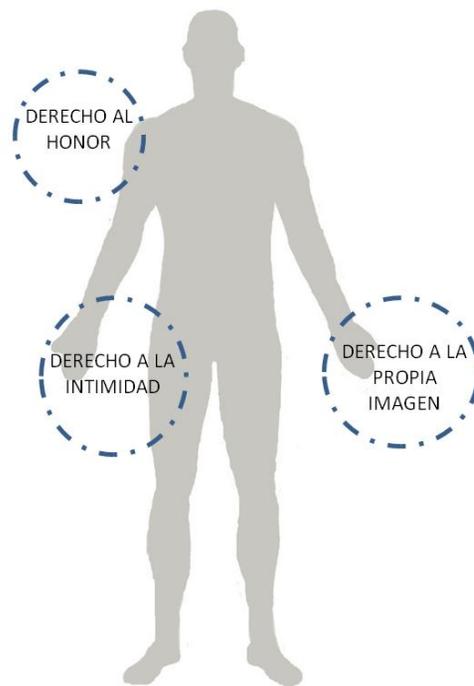
<sup>1</sup> Algunos de los mecanismos internacionales que protegen el derecho a la privacidad son: Comité de derechos humanos de las Naciones Unidas, Representante especial de los defensores de los derechos humanos, Comisión Interamericana sobre Derechos Humanos, Comisión Africana sobre Derechos Humanos y de los Pueblos, Tribunal Europeo de Derechos Humanos, entre otros.

# Protección de Privacidad

**DERECHO AL HONOR:** es aquel que tiene toda persona a su buena imagen, nombre y reputación, de tal forma que cualquier ciudadano puede exigir que se respete su esfera personal, con independencia de las circunstancias particulares, siendo un derecho irrenunciable.

**DERECHO A LA INTIMIDAD:** tiene por objeto la protección de la esfera más íntima de la persona, y se encuentra estrechamente ligado a la protección de la dignidad del individuo.

**DERECHO A LA PROPIA IMAGEN:** pretende salvaguardar un ámbito propio y reservado del individuo, aunque no íntimo, frente a la acción y conocimiento de los demás.



## Situaciones de Riesgo para la protección de la intimidad en el Internet:

- **Alta como usuario:** en la medida en que no sea configurado correctamente el nivel de privacidad del perfil, así como por el hecho de que sea publicada información sensible desde el inicio de la actividad en la red.
- **Participación en la red como usuario:** en el supuesto de que el grado de información, datos e imágenes publicados puedan ser excesivos y afectar a la privacidad, tanto personal como de terceros.

# Protección de Privacidad

- **Privacidad personal:** a pesar de que sean los usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance mayor al que consideran en un primer momento, ya que estas plataformas disponen de potentes herramientas de intercambio de información, la capacidad de procesamiento y el análisis de la información facilitada por los usuarios.
- **Privacidad de terceros:** es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si estos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata.
- **Darse de baja de la plataforma:** en el caso en que el usuario solicite dar de baja su perfil, pero aún así continúen datos publicados por este, o información personal e imágenes propias publicadas en los perfiles de otros usuarios.

**IMPORTANTE:** Las redes sociales permiten a los motores de búsqueda de Internet indexar en sus búsquedas los perfiles de los usuarios, junto con información de contacto y de perfiles amigos, lo que puede suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de su información en Internet.

Como te podrás dar cuenta, las nuevas tecnologías, además de tener grandes ventajas, también tienen la gran desventaja de exponernos como personas de manera cibernética y física. Muchas veces al acceder a una red social les damos a los proveedores el derecho a controlar el uso que se realice de nuestros datos personales. Toda la información que publicamos en nuestros perfiles, fotos, datos personales, pensamientos, entre otros, se convierten en una "identidad digital" que da a conocer fácilmente nuestro datos de contacto, preferencias y hábitos.

## Situaciones de Riesgo para la protección datos de carácter personal en el Internet:

- **Phishing y pharming:** mediante estos, los ciberdelincuentes obtienen datos personales de los usuarios de Internet, así como de datos de carácter sensible o relativos a aspectos económicos (tarjetas de crédito, PIN de usuarios, entre otros).
- **Spammer y spam:** el uso de las redes sociales como plataformas para el envío de correos electrónicos no deseados.

# Protección de Privacidad

- **Indexación** no autorizada por parte de buscadores de Internet.
- **Acceso al perfil incontrolado:** la mayoría de redes sociales disponen del perfil completo del usuario, o al menos de parte de este, en formato público, de forma que cualquier usuario de Internet o de la red social puede acceder a información de carácter personal ajena sin que el propietario de los datos tenga que dar su consentimiento expreso.
- **Suplantación de identidad:** cada vez es más frecuente que usuarios que nunca se habían registrado en redes sociales online, comprueben cómo en el momento en el que intentan acceder, su “identidad digital” ya está siendo utilizada.
- **Publicidad hipercontextualizada:** esta aporta, a priori, una ventaja para los usuarios, ya que con ella evitan que se muestren durante su navegación contenidos para ellos irrelevantes e incluso ofensivos. Sin embargo, desde el punto de vista legal, podría considerarse una práctica ilegal, ya que para poder contextualizar la publicidad que se va a mostrar a un usuario se tienen que examinar sus datos y preferencias.
- **La instalación y uso de “cookies” sin conocimiento del usuario:** radica en la posibilidad de que el sitio web utilice cookies que permitan a la plataforma conocer cuál es la actividad del usuario dentro de la misma. Mediante estas herramientas, las redes sociales pueden conocer el lugar desde el que el usuario accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de clicks realizados, e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la red.

## Protección de la propiedad intelectual e industrial

Se está produciendo un aumento en el número de contenidos protegidos por el derecho de propiedad intelectual que están siendo utilizados, compartidos y difundidos a través de las redes sociales y sitios web colaborativos. La protección se centra, por tanto, en el derecho que el autor tiene sobre su creación literaria, artística o científica.

# Protección de Privacidad

## Protección de los consumidores y usuarios

Una de las principales ventajas que presenta este tipo de plataformas, es la capacidad de obtener beneficios económicos derivados de la publicidad y de las aplicaciones internas desarrolladas por los propios usuarios de la red.

La facilidad con la que los usuarios pueden anunciar o ser receptores de anuncios de productos y servicios es muy elevada si se compara con el mundo físico, ya que junto a la sencillez con la que se pueden comercializar productos y servicios a distancia, las redes sociales cuentan con una base de datos de usuarios (potenciales clientes), perfectamente segmentados por gustos y perfiles, lo que implica que las capacidades de éxito del procedimiento comercial sean muy altas.

## Privacidad y Seguridad para los usuarios de la RED

Como usuarios de la Red, ya sea como individuos u organizaciones, la población demanda:

1. **Transparencia y facilidad de acceso a la información:** es fundamental que este tipo de plataformas expongan toda la información relativa a sus servicios de forma clara, de manera que el lenguaje empleado en sus condiciones de uso y políticas de privacidad sea absolutamente comprensible para cualquier tipo de usuario.
2. **Establecer estándares de seguridad y privacidad:** referidos a la no indexación por defecto de los datos personales o a la especial protección de los datos sensibles.
3. **Garantizar la seguridad tecnológica de la plataforma:** es vital la correcta elección por parte de la plataforma de un prestador de servicios de Internet que cuente con un elevado nivel de seguridad: servidores seguros, centros de respaldo y accesos seguros, entre otras medidas.
4. **Eliminación de la información:** después de un tiempo prudencial sin que el usuario haya entrado en la plataforma.
5. **Respetar los derechos de acceso y cancelación.**
6. **Desarrollo interno de espacios web dedicados a poner a disposición de los usuarios el máximo y más claro posible nivel de información respecto al tratamiento de datos personales, los sistemas publicitarios empleados en la plataforma, las situaciones de riesgo a las que se pueden enfrentar, así como de las implicaciones que pueden derivarse de la publicación de contenidos en la red social.**
7. **Teniendo en cuenta que la gran mayoría de usuarios de las redes sociales son menores de edad, es fundamental que las redes sociales y plataformas colaborativas, junto con las autoridades públicas, asociaciones y organizaciones**

# Protección de Privacidad

cuya finalidad sea la protección de este tipo de colectivos, lleven a cabo iniciativas conjuntas encaminadas a fomentar la formación entre los menores y tutores respecto a la seguridad de los usuarios, investigando las posibilidades tecnológicas existentes para lograr la identificación de la edad de los usuarios del servicio.

8. La prevención del fraude online.
9. Investigación y desarrollo en materia de seguridad tecnológica.
10. El desarrollo de parches de seguridad y actualizaciones.

## Medidas de Seguridad

1. Utiliza seudónimos o nicks personales: te permiten disponer de una auténtica “identidad digital”, que no pone en entredicho la seguridad de tu vida personal y profesional. De esta forma, únicamente te conocerán tu círculo de contactos que conocen el nick que empleas en Internet.
2. Ten cuidado a la hora de publicar contenidos audiovisuales y gráficos en tu perfil, dado que en este caso puedes estar poniendo en riesgo la privacidad e intimidad de tu persona y/o las personas que te rodean.
3. Revisa y lee las condiciones generales de uso y la política de privacidad que la plataforma pone a tu disposición en los sitios web.
4. Configurar adecuadamente el grado de privacidad de tu perfil de usuario en la red social, de tal forma que este no sea completamente público, sino que únicamente tengan acceso a la información publicada en el perfil aquellas personas que hayan sido catalogadas como “amigos” o “contactos directos” previamente autorizados por ti.
5. Acepta únicamente a aquellas personas conocidas o con las que mantienes alguna relación previa, no aceptando de forma compulsiva todas las solicitudes de contacto que recibes, e investiga siempre que fuera posible y necesario, quién es la persona que solicita tu contacto a través de la red social.
6. No publiques en tu perfil, información de contacto físico, que permita a cualquier persona conocer dónde vives, dónde trabajas o estudias diariamente o los lugares de ocio que sueles frecuentar.
7. Ten especial cuidado respecto a la publicación de información relativa a los lugares en que te encuentras en todo momento.
8. Utiliza y publica únicamente contenidos respecto a los que cuenten con los derechos de propiedad intelectual suficientes. En caso contrario, estarás cometiendo un acto ilícito.
9. Utiliza diferentes nombres de usuario y contraseñas para entrar en las distintas redes sociales de las que seas miembro.
10. Es recomendable utilizar contraseñas con una extensión mínima de 8 caracteres, alfanuméricos y con uso de mayúsculas y minúsculas.
11. Es importante disponer en tus equipos de software antivirus instalado y debidamente actualizado.

# Protección de Privacidad

12. Las Redes Sociales no son para menores de 14 años y los menores no deben revelar datos personales excesivos. Nunca se deben suministrar los datos a desconocidos.
13. Debes leer toda la información concerniente a la página web. En ella se explica quiénes son los titulares de la misma y la finalidad para la que se solicitan los datos.
14. No compartas con terceros los nombres de usuario y contraseña, ni los compartas entre amigos o compañeros de clase. Estos datos son privados y no deben ser comunicados a terceros y/o desconocidos.

## 10 simples pasos para operar en Internet

- Usar un antivirus: para computadoras y smartphones.
- Actualizar el sistema operativo, navegador, apps y programas para evitar malware.
- Enseñar a los niños el uso de internet: bloquear contenidos no aptos para menores.
- No abras "spam": desechar de inmediato el llamado correo basura.
- Usar contraseñas seguras: con mayúsculas, números y caracteres combinados.
- Copia de Seguridad: de los archivos que no quieras perder.
- Descargar aplicaciones de confianza: solo de mercados oficiales.
- Conexiones solo cuando sea necesario: Bluetooth, WiFi y función GPS.
- Amigos en redes sociales: agregar solo personas que conozcan fuera de la red.
- Información personal: piénsalo antes de subirla a las redes sociales.

### Referencia:

- Abad, A. (2013). *Seguridad y Alta Disponibilidad*. (1ª Edición) España. Ibergarceta Publicaciones.
- Brookshear, J. (1995). *Introducción a las ciencias de la computación*. Editorial Addison Wesley.
- Gralla, P. (2008). *Cómo Funciona Internet*. Editorial Anaya Multimedia.
- Negroponte, N. (1996). *Ser digital*. Editorial Océano
- Vasconcelos, J. (2011). *Introducción a la Computación*. (3ª Edición). México. Grupo Editorial Patria.
- Vasconcelos, J. (2015). *Tecnologías de la Información*. (Segunda Edición). México, Grupo Editorial Patria.