



ASISTENCIA TÉCNICA EN MATERIA DE  
ORDENACIÓN, PROMOCIÓN Y  
FOMENTO DE LA ACTIVIDAD  
COMERCIAL DE ÓPTICA



**Comunidad  
de Madrid**



# ÍNDICE

1.	Marco en materia de protección de datos	1
1.1.	Listado de cumplimiento de RGPD	26
2.	Corporate Defense-Modelo de Cumplimiento y Prevención Penal	42
2.1.	Listado compliance de Cumplimiento y Prevención Penal	61
3.	Estrategias de Marketing Digital SEO & SEM	63

---



# 1

## *Marco en materia de Protección de Datos*



## Tabla de Contenidos

<b>1. INTRODUCCIÓN</b>	<b>3</b>
<b>2. DATOS PERSONALES: CONCEPTO Y TIPOS</b>	<b>4</b>
<b>3. PRINCIPIOS FUNDAMENTALES</b>	<b>6</b>
3.1 LICITUD, PROPORCIONALIDAD Y TRANSPARENCIA	6
3.2 FINALIDADES COMPATIBLES CON EL ORIGEN DE LA RECOGIDA	6
3.3 MINIMIZACIÓN Y EXACTITUD DE LOS DATOS PERSONALES	7
3.4 CONSERVACIÓN DE LOS DATOS PERSONALES	7
3.5 INTEGRIDAD Y CONFIDENCIALIDAD	7
3.6 PRIVACIDAD DE LOS DATOS PERSONALES DESDE EL DISEÑO Y POR DEFECTO	7
<b>4. PRINCIPIO DE RESPONSABILIDAD PROACTIVA</b>	<b>8</b>
<b>5. DEBER DE INFORMACIÓN</b>	<b>8</b>
<b>6. LICITUD DEL TRATAMIENTO</b>	<b>9</b>
6.1. SUPUESTOS LEGITIMADORES EN EL TRATAMIENTO DE DATOS PERSONALES	9
6.2. CONSENTIMIENTO	10
<b>7. SUJETOS INTERVINIENTES</b>	<b>11</b>
7.1. RESPONSABLE DEL TRATAMIENTO	11
7.2. ENCARGADO DEL TRATAMIENTO	12
7.3. LA AUTORIDAD DE CONTROL Y LOS SUJETOS INTERVINIENTES	13
<b>8. DERECHOS DE LOS INTERESADOS</b>	<b>13</b>
8.1. DERECHO DE ACCESO	14
8.2. DERECHO DE RECTIFICACIÓN	14
8.3. DERECHO DE SUPRESIÓN (“DERECHO AL OLVIDO”)	15
8.4. DERECHO DE OPOSICIÓN	15
8.5. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO	16
8.6. DERECHO A LA PORTABILIDAD DE LOS DATOS	17
8.7. DERECHO A NO SER OBJETO DE UNA DECISIÓN INDIVIDUAL AUTOMATIZADA	17
<b>9. DELEGADO DE PROTECCIÓN DE DATOS</b>	<b>18</b>
9.1. SUPUESTOS OBLIGATORIOS EXISTENCIA DPO	18
9.2. FUNCIONES DEL DPO	18
9.3. NOMBRAMIENTO DEL DPO	19
<b>10. NOTIFICACIÓN INCIDENTES DE SEGURIDAD</b>	<b>19</b>
<b>11. INVENTARIO DE TRATAMIENTOS</b>	<b>21</b>
<b>12. PRIVACY IMPACT ASSESSMENT</b>	<b>21</b>
<b>13. SANCIONES</b>	<b>22</b>



## 1. INTRODUCCIÓN

La nueva normativa europea en materia de protección de datos, en concreto, el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679, de 27 de abril de 2016), obliga a todas las organizaciones a adaptarse a nuevas exigencias legales cuya implantación implica necesariamente cambios organizativos, procedimentales, así como de sistemas en el seno de las organizaciones. El objetivo de los cambios normativos en esta materia es garantizar a las personas físicas una mayor seguridad en relación con sus datos personales y consagrar la protección de los datos personales como un derecho fundamental para todas ellas.

La nueva regulación aborda el derecho a la protección de datos, con la privacidad en su esencia, en un mundo ampliamente digitalizado y proporciona un marco único de protección de datos aplicable a todas las ópticas e instituciones que tratan datos en la Unión Europea.

La consecuencia de incumplir la referida norma puede conllevar multas administrativas de hasta 20 millones de euros o el 4% de la facturación anual global.

Asimismo, el riesgo de que las personas afectadas por el incumplimiento de las obligaciones en materia de protección de datos, presenten más reclamaciones es superior que en cualquier otro sector, dado que el incumplimiento de estas medidas puede provocar decisiones en las que los sujetos puedan salir perjudicados. A dicho factor se suma la posibilidad que recoge la nueva normativa a presentar reclamaciones tanto por la vía administrativa como la judicial y así poder exigir coberturas concretas por los daños causados.

El presente Marco pretende recoger los principios fundamentales que en materia de protección de datos, todas las ópticas deben tener en cuenta en su operativa diaria.

El contenido del presente Marco viene dividido en las siguientes secciones: **(i)** concepto y tipos de datos de carácter personal, **(ii)** principios fundamentales, **(iii)** responsabilidad proactiva, **(iv)** deber de información, **(v)** licitud del tratamiento, **(vi)** sujetos intervinientes, **(vii)** derechos de los interesados y **(viii)** delegado de protección de datos, **(ix)** notificación de incidentes de seguridad, **(x)** inventario de tratamientos y **(xi)** evaluaciones de impacto en protección de datos o *PrivacyImpactAssessments*.



## 2. DATOS PERSONALES: CONCEPTO Y TIPOS

La definición de dato de carácter personal se refiere a cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Los datos personales nunca incluirán datos anónimos.

Tal y como se desprende de lo anterior, se considerará persona identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos y característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. En este sentido, se diferenciará:

- i. Información identificable directamente: datos que incluyen información que permita identificar o distinguir a una persona física directamente y sin limitaciones, como por ejemplo: nombre, dirección, número de teléfono, número de fax, dirección de correo electrónico, perfiles financieros, identificadores únicos, como el número de la seguridad social, el número del pasaporte, etc. Asimismo, información de tarjetas de crédito, perfil del cliente, preferencias, expectativas y otra información accesorio.
- ii. Información identificable indirectamente: datos personales que también incluyen información que, aunque por sí misma no pueda identificar ni distinguir directamente a una persona física, el responsable o un tercero puedan asociarla o vincularla con una persona física teniendo en cuenta todos los medios que probable y razonablemente se usaran.

A continuación, se detallan distintos ejemplos de información identificable indirectamente:

- Debe considerarse que la información (como el tipo de producto financiero preferido) vinculada a un número de tarjeta de un programa de fidelidad de clientes (como identificador único), en un conjunto de datos que no contenga el nombre del cliente ni otro identificador único, son datos personales, porque es posible vincular la información a través del número de tarjeta con el cliente usando información que se gestione en otro conjunto de datos.
- Debe considerarse que la información en registros de red que contenga direcciones de sitios web visitados por las direcciones IP de ordenadores en los establecimientos son datos personales, porque al vincular las direcciones de sitios web y la dirección IP con los datos de inicio de sesión del ordenador, es posible identificar qué persona física ha visitado sitios webs en cada ordenador.

Finalmente, hay que considerar los datos pseudónimos, los cuales no pueden atribuirse a un interesado específico sin usar información adicional, siempre que dicha información adicional se guarde por separado y esté sujeta a medidas técnicas y organizativas que garanticen que no se atribuye a una persona física identificada o identificable. Estos datos seguirán considerándose datos de carácter personal en tanto en cuanto se pueda llegar a identificar a la persona física a la que corresponden. En cualquier caso, el procedimiento de seudonimización de los datos será una de las medidas a aplicar para minimizar riesgos en materia de protección de datos.



Sentando lo anterior, se pueden categorizar ciertos tipos de datos, en función de la información que aporta:

- **Datos de carácter identificativo:** DNI, dirección, imagen, voz, número de seguridad social, teléfono, marcas físicas, nombre y apellidos, firma, huella y firma electrónica.
- **Datos relativos a las características personales:** estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna y características físicas.
- **Datos relativos a la personalidad:** evaluaciones de perfiles, comportamientos y actitudes.
- **Datos relativos a las circunstancias sociales:** características de alojamiento, vivienda, situación familiar, posesiones, aficiones, estilos de vida, pertenencia a asociaciones o clubes, licencias, permisos y autorizaciones.
- **Datos académicos y profesionales:** formación, titulaciones, expediente académico y experiencia profesional.
- **Datos relativos al empleo:** profesión, puestos de trabajo, datos no económicos de nómina e historial del trabajador.
- **Datos que aportan información comercial:** actividades y negocios, licencias comerciales y publicaciones en medios de comunicación.
- **Datos económicos, financieros y de seguros:** ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, hipotecas, datos bancarios, nóminas, tarjeta de crédito, deducciones económicas y subsidios.
- **Datos relativos a transacciones de bienes y servicios:** bienes y servicios suministrados y/o recibidos por el afectado, direcciones IP, compensaciones, e indemnizaciones.
- **Datos especialmente protegidos:** ideología, afiliación sindical religión, creencias, origen racial o étnico, salud, vida sexual, datos sobre condenas e infracciones penales.



## 3. PRINCIPIOS FUNDAMENTALES

La normativa aplicable en materia de protección de datos tiene una incidencia directa en la operativa de los establecimientos, por cuanto en la actividad diaria de éstas se tratan datos de carácter personal. Para dicho tratamiento es necesario que todos los empleados cumplan con una serie de principios y medidas establecidas en la mencionada normativa. A continuación, detallaremos los principales pilares que los establecimientos deberán cumplir en su operativa diaria:

### 3.1 Licitud, proporcionalidad y transparencia

Cualquier establecimiento deberán tratar los datos de carácter personal de manera:

- Lícita: Se obtendrán los datos siguiendo los requerimientos que establece la normativa aplicable.
- Proporcional: Se tratarán los datos únicamente acordes con las finalidades que sean necesarias, adecuadas y pertinentes.
- Transparente: La información debe ser clara, evidente y sin ambigüedades.

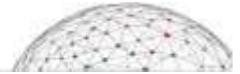
### 3.2 Finalidades compatibles con el origen de la recogida

Los establecimientos deberán asegurarse de que el tratamiento de los datos personales se circunscribe a los fines determinados, explícitos y legítimos para aquellos que fueron recogidos en origen y que no serán tratados ulteriormente de manera incompatible con dichos fines.

Si bien las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles, es necesario que se solicite el consentimiento expreso de los interesados cuando el tratamiento de los datos vaya más allá de los fines para los que se recogieron inicialmente y no sean compatibles con los mismos.

Con objeto de determinar la compatibilidad de los distintos fines de tratamiento, los establecimientos deberán tener en cuenta:

- cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
- el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
- la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales.
- las posibles consecuencias para los interesados del tratamiento ulterior previsto;
- la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.



Así pues, siempre y cuando el tratamiento de datos no esté basado en el consentimiento, el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente sólo debe permitirse cuando sea compatible con los fines de su recogida inicial.

### **3.3 Minimización y exactitud de los datos personales**

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines específicos para los que son tratados. Asimismo, se deberán adoptar todas las medidas razonables para suprimir o rectificar todos aquellos datos que puedan resultar inexactos o incompletos, con respecto a las finalidades para los que se tratan.

### **3.4 Conservación de los datos personales**

Los establecimientos deberán mantener los datos personales que tratan, de forma que se permita la identificación de los interesados y únicamente durante el tiempo que sea necesario para los fines del tratamiento de los datos lícitos y legítimos.

No obstante lo anterior, los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas para proteger los derechos y libertades de los interesados.

### **3.5 Integridad y confidencialidad**

Los establecimientos deberán asegurarse y garantizar a todas las personas físicas de las que recabe datos personales, que los datos serán tratados con el debido nivel de seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas, como por ejemplo la seudonimización o el cifrado de datos personales.

En este sentido, los establecimientos deberán valorar cuáles son las medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, así como la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

Adicionalmente, deberán asegurarse especialmente que los empleados, los terceros que presten servicios y los empleados de dichos terceros que en el desempeño de sus funciones tienen acceso a datos personales, se comprometan a guardar secreto y a no comunicar, en ningún caso, a terceras personas dicha información personal. En este sentido todas las personas con acceso a este tipo de información deberán firmar un acuerdo de secreto y confidencialidad.

### **3.6 Privacidad de los datos personales desde el diseño y por defecto**



Todos los establecimientos deberán llevar a cabo medidas que garanticen y permitan demostrar el cumplimiento de las exigencias legales en materia de protección de datos. Esto significa que las políticas de protección de datos desarrolladas por los establecimientos no solo han de existir, sino que han de estar adaptadas a las circunstancias de la organización, implementadas y funcionar en la práctica.

Una de las principales medidas es la implantación de la privacidad desde el diseño y por defecto. En este sentido, la concepción de una aplicación, un producto o servicio, deberá tener en cuenta *ab initio* (desde su inicio) cuestiones como el deber de información o la adecuada obtención del consentimiento para el tratamiento de datos de carácter personal de los clientes (privacidad desde el diseño), así como que por defecto únicamente sean objeto de tratamiento los datos personales necesarios para alcanzar el fin legítimo perseguido, garantizando siempre la confidencialidad de los datos personales (privacidad por defecto).

## 4. PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Los establecimientos deberán adoptar políticas adecuadas e implementará medidas técnicas y organizativas apropiadas y verificables para asegurar y poder acreditar de forma transparente que el tratamiento de datos personales se lleve a cabo de conformidad con la normativa aplicable en materia de protección de datos.

A lo largo del presente Marco se irán detallando algunas de las principales medidas que se deberán aplicar para poder demostrar la debida diligencia en esta materia. Algunas de las medidas son:

- i. Cumplimiento con el deber de información y obtención de consentimiento,
- ii. la realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas,
- iii. la designación de una figura de Delegado de Protección de Datos (*Data Protection Officer*),
- iv. el cumplimiento de las medidas de seguridad,
- v. la protección de datos desde el diseño y por defecto,
- vi. la elaboración de un registro de actividades de tratamiento y
- vii. la adopción de mecanismos de notificación de incidentes de seguridad.

## 5. DEBER DE INFORMACIÓN

Antes de recabar cualquier tipo de dato personal, los establecimientos deberán comunicara los interesados, la siguiente información, de manera sencilla y clara, de modo que sea fácil de entender:

- i. La identidad y los datos de contacto del responsable que corresponda, como responsable del tratamiento de los datos.



- ii. Los datos de contacto del delegado de protección de datos.
- iii. Los fines del tratamiento a que se destinan los datos personales.
- iv. La base jurídica del tratamiento de los datos. Cuando la base jurídica se base en los intereses legítimos de la óptica o de un tercero, se deberá especificar el detalle de los supuestos legitimadores basados en el interés legítimo.
- v. Los destinatarios o las categorías de destinatarios de los datos personales.
- vi. La intención de transferir datos personales a un tercer país u organización internacional y la referencia a las garantías adecuadas o apropiadas para realizar dichas transferencias.
- vii. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- viii. La existencia del derecho a solicitar el acceso a los datos personales relativos al interesado y su rectificación o supresión o la limitación de su tratamiento o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
- ix. La posibilidad de revocar el consentimiento, en cualquier momento, cuando el tratamiento se haya basado en el consentimiento del interesado sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
- x. El derecho a presentar una reclamación ante una autoridad de control.
- xi. Si la comunicación de datos personales es un requisito legal o contractual o un requisito necesario para suscribir un contrato.
- xii. Las posibles consecuencias de no facilitar los datos de carácter personal, cuando el interesado esté obligado a facilitarlos.
- xiii. La existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Asimismo, cuando los datos personales se obtengan datos a través de terceros, se deberá además informar de los siguientes aspectos:

- i. De todos los aspectos anteriores. Es decir, toda la información que se debe ofrecer cuando los datos personales se recaban directamente por el interesado.
- ii. Las categorías de datos personales de que se trate.
- iii. La fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

## 6. LICITUD DEL TRATAMIENTO

En relación a las condiciones para la licitud del tratamiento, a continuación, se detallan distintos aspectos a tener en cuenta para poder cumplir con dicho principio.

### 6.1. Supuestos legitimadores en el tratamiento de datos personales

El tratamiento será lícito y conforme a lo recogido en la normativa aplicable en materia de protección de datos y los datos personales deben ser tratados en base a cualquiera de los siguientes supuestos:



- i. El consentimiento del sujeto afectado para uno o varios fines específicos: El consentimiento deberá recogerse para cada uno de los fines para los que se recaban los datos y deberá existir una información detallada de cada finalidad y un claro mecanismo para que el interesado pueda consentir afirmativamente de manera individual a cada tratamiento concreto.
- ii. El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. Se encontraría amparado por este supuesto legitimador el tratamiento de datos de clientes, empleados o proveedores siempre y cuando tenga como finalidad el cumplimiento y desarrollo de la relación contractual existente entre el responsable y cada uno de los interesados.
- iii. El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Por ejemplo, en caso de que el responsable cediera los datos de un cliente a Administración Tributaria amparada en una Ley de naturaleza fiscal.
- iv. El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Por ejemplo, la comunicación de datos previo requerimiento por parte de una Autoridad local en el marco de un proceso de investigación.
- v. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Asimismo, este supuesto legítimo se podría dar para procedimientos de reestructuraciones societarias o para la lucha de actividades fraudulentas y contra la corrupción.

## 6.2. Consentimiento

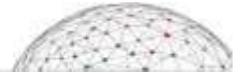
El consentimiento<sup>1</sup> debe ser una manifestación de voluntad libre, informada, inequívoca y explícita. Los silencios e inactividad como base de obtención del consentimiento, así como las casillas pre marcadas, no serán considerados vías de obtención del consentimiento válidas.

Existen varias modalidades que un responsable podrá utilizar para obtener por parte del cliente su manifestación de voluntad libre, informada, inequívoca y explícita:

- Una declaración por escrito mediante:
  - ✓ medios ordinarios, por escrito: formularios, solicitudes concretas de información o de servicios, políticas de protección de datos, contratos, anuncios, leyendas, señales y carteles.

---

<sup>1</sup>El nuevo cambio normativo relativo al consentimiento en materia de protección de datos implica la necesidad de revisar todos los consentimientos otorgados por los interesados con el fin de verificar si, en los casos que sean necesario la obtención del consentimiento, se ha obtenido de una manera que cumpla los requisitos anteriormente mencionados y en caso de que no sea así, proceder a renovar su obtención. Así pues, todos los tratamientos cuya base legal fuera el consentimiento y dicho consentimiento que se hubieren recogido de manera tácita, deberán de remediarse.



- ✓ medios electrónicos:
  - Marcando una casilla afirmativa (opt-in) de un sitio web en internet.
  - Escogiendo parámetros técnicos para la utilización de servicios de la sociedad de la información (como por ejemplo la aceptación del uso de “cookies”).
- Cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales (como por ejemplo la aceptación de un acuse de recibo, a través de un link en un correo electrónico o bien, el envío de un código a introducir en el procedimiento de alta de un servicio).
- Una declaración verbal grabada (telefónicamente).

## 7. SUJETOS INTERVINIENTES

Los establecimientos deberán velar por la seguridad e integridad de la información de carácter personal de la que cada óptica es responsable, así como garantizar que todos los terceros con acceso a datos de la sociedad, es decir, los encargados del tratamiento, asuman el compromiso de cumplir con las garantías y obligaciones legales y contractuales respecto al tratamiento de los datos e información a los que acceden.

Asimismo, la sociedad deberá tener en cuenta que en ocasiones actuará como responsables del tratamiento, pero en el caso de que presten servicios a otras ópticas estarán actuarán como encargados del tratamiento. En este sentido, todos los responsables implicados en el tratamiento de datos personales deberán ajustarse a las obligaciones detalladas a continuación, según actúen como responsables o encargados.

### 7.1. Responsable del Tratamiento

Los responsables de tratamiento (las “Ópticas”) decidirán sobre la finalidad, el contenido y el uso del tratamiento de los datos personales de los clientes, empleados y de todos aquellos interesados con los que mantenga un vínculo. Los empleados que traten o quieran tratar datos de carácter personal, deberán respetar en todo momento las instrucciones y directrices, en materia de protección de datos. Asimismo, los establecimientos tendrán entre sus funciones:

- i. Asegurar que los datos personales que tratan sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.
- ii. Garantizar el cumplimiento de los deberes de secreto y confidencialidad de todos los empleados.
- iii. Informar a los titulares de los datos personales en la recogida de éstos de las finalidades para los que se tratarán, así como obtener el consentimiento expreso para dicho tratamiento en caso necesario
- iv. Facilitar y garantizar el ejercicio de los derechos de los interesados.



- v. Aplicar medidas técnicas y organizativas para poder garantizar un tratamiento lícito y leal de los datos. En este sentido, los establecimientos deberán realizar evaluaciones de impacto en materia de protección de datos, así como mantener un registro de actividades de tratamiento.
- vi. Notificar las “violaciones de seguridad de los datos”, en caso de producirse, a las Autoridades de Control y a los interesados siempre que fuese necesario.
- vii. Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla con lo dispuesto en la normativa sobre protección de datos.

## 7.2. Encargado del Tratamiento

Las Ópticas deberán trasladar a los terceros proveedores de servicios con acceso a datos personales las obligaciones como si el tratamiento fuera realizado por ellos mismos.

Los encargados del tratamiento deberán poner a disposición del responsable de tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como ofrecer garantías suficientes, de manera que el tratamiento sea conforme con los requisitos de la normativa y garantice la protección de los derechos de los afectados por esa relación entre el responsable del tratamiento y el tercero. En este sentido, la adhesión por parte de un encargado de tratamiento a un código de conducta aprobado o a un mecanismo de certificación aprobado puede operar como una garantía.

El encargado del tratamiento deberá ajustarse estrictamente a las instrucciones del responsable. Para poder vincular al encargado respecto del responsable, ambas partes deberán suscribir un contrato que establezca:

- el objeto,
- la duración,
- la naturaleza,
- la finalidad del tratamiento,
- el tipo de datos personales y categorías de interesados, y
- las obligaciones y derechos del responsable y del encargado. Las relativas a los encargados, se enumeran a continuación:
  - i. Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad de los datos de carácter personal.
  - ii. Adoptar las medidas necesarias técnicas y organizativas para garantizar un tratamiento seguro de los datos tomando en consideración el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.
  - iii. Recabar la autorización previa por escrito del responsable, para contratar a otro encargado y asegurarse, mediante contrato, que el subencargado cumple las mismas condiciones para el tratamiento de datos de carácter personal que a él le resultan de aplicación.



- iv. Permitir y cooperar respecto a la realización de auditorías e inspecciones, por parte del responsable.
- v. Asistir al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que éste pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.
- vi. Ayudar al responsable a garantizar el cumplimiento de las obligaciones relativas a las medidas de seguridad, comunicación de brechas de seguridad y evaluaciones de impacto o *PrivacyImpactAssessments*.
- vii. Suprimir o devolver todos los datos personales una vez finalice la prestación de los servicios, y suprimir las copias existentes, a menos que se requiera la conservación de los datos personales.

Será necesario revisar todas las relaciones que mantengan las Ópticas con las terceras empresas proveedoras de servicio que acceden a datos responsabilidad de la óptica con el fin de adaptar su relación jurídica con los nuevos requerimientos regulatorios.

### 7.3. La autoridad de control y los sujetos intervinientes

Cualquier establecimiento responderá frente a la Autoridad de Control que le corresponda. En este sentido, deberá notificar a la Autoridad de Control Local las brechas de seguridad que puedan producirse, solicitarle la autorización previa para determinados tratamientos que impliquen un alto riesgo para los interesados así como el nombramiento del *Data ProtectionOfficer* si ha sido designado.

Asimismo, respecto a aquellas responsabilidades legales y contractuales de los encargados de tratamientos, al igual que en el caso de los responsables, cualquier incumplimiento de las mismas puede conllevar una sanción por parte de la Autoridad de Control.

## 8. DERECHOS DE LOS INTERESADOS

Las Ópticas deberán informar a todas las personas que les faciliten datos personales de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de sus datos de carácter personal, así como la manera de llevar a cabo el ejercicio de sus derechos en relación con el tratamiento de sus datos. El objetivo de dicho principio es que las personas estén informadas de todo el ciclo de vida de sus datos, y sean conscientes tanto de lo que sucede con sus datos, como de cualquier riesgo que pudiera existir y, en particular, de los derechos que les asisten en relación con el tratamiento de datos de carácter personal.

En este sentido, las Ópticas que sean responsables del tratamiento, deberán arbitrar fórmulas para facilitar al interesado el ejercicio de sus derechos de forma gratuita y sencilla.

Asimismo, los establecimientos deberán garantizar al interesado el ejercicio de sus derechos, encontrando como únicos límites a este ejercicio el respeto a los derechos e intereses de terceros, incluidos los secretos comerciales y los derechos de propiedad intelectual, así como la salvaguarda de



la seguridad pública, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, la protección de la seguridad pública, o la protección de un interés público general.

Las Ópticas quedarán obligadas a responder a las solicitudes en relación con el ejercicio de cualquiera de los derechos reconocidos a los interesados sin dilación indebida, eso es, en el plazo de un mes desde el momento de recepción de la solicitud. Asimismo, la respuesta al ejercicio de dichos derechos se realizará por medios electrónicos siempre que el interesado haya presentado su solicitud por medios electrónicos, y esto resulte posible y no desproporcionado para el responsable del tratamiento.

Sin embargo, cuando las solicitudes de ejercicio de los derechos sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá no dar curso a la solicitud del interesado, negándose a actuar.

A continuación, se detallan los derechos que podrán ejercer los interesados frente a las Ópticas:

## 8.1. Derecho de acceso

Los interesados deben tener derecho a acceder a aquellos datos que les conciernan, con el fin de conocer y verificar la licitud del tratamiento que se realiza con los mismos.

Cuando cualquier Óptica decida llevar a cabo la comunicación o cesión a un tercero de los datos de carácter personal del interesado sometidos a tratamiento, deberá facilitar al interesado el acceso a la información identificativa del destinatario de dichos datos. Asimismo, si una Óptica decidiera llevar a cabo una transferencia internacional empleando para ello los datos de carácter personal del interesado sometidos a tratamiento, deberá facilitarle el acceso a la información concerniente a las garantías adecuadas a adoptar en relación con la transmisión de datos personales a un tercer país u organización internacional.

En el supuesto que cualquier Óptica decidiera llevar a cabo la implantación de sistemas para la toma de decisiones automatizadas, tales como la elaboración de perfiles, deberá aportar información relativa, al menos, a la lógica aplicada a la toma de decisiones, así como de las consecuencias derivadas de la toma de decisiones basadas en estas soluciones.

## 8.2. Derecho de rectificación

Los interesados deben tener derecho a solicitar la rectificación de aquella información personal inexacta o incompleta que les concierna, con el fin de verificar la exactitud de la misma y la adecuación al tratamiento que se realiza.

Si alguno de los establecimientos decidiera llevar a cabo la comunicación o cesión a un tercero de los datos de carácter personal del interesado sometidos a tratamiento, y el interesado ejercitase el derecho de rectificación en relación con la información personal sometida a tratamiento por parte de la Óptica, ésta deberá comunicar las rectificaciones realizadas al destinatario de dichos datos, para que las lleve a cabo a su vez, a menos que resulte imposible o suponga un esfuerzo desproporcionado.



### 8.3. Derecho de supresión (“Derecho al olvido”)

Los interesados deben tener derecho a solicitar al responsable del tratamiento la supresión de aquella información que le concierna cuando concurra alguna de las circunstancias siguientes:

- i. Los datos personales ya no resultan necesarios en relación con los fines para los que fueron recogidos o tratados;
- ii. El interesado retire el consentimiento prestado para el tratamiento de sus datos de carácter personal, y este tratamiento no se base en otro fundamento jurídico distinto de dicho consentimiento.
- iii. El interesado se oponga al tratamiento, ejercitando su derecho de oposición, y no existan motivos o intereses legítimos que justifiquen dicho tratamiento, o bien ha ejercitado su derecho de oposición para la recepción de comunicaciones o cualquier otra acción de marketing directo.
- iv. El tratamiento de datos realizado sea ilícito, de conformidad con la normativa en materia de protección de datos.
- v. Los datos deban suprimirse para el cumplimiento de una obligación legal recogida en el ordenamiento español o comunitario.
- vi. El consentimiento para el tratamiento de los datos de carácter personal ha sido prestado por un menor de dieciséis (16) años, sin el consentimiento de sus padres o tutores legales, en el contexto de la prestación de servicios de la sociedad de la información.

No obstante, lo anterior, cualquier Óptica se encontrará excepcionado del deber de supresión cuando:

- i. La supresión pudiera limitar el derecho a la libertad de expresión y/o información.
- ii. Se pretenda garantizar el cumplimiento de una obligación legal recogida en el derecho comunitario o nacional, por parte del responsable del tratamiento, o bien para garantizar el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.
- iii. Se pretenda garantizar la búsqueda de un interés público en el ámbito de la salud pública.
- iv. El tratamiento se encuentra justificado por una finalidad de archivo en interés público, de investigación científica o histórica, con fines estadísticos, y la supresión de los datos sometidos a tratamiento pueda impedir o dificultar estas finalidades.
- v. Se quiera defender y hacer cumplir las reclamaciones.

Si alguna de los establecimientos decidiera llevar a cabo la comunicación o cesión a un tercero de los datos de carácter personal del interesado sometidos a tratamiento, y el interesado ejercitase el derecho de supresión en relación con la información personal sometida a tratamiento por parte de la Óptica, ésta deberá comunicar las supresiones realizadas al destinatario de dichos datos, para que las lleve a cabo a su vez, a menos que resulte imposible o suponga un esfuerzo desproporcionado.

### 8.4. Derecho de oposición

Los interesados que hubieran facilitado sus datos personales, para el cumplimiento de una finalidad determinada, tienen derecho a oponerse, en cualquier momento, y sin justificar dicha decisión, al



tratamiento de dicha información personal. En este sentido la Óptica deberá dar cumplimiento al ejercicio del derecho de oposición cuando concorra alguna de las circunstancias siguientes:

- i. El tratamiento de los datos de carácter personal del interesado tiene como finalidad actividades de mercadotecnia directa (como el envío de comunicaciones comerciales por correo electrónico).
- ii. El tratamiento de los datos de carácter personal del interesado pasa por la elaboración de perfiles, ya sean de personalidad, de comportamientos de clientes, etc.
- iii. El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- iv. El tratamiento es necesario para la satisfacción de intereses legítimos del responsable o un tercero, pero el interesado está en disposición de demostrar que sus intereses y derechos prevalecen sobre los intereses del responsable, especialmente cuando el interesado es menor de edad.
- v. El tratamiento de los datos de carácter personal del interesado se trate con fines estadísticos, por motivos relacionados con su situación particular, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público

Ahora bien, siempre que se den las situaciones enumeradas a continuación, cualquier Óptica podrá excepcionar dar respuesta y cumplimiento a la solicitud de oposición del interesado:

- i. El tratamiento de los datos de carácter personal sea necesario para el cumplimiento de una misión realizada en interés público, cuando los datos personales se procesan con fines de investigación científica o histórica o con fines estadísticos.
- ii. El tratamiento de los datos sea necesario para la satisfacción de intereses legítimos imperiosos del responsable del tratamiento un tercero, pero el tratamiento se considera lícito en tanto que el responsable del tratamiento puede demostrar la prevalencia de sus intereses sobre los intereses y derechos del titular de los datos.
- iii. Para defender y hacer cumplir las reclamaciones.

## 8.5. Derecho a la limitación del tratamiento

Los interesados deben tener derecho a solicitar por parte del responsable del tratamiento la limitación por su parte del tratamiento de aquella información que le concierna, a través de la implantación de métodos tales como:

- Trasladar temporalmente los datos sometidos a tratamiento a otros sistemas de tratamiento.
- Impedir el acceso de usuarios a los datos personales seleccionados.
- Retirar temporalmente los datos publicados, cuando éstos se encuentren publicados en un sitio de internet.
- Emplear medidas técnicas de bloqueo, haciendo inaccesible la información personal sometida a limitación.

El responsable del tratamiento, es decir, cualquier Óptica que trate los datos personales, deberá limitar la información personal concerniente al interesado cuando concorra alguna de las circunstancias siguientes:



- i. El interesado ha impugnado la exactitud de los datos de carácter personal. En tal caso, el responsable deberá limitar el tratamiento de dichos datos durante un plazo que permita al responsable verificar la exactitud de los mismos.
- ii. En aquellos supuestos en los cuales el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos de carácter personal facilitados.
- iii. Cuando la Óptica no pueda extraer ningún tipo de utilidad de los datos recabados para la finalidad para la cual los obtuvo, pero no pueda suprimirlos para permitir al interesado la formulación, el ejercicio o la defensa de reclamaciones.
- iv. En el caso de que el interesado haya ejercitado el derecho de oposición. En ese caso, la Óptica deberá limitar el tratamiento de los datos de carácter personal en el tiempo necesario en que se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

## 8.6. Derecho a la portabilidad de los datos

Los interesados que hubieran facilitado datos personales que les conciernan, tienen derecho a recibir sus datos personales y a transmitirlos a otro responsable, en un formato estructurado, de uso común, de lectura mecánica e interoperable, siempre que el tratamiento esté basado en:

- (i) el consentimiento expreso prestado por el interesado o
- (ii) en el contenido de un contrato suscrito entre el interesado y el responsable del tratamiento, para adoptar medidas a petición del interesado antes de la celebración del contrato y el tratamiento se efectúe por medios automatizados.

Como consecuencia del ejercicio de dicho derecho, y siempre que técnicamente sea posible, el interesado podrá solicitar o bien la recepción de dichos datos o bien que sea la Óptica la que directamente transmita dichos datos personales a otro responsable.

Por último, la normativa recoge que el interesado tendrá derecho a recibir los datos personales que le incumben y haya facilitado a un responsable del tratamiento. Podríamos entender que estarán sujetos por este derecho a la portabilidad, únicamente los datos personales que el interesado haya facilitado a una Óptica, quedando fuera aquellos datos que la óptica pueda tener legítimamente y no haya facilitado el interesado.

Además, el derecho a la portabilidad no provoca automáticamente el borrado de los datos personales del sistema del responsable del tratamiento y no afecta al período de retención original. El interesado podrá ejercer sus derechos mientras el responsable de los datos siga procesando sus datos personales.

## 8.7. Derecho a no ser objeto de una decisión individual automatizada

El interesado tendrá derecho a no ser objeto de una decisión que le afecte, basada en el tratamiento automatizado de información, incluyéndose aquí la elaboración de perfiles.

Sin embargo, la Óptica, podrá no dar cumplimiento a la solicitud del interesado cuando:



- i. la decisión resulte necesaria para la ejecución de un contrato, adoptando siempre las medidas adecuadas para salvaguardar los derechos e intereses legítimos del interesado.
- ii. la toma de la decisión está autorizada por el Derecho Comunitario, o de los Estados Miembros, y el responsable del tratamiento haya adoptado las medidas adecuadas para proteger los derechos e intereses legítimos de interesado.
- iii. el interesado ha prestado su consentimiento explícito para esta finalidad, adoptando siempre las medidas adecuadas para salvaguardar los derechos e intereses legítimos del interesado.

## 9. DELEGADO DE PROTECCIÓN DE DATOS

Las nuevas exigencias legales en materia de protección de datos incluyen la obligación de incorporar, en ciertos casos una nueva figura llamada Delegado de Protección de Datos o *Data Protection Officer* (en adelante, “DPO”) dotada de funciones, responsabilidades y competencias profesionales.

A continuación, se detallarán las funciones y obligaciones del DPO, los supuestos en los que la mencionada figura debe existir en una óptica, así como los requisitos que debe darse en el momento del nombramiento de un DPO.

### 9.1. Supuestos obligatorios existencia DPO

A continuación, se detallan los supuestos en los que resulta obligatorio llevar a cabo el nombramiento de un DPO:

- i. Cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.
- ii. Cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales relativos al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física, así como de datos relativos a condenas e infracciones penales.
- iii. Cuando lo exija el Derecho de la Unión o de los Estados Miembros.

### 9.2. Funciones del DPO

El papel principal del DPO es asesorar a todos los empleados de su óptica para que cumplan con la nueva normativa, así como facilitar información y prestar asesoramiento en materia de protección de datos. A continuación, se detallan las principales funciones que todo DPO debe desempeñar:

- i. Ser el punto de contacto con la Autoridad de Control y con los interesados.
- ii. Cooperar con la Autoridad de Control Local.



- iii. Controlar y supervisar que todos los empleados de la óptica cumplen con la normativa en materia de protección de datos, con sus políticas internas en dicha materia y con las responsabilidades y auditorías que les correspondan.
- iv. Promover la concienciación y garantizar la formación de los empleados de la óptica que tratan datos de carácter personal con el fin de informarles de los derechos y las obligaciones que les incumben como consecuencia de su puesto de trabajo.
- v. Asesorar a las áreas y responsables de la óptica en relación con las evaluaciones de impacto que se lleven a cabo.
- vi. Realizar las consultas necesarias ante la Autoridad de Control Local cuando una evaluación de impacto muestre que el tratamiento entrañaría un riesgo alto para los interesados.
- vii. Supervisar el registro de actividades de tratamiento.
- viii. Comunicar las brechas de seguridad a la Autoridad de Control Local, en 72 horas, cuando entrañe un riesgo alto para los derechos y libertades de las personas físicas.
- ix. Cooperar en los programas de selección de proveedores, para delimitar las obligaciones en materia de protección de datos que dichos terceros deben cumplir,

Asimismo, el DPO deberá cumplir con el deber de secreto y confidencialidad, en lo que respecta al desempeño de sus funciones; poner de manifiesto cualquier cometido adicional al de protección de datos que suponga un conflicto de intereses y actuar en todo momento con la debida diligencia, prestando atención a los riesgos asociados a los tratamientos de datos personales que realice su óptica u ópticas que le tengan designado.

### 9.3. Nombramiento del DPO

El nombramiento voluntario de un DPO resulta aconsejable para la mayor parte de ópticas u organizaciones que lleven a cabo un tratamiento de datos, en la medida en que esta figura puede encabezar el programa de cumplimiento normativo en materia de protección de datos, y actuar como interlocutor intermedio entre las capas ejecutivas de la organización (los más altos niveles jerárquicos) y la Autoridad de Control competente.

La asignación de un DPO deberá realizarse atendiendo, principalmente, a las cualidades profesionales y a la capacidad para desempeñar las tareas en materia de protección de datos. Si bien la normativa no recoge requisitos en relación con la posesión de una cualificación o certificación específica, sí establece que el DPO debe necesariamente tener conocimientos y experiencia en materia de protección de datos.

En este sentido y como consecuencia de lo anteriormente expuesto, cada Óptica deberá designar, como mínimo, en todas sus jurisdicciones, un DPO que asuma las funciones y responsabilidades que exige la nueva normativa. No obstante, lo anterior, podrán designarse tantos DPOs en las distintas sociedades como se consideren necesarios para garantizar el cumplimiento de las obligaciones en materia de protección de datos.

Finalmente, será necesario que cada Óptica colabore con el DPO mediante la puesta a su disposición de los recursos adecuados para la cumplimentación de sus funciones y, en particular, la no obstaculización de la misma, de tal forma que pueda desempeñar las funciones que la normativa le exige en condiciones de independencia y transparencia.

## 10. NOTIFICACIÓN INCIDENTES DE SEGURIDAD



Todas las incidencias de seguridad que posibiliten la materialización de un riesgo que afecte a los datos de los interesados deberán ser notificadas por el responsable del tratamiento a la Autoridad de Control Local competente con la menor dilación posible (antes de 72 horas). Además, cuando el riesgo de la incidencia sea alto, es decir, cuando haya mucha probabilidad de que una persona externa a la óptica acceda o manipule los datos de personas físicas sin autorización, se deberá realizar una comunicación a la persona física afectada tan pronto como sea razonablemente posible y en estrecha cooperación con la Autoridad de Control Local y siguiendo sus orientaciones o las de otras autoridades competentes.

La notificación a la Autoridad de Control Local competente se deberá realizar a través del mecanismo que establezca la Autoridad de Control local para realizar las notificaciones de incidentes de seguridad. Como mínimo, la notificación del incidente deberá contener:

1. La naturaleza del incidente de seguridad de datos personales,
2. Cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
3. El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
4. La descripción de las posibles consecuencias del incidente de seguridad de datos personales.
5. La descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio al incidente de seguridad de datos personales incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

En el caso de que el tratamiento lo realice un proveedor, será el encargado del tratamiento quien notifique al responsable de tratamiento los incidentes de seguridad en materia de privacidad, de las que se tenga conocimiento. Posteriormente, el responsable del tratamiento será el encargado de notificarlo a la Autoridad de Control Local competente de igual forma que se realiza con los demás incidentes.

Para las incidencias que conlleven un riesgo alto para los interesados, la notificación del incidente también deberá ser comunicada a los mismos. Dicha comunicación se realizará en base a la magnitud del esfuerzo necesario para la notificación. Cuando sea posible la notificación se deberá hacer de forma individual sobre cada afectado, a través de medios de comunicación directa como un correo electrónico, una llamada telefónica, un aviso en el área privada del cliente o un correo postal, teniendo en cuenta siempre que ésta debe ser demostrable y con posibilidad de seguir su trazabilidad (no es necesario un acuse de recibo por parte de los interesados). En caso de que la notificación suponga un esfuerzo desproporcionado, se podrán tomar medidas alternativas como publicaciones a través de prensa nacional/internacional.

De igual forma que las notificaciones a la Autoridad de Control competente, éstas como mínimo deberán contener:

1. Descripción de la naturaleza y ocurrencia del incidente de seguridad de datos personales.
2. Detalles de los datos que han sido accedidos.
3. Recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes del incidente.

En cualquier caso, será necesario consultar con la Autoridad de Control Local la mejor forma de abordar la situación y realizarla en base a las pautas que sean determinadas a raíz de la consulta.



## 11. INVENTARIO DE TRATAMIENTOS

Toda Óptica deberá mantener un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. La obligación de dicho registro se extiende al Responsable del tratamiento y al Encargado del tratamiento, si bien el contenido de la información que deberá contener el registro del Responsable del tratamiento será distinto que el que deberá llevar a cabo el Encargado del tratamiento.

Se define tratamiento de datos de carácter personal a cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias de datos que identifican a una persona física o pueden hacer que la identifique de manera directa o indirecta.

Se deberá mantener un repositorio donde se registren todos los tratamientos que se realicen en la organización en base a 2 criterios:

- a) Tratamientos realizados por la Óptica por cuenta propia (responsable de tratamiento).
- b) Tratamientos realizados para la prestación de un servicio a otra sociedad (encargado de tratamiento).

No es obligatorio comunicar el registro de actividades a la Autoridad de Control Local, ahora bien, deberá estar a disposición de ésta si ésta lo requiere. Será el DPO de la óptica que recibe la petición quien hará efectiva la comunicación.

El registro que deberá llevar a cabo el encargado del tratamiento se refiere a las categorías de actividades de tratamiento efectuadas por cuenta del Responsable del tratamiento, y no del detalle de todos los tratamientos.

Cada área de la óptica, tendrá que recopilar toda la información necesaria para realizar el registro de sus actividades de tratamiento. El DPO local tendrá que revisar y verificar la completitud y validez de la información recogida. Si hubiera cualquier aspecto a modificar se informaría al área responsable.

## 12. *PRIVACY IMPACT ASSESSMENT*

Los tratamientos de datos personales están expuestos a riesgos durante su ciclo de vida, riesgos que deben ser gestionados y reducidos en la medida de lo posible hasta un nivel razonable. El Reglamento General de Protección de Datos introduce el concepto de PrivacyImpactAssesment (PIA), una nueva herramienta de análisis de riesgos enfocados a la privacidad de los datos personales.

La regulación establece en qué casos es necesario realizar un PIA, que información debe contener, la involucración del DPO, etc. Sin embargo, el PIA es un elemento que necesita una metodología que permita realizar un enfoque lo más objetivo posible y que establezca los pasos mínimos y requerimientos de información que debe incluir un PIA.

Antes de la realización del PIA, se debe establecer un análisis previo inicial para determinar en qué casuísticas y circunstancias será necesario su realización y en qué casos se podrán admitir excepciones. El Reglamento General de Protección de Datos, recoge tres casos donde sí es obligatorio realizar un PIA:



- evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar, o;
- tratamiento a gran escala de las categorías especiales de datos o datos personales relativos a condenas e infracciones penales, o;
- observación sistemática a gran escala de una zona de acceso público (videovigilancia).

Adicionalmente, las Autoridades de Control Locales emitirán listas de tratamientos donde será obligatorio la realización de un PIA y opcionalmente emitirán listas de casos que estarán excepcionados.

El DPO local actuará como figura de asesoramiento durante la realización del PIA y deberá realizar la aprobación final del mismo. No se puede llevar a cabo un tratamiento, que requiera obligatoriamente la realización de un PIA, sin la autorización del DPO local.

Si se determina la necesidad de realizar un PIA, se debe poner en marcha la metodología establecida para la ejecución de este procedimiento para identificar las amenazas y riesgos asociados y, a posteriori, evaluar el impacto y la probabilidad de que se materialicen los riesgos identificados. Dicha metodología deberá ser revisada por el DPO.

Es importante destacar que se debe plantear un enfoque de máximos, dentro de lo razonable, a la hora de determinar las medidas de control, con el objetivo de reducir la exposición al riesgo lo máximo posible.

Para poder decidir si el PIA es favorable y se lleva a cabo o no un tratamiento se debe establecer un criterio estandarizado que permita determinar el nivel de riesgo residual aceptable. EL DPO deberá formar parte del equipo de la realización del PIA, asesorando en la ejecución del mismo.

Aquel tratamiento cuyo resultado del PIA sitúe en un nivel de riesgo alto no se podrá llevar a cabo. El DPO local deberá proceder a realizar el procedimiento de consulta previa a la Autoridad de Control Local.

Todo PIA deberá contar con un informe final y un plan de acción asociado que incluya las medidas de control implantadas para llevar a cabo dicho tratamiento.

## 13. SANCIONES

Será necesario un deber de concienciación de dichos derechos y obligaciones que pueda trasladarse desde posiciones de alto nivel jerárquico a todos los empleados de las distintas ópticas o unidades que tratan datos personales en su operativa diaria.

El incumplimiento de las obligaciones de protección de datos puede estar sujetas a multas administrativas que pueden ir de los 10.000.000€ o 20.000.000€ EUR o de una cuantía equivalente al 2% o 4 % del volumen de negocio total anual global. Las sanciones previstas por el Reglamento General de Protección de Datos, afectarán a la totalidad del Grupo y no se verán individualizadas a una concreta filial o a un determinado país. Como consecuencia de lo anterior, es fundamental el íntegro cumplimiento de los estándares recogidos en este Marco, que serán la base de mínimos, en materia de



Comunidad  
de Madrid

ASOCIACIÓN  
ÓPTICAS  
MADRID



Compliance & Conduct



protección de datos, que cualquier compañía deberá cumplir en el tratamiento de datos de carácter personal.

# 1.1

## *Listado del cumplimiento del RGPD*



## LISTADO DE CUMPLIMIENTO DEL RGPD

CUMPLE

SI / NO

PRINCIPIOS RELATIVOS AL TRATAMIENTO	REVISIÓN PERMANENTE
Se recogen los datos personales con fines determinados	
Se recogen los datos personales con fines explícitos	
Se recogen los datos personales con fines legítimos	
Se tratan ulteriormente de manera incompatible con otros fines	
Los datos personales se mantienen exactos	
Se mantienen actualizados	
Se rectifican los datos personales inexactos respecto de la finalidad	
Se suprimen los datos personales inexactos respecto de la finalidad	
Se mantienen durante más tiempo del necesario respecto de la finalidad	
Se tratan con fines de archivo en interés Público	
Se tratan con fines de investigación científica	
Se tratan con fines históricos	
Los datos personales se tratan con fines estadísticos	
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	
Se mantiene la trazabilidad de los fines del tratamiento	
LICITUD DEL TRATAMIENTO	REVISIÓN PERMANENTE
Se tiene consentimiento para cada finalidad del tratamiento	
El tratamiento es necesario para ejecutar un contrato o precontrato	
Existe obligación legal	
El tratamiento es necesario para proteger intereses vitales	
El tratamiento es necesario para el cumplimiento de interés Público	
El tratamiento es necesario para satisfacer intereses legítimos	
CONDICIONES PARA EL CONSENTIMIENTO	REVISIÓN PERMANENTE
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	

Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal	
Se solicita el consentimiento de forma clara e independiente de los demás asuntos	
Se solicita el consentimiento de forma inteligible y de fácil acceso	
Se solicita usando lenguaje claro y sencillo	
Se informa con carácter previo a recabar el consentimiento	
Se permite retirar el consentimiento con la misma facilidad que se recaba	
Se ofrecen medios para retirar el consentimiento en cualquier momento	
Se recaba el libre consentimiento	
Para prestar un servicio se solicitan sólo los datos necesarios	
Para ejecutar un contrato se solicitan sólo los datos necesarios	
<b>CONSENTIMIENTO DE NIÑOS EN RELACIÓN CON LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN</b>	<b>REVISIÓN SEMESTRAL</b>
Se recaba el consentimiento de menores de 16 años al titular de la patria potestad o tutela sobre el niño	
Se verifica que el consentimiento fue dado por el titular de la patria potestad o tutela sobre el niño	
<b>TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS</b>	<b>REVISIÓN SEMESTRAL</b>
Se tratan los datos sólo cuando existen normas que lo exceptúen	
Se tratan los datos con consentimiento explícito y no existen normas de derecho que prohíban expresamente su tratamiento	
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que está establecido por las normas de derecho	
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que existe un convenio colectivo con arreglo a derecho	
Es necesario para proteger los intereses vitales de una persona y el interesado no está capacitado, física o jurídicamente, para dar su consentimiento	
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y se refiere exclusivamente a los miembros actuales o antiguos o a personas que mantienen contactos regulares en relación con la finalidad (política, filosófica, religiosa o sindical)	
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y no se comunican a terceros sin consentimiento de los interesados	

Se tratan datos que el interesado ha hecho manifiestamente Públicos	
Es necesario para la formulación, el ejercicio o la defensa de reclamaciones	
Es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstica médica, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social	
Es necesario por razones de interés Público en el ámbito de la salud Pública sobre la base de normas de Derecho que establecen medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional	
Es necesario con fines de archivo en interés Público, fines de investigación científica o histórica o fines estadísticos en base de normas de derecho	
Se realiza cumpliendo las condiciones con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud que establece la normativa nacional	
<b>TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES</b>	<b>REVISIÓN SEMESTRAL</b>
Se tratan los datos bajo la supervisión de las autoridades Públicas	
Se tratan los datos bajo la autorización de normas de derecho	
El registro completo de condenas penales se realiza bajo el control de las autoridades Públicas	
<b>TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN</b>	<b>REVISIÓN TRIMESTRAL</b>
Se mantiene información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación	
Se obtiene y/o trata información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación	
Se puede demostrar que los datos anonimizados no permiten identificar a los interesados	
Se informa al interesado y se recaba su consentimiento cuando se llega a su identificación	
Se cancelan los datos cuando se llega a identificar al interesado	
<b>TRANSPARENCIA DE LA INFORMACIÓN</b>	<b>REVISIÓN PERMANENTE</b>
Se toman medidas para facilitar al interesado toda la información relativa al tratamiento	
La información se facilita de forma concisa, transparente e inteligible	
La información se facilita en lenguaje claro y sencillo	
Se facilita por escrito o por otros medios, incluidos los electrónicos	
Se facilita verbalmente, previa acreditación de su identidad	

Se facilita al interesado el ejercicio de sus derechos	
Se atienden las peticiones del ejercicio de derechos, aunque el tratamiento no requiera identificación salvo que no se pueda identificar al interesado	
Se informa al interesado en el plazo de un mes desde la recepción de su solicitud	
Se informa ante el ejercicio de derechos complejos o ante muchas solicitudes en el plazo máximo de tres meses desde la recepción de la solicitud	
Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de la dilación	
Se permite a los interesados el ejercicio de derechos por medios electrónicos	
Se informa por medios electrónicos cuando se recibe la solicitud por esos medios salvo que solicite que se realice por otro medio	
Se informa de las razones de la no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales, en el plazo de un mes desde la recepción de la solicitud cuando no se da curso a la solicitud	
Se facilita gratuitamente el ejercicio de derechos	
Se solicita información para acreditar la identidad de la persona física que ejerce sus derechos	
Cuando la información que se facilita utiliza iconos normalizados, el formato electrónico es legible mecánicamente	
<b>INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO</b>	<b>REVISIÓN PERMANENTE</b>
Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos	
Se facilitan los datos de contacto del delegado de protección de datos	
Se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento	
Se facilita información sobre el interés legítimo	
Se informa sobre los destinatarios o las categorías de destinatarios	
Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo	
Se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad	
Si el tratamiento se basa en el consentimiento se informa de la existencia del derecho a retirarlo en cualquier momento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	

Se informa de las cesiones basadas en requisitos legales o contractuales	
Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato	
Se informa de la existencia de decisiones automatizadas, elaboración de perfiles, sobre la lógica aplicada, la importancia y consecuencias previstas del tratamiento	
Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente	
<b>INFORMACIÓN A FACILITAR CUANDO LOS DATOS NO SE OBTIENEN DEL INTERESADO</b>	<b>REVISIÓN PERMANENTE</b>
Se informa de la identidad y los datos de contacto del responsable y, en su caso, de su representante	
Se informa de los datos de contacto del DPD	
Se informa de los fines del tratamiento	
Se informa de la base jurídica del tratamiento	
Se informa de las categorías de datos personales de que se trate	
Se informa de los destinatarios o las categorías de destinatarios de los datos	
Se informa del plazo durante el cual se conservarán los datos personales	
Se informa de los criterios utilizados para determinar este plazo o el plazo de conservación cuando no es posible informar del mismo	
Se informa de los intereses legítimos concretos en que se basa el tratamiento	
Se informa del derecho a solicitar el acceso a sus propios datos personales	
Se informa del derecho a solicitar la rectificación de sus datos	
Se informa del derecho a solicitar la supresión	
Se informa del derecho a la limitación del tratamiento	
Se informa del derecho a oponerse al tratamiento	
Se informa del derecho a la portabilidad de los datos	
Se informa de la existencia del derecho a retirarlo el consentimiento en cualquier momento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	
Se informa de la fuente de la que proceden los datos personales	
Si proceden de fuentes de acceso público, se informa de ello	
Se proporciona la información antes de un mes	
Si los datos personales se utilizan para comunicación con el interesado, se le comunica la información a que tiene derecho en el momento de	

la primera comunicación	
Si está previsto comunicar los datos personales del interesado a otro destinatario, se le comunica la información a más tardar en el momento en que los datos personales son comunicados por primera vez	
Se informa al interesado si se realizan tratamientos para finalidades diferentes de la que fueron recogidos	
No se informa cuando ya dispone de la información el interesado	
No se informa cuando la comunicación de dicha información resulta imposible o supone un esfuerzo desproporcionado	
No se informa porque puede imposibilitar u obstaculizar gravemente el logro de los objetivos del tratamiento pero se adoptan medidas para proteger los derechos, libertades e intereses legítimos del interesado	
No se informa porque la obtención o la comunicación está expresamente establecida por normas de derecho aplicables	
No se informa porque los datos personales tienen carácter confidencial sobre la base de una obligación de secreto profesional regulada por normas de Derecho	
<b>DERECHOS DEL INTERESADO. DERECHO DE ACCESO</b>	<b>REVISIÓN TRIMESTRAL</b>
Se informa respecto a los fines del tratamiento	
Se informa de las categorías de datos personales que se tratan	
Se informa de los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales	
Se informa del plazo previsto de conservación de los datos personales	
Se informa de los criterios utilizados para determinar el plazo de conservación	
Se informa del derecho a solicitar la rectificación o supresión de sus datos	
Se informa del derecho a solicitar la limitación del tratamiento de los datos	
Se informa del derecho a solicitar la oposición al tratamiento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	
Se proporciona información sobre el origen de los datos cuando no recogen del propio interesado	
Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo solicita	
Se facilita la información en formato electrónico de uso común si lo solicita por medios electrónicos salvo que se facilite otro medio	
<b>DERECHO DE RECTIFICACIÓN</b>	<b>REVISIÓN TRIMESTRAL</b>
Se rectifican los datos personales inexactos sin dilación indebida	

Se completan los datos personales incompletos teniendo en cuenta los fines del tratamiento	
<b>DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO»)</b>	<b>REVISIÓN TRIMESTRAL</b>
Se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos	
Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento	
Se suprimen los datos cuando se opone al tratamiento	
Se suprimen los datos cuando han sido tratados ilícitamente	
Se suprimen los datos cuando lo exige una obligación legal	
Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la información	
<b>DERECHO A LA LIMITACIÓN DEL TRATAMIENTO</b>	<b>REVISIÓN TRIMESTRAL</b>
Se limita el tratamiento durante un plazo para verificar la exactitud de los datos, cuando el interesado impugna su exactitud	
Se limita el tratamiento cuando es ilícito y el interesado se opone a la supresión de sus datos personales y solicita en su lugar la limitación de su uso	
Se limita el tratamiento cuando no son necesarios para los fines pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones	
Se limita el tratamiento cuando el interesado se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado	
Se informa al interesado cuando se levanta la limitación del tratamiento	
<b>INFORMACIÓN AL INTERESADO ANTE RECTIFICACIÓN, SUPRESIÓN O LIMITACIÓN EN EL TRATAMIENTO</b>	<b>REVISIÓN TRIMESTRAL</b>
Se comunican al interesado la rectificación, supresión o limitación en el tratamiento	
<b>DERECHO A LA PORTABILIDAD DE LOS DATOS</b>	<b>REVISIÓN TRIMESTRAL</b>
Se facilitan los datos cuando el interesado lo solicita en un formato estructurado, de uso común y lectura mecánica	
Se transmiten dichos datos a otro responsable si el tratamiento está basado en el consentimiento o en un contrato	
Se transmiten dichos datos si el tratamiento se efectúe por medios automatizados	
Se transmiten los datos al nuevo responsable que el interesado determina, si es posible técnicamente	
<b>DERECHO DE OPOSICIÓN</b>	<b>REVISIÓN TRIMESTRAL</b>
Se atienden las solicitudes de oposición y se dejan de tratar los datos	

Se atienden las solicitudes de oposición pero no se dejan de tratar los datos por motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, los derechos y las libertades o para la formulación, el ejercicio o la defensa de reclamaciones	
Se ponen los medios necesarios para que pueda ejercer su derecho a oponerse por medios automatizados	
<b>DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES</b>	<b>REVISIÓN SEMESTRAL</b>
No se realizan tratamientos que supongan la toma una decisión basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque es necesario para la celebración o la ejecución de un contrato	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque están autorizados en Derecho	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque se cuenta con el consentimiento explícito	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para salvaguardar el derecho a obtener intervención humana por parte del responsable	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para dar al interesado ocasión de expresar su punto de vista e impugnar la decisión	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con el consentimiento del interesado	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con habilitación legal	
Se informa a los interesados acerca de estas decisiones individuales automatizadas y de la habilitación legal de las mismas	

Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado	
<b>RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO</b>	<b>REVISIÓN PERMANENTE</b>
Se tiene en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento para garantizar y poder demostrar que el tratamiento es conforme con el RGPD	
Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas	
Se aplican medidas técnicas y organizativas apropiadas	
Las medidas se revisan y actualizan cuando es necesario	
Se han confeccionado políticas de protección de datos	
Se aplican las políticas de protección de datos	
<b>PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO</b>	<b>REVISIÓN PERMANENTE</b>
Se analizan las medidas técnicas y organizativas apropiadas antes de determinar los medios de tratamiento	
Durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD	
Durante el tratamiento se aplican las medidas que han sido determinadas	
Durante el tratamiento se comprueba la efectividad de las medidas aplicadas	
Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines	
Se aplican medidas técnicas y organizativas teniendo en cuenta la cantidad de datos personales recogidos, la extensión de tratamiento, el plazo de conservación y la accesibilidad	
Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal	
<b>CORRESPONSABLES DEL TRATAMIENTO</b>	<b>REVISIÓN TRIMESTRAL</b>
Se han determinado de modo transparente, y de mutuo acuerdo las responsabilidades respectivas de los corresponsables en el cumplimiento de las obligaciones impuestas por el RGPD	
El acuerdo fija las respectivas obligaciones de suministro de información al interesado	
El acuerdo entre corresponsables del tratamiento refleja las funciones y relaciones respectivas de ambos en relación con los interesados	
Los aspectos esenciales del acuerdo están a disposición del interesado	
<b>ENCARGADO DEL TRATAMIENTO</b>	<b>REVISIÓN TRIMESTRAL</b>

Se eligen los que ofrecen garantías suficientes conforme con los requisitos del RGPD y garantizando la protección de los derechos del interesado	
El encargado del tratamiento no recurre a otro encargado sin la autorización previa por escrito	
El tratamiento por el encargado se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho	
El contrato establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados así como las obligaciones y derechos de responsable	
El contrato establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas de responsable	
El contrato garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad y están sujetas a una obligación de confidencialidad de naturaleza estatutaria	
El contrato establece que se tomarán las medidas de seguridad necesarias	
El contrato establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento	
El contrato establece que el encargado asistirá para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados	
El contrato establece que se suprimirán o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales	
El contrato establece que pondrá a disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable	
El contrato establece que si el encargado del tratamiento recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se imponen a este otro encargado las mismas obligaciones de protección de datos que las estipuladas en el contrato, mediante contrato u otro acto jurídico establecido con arreglo a Derecho	
El contrato consta por escrito	
Sólo se accede a los datos siguiendo instrucciones del responsable	
<b>REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO</b>	<b>REVISIÓN TRIMESTRAL</b>
Se lleva un registro de las actividades de tratamiento	
El registro recoge el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos	

El registro recoge los fines del tratamiento	
Recoge una descripción de las categorías de interesados y de las categorías de datos personales	
Recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales	
Recogen las transferencias de datos personales a un tercer país o a una organización internacional, incluida la identificación de dicho tercer país u organización internacional	
Incluye los plazos previstos para la supresión de las categorías de datos	
Incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos	
<b>NOTIFICACIÓN DE BRECHAS DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL</b>	<b>REVISIÓN TRIMESTRAL</b>
Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad	
Existe un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas	
Existe un procedimiento para notificar a la autoridad de control en el plazo de 72 horas	
Existe un procedimiento para documentar los motivos por los que no se puede notificar en el plazo de 72 horas	
Existe un procedimiento para facilitar la información de manera gradual cuando no es posible facilitarla simultáneamente	
Se documenta cualquier brecha de seguridad de los datos personales	
En la documentación se incluyen los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas	
Se ha comprobado que el procedimiento de notificación funciona	
<b>COMUNICACIÓN DE UNA BRECHA AL INTERESADO</b>	<b>REVISIÓN TRIMESTRAL</b>
Existe un procedimiento para comunicar la brecha sin dilación indebida cuando sea probable que entrañe un alto riesgo para los derechos y libertades	
La comunicación al interesado, se lleva a cabo en un lenguaje claro y sencillo, describe la naturaleza de la brecha	
<b>EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS</b>	<b>REVISIÓN TRIMESTRAL</b>
Se recaba el asesoramiento del DPD	
Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgo para los derechos y libertades de las personas	

Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales	
Se realiza una EIPD antes de tratamiento que suponen una observación sistemática a gran escala de una zona de acceso público	
Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada por la autoridad de control	
La EIPD incluye una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, y cuando procede el interés legítimo perseguido	
Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad	
La EIPD incluye una evaluación de los riesgos para los derechos y libertades	
Incluye medidas previstas para demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas	
Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos	
Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de los riesgos que representen las operaciones de tratamiento	
Se consulta a la autoridad de control antes de proceder al tratamiento cuando una EIPD muestre que el mismo entrañaría un alto riesgo si no se toman medidas para mitigarlo	
Se informa de las responsabilidades respectivas de los implicados en el tratamiento en la consulta a la autoridad de control	
Se informa de los fines y medios del tratamiento previsto en la consulta	
Se informa de las medidas y garantías establecidas para proteger los derechos y libertades en la consulta	
Se facilitan los datos de contacto del delegado de protección de datos	
Se incluye la evaluación de impacto	
Cuando se consulta se facilita cualquier información adicional que solicite la autoridad de control	
<b>DELEGADO DE PROTECCIÓN DE DATOS</b>	<b>REVISIÓN SEMESTRAL</b>
Se ha designado un DPD por requerimiento legal	
Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia	
Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control	

Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales	
Se da respaldo en el desempeño sus funciones	
Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento	
Se le facilitan los recursos necesarios para mantener sus conocimientos	
Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones	
No se puede destituir ni sancionar al DPD por desempeñar sus funciones	
El DPD rinde cuentas directamente al más alto nivel jerárquico	
El DPD atiende las solicitudes de los interesados	
El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones	
Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto de intereses	
Las funciones del DPD son informar, asesorar y formar al personal de las obligaciones que les incumben	
El DPD coopera y actúa como punto de contacto con la autoridad de control	
<b>TRANSFERENCIAS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES</b>	<b>REVISIÓN ANUAL</b>
Se realizan transferencias a países, o sectores de los mismos, u organizaciones internacionales declarados de nivel de protección adecuado por la Comisión Europea	
Se realiza un seguimiento de la validez de las decisiones de adecuación de la Comisión europea	
Se realizan transferencias mediante garantías adecuadas que ofrezcan a los interesados derechos exigibles y posibilidad de acciones legales.	
Existe un instrumento jurídico vinculante y exigible entre las autoridades u organismos públicos	
Existen normas corporativas vinculantes	
Existen cláusulas tipo de protección de datos adoptadas por la Comisión	
Existen cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión	
Existe un código de conducta junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existe un mecanismo de certificación junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existen cláusulas contractuales que requieren la autorización previa de	

la autoridad de control	
Existen acuerdos administrativos entre autoridades y organismos públicos que incorporen disposiciones que incluyan derechos efectivos y exigibles para los interesados	
Se realizan transferencias internacionales en ausencia de decisión de adecuación de la Comisión europea y de garantías adecuadas	
Se dispone del consentimiento explícito del interesados y se le ha informado de los posibles riesgos	
Son necesarias para la ejecución de un contrato con el interesado o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado	
Son necesarias para la formulación, ejercicio o la defensa de reclamaciones	
Son necesarias para la protección de los intereses vitales del interesado o de otras personas, cuando el interesado esté incapacitado para dar su consentimiento	
Por intereses legítimos imperiosos	
Afecta a un número limitado de interesados y no es repetitiva	
Se han evaluado todas las circunstancias concurrentes y se han ofrecido garantías apropiadas	
Se ha informado a la autoridad de control	
<b>SEGURIDAD DEL TRATAMIENTO</b>	<b>REVISIÓN PERMANENTE</b>
Para determinar las medidas a aplicar se tiene en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas	
Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo	
Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	
Medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico	
Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	
Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado	

Se han tomado medidas para garantizar que las personas autorizadas a acceder a datos sólo los tratan siguiendo instrucciones	
<b>CONTROLES DE SEGURIDAD DEL TRATAMIENTO PROPUESTOS</b>	<b>REVISIÓN SEMESTRAL</b>
Se realiza un control de accesos físicos al CPD	
Se implementan las medidas adecuadas de protección física en CPD	
Cuenta con un inventario de gestión de soportes y está debidamente actualizado y preparado	
Se realiza una adecuada gestión de soportes a través de medidas como cifrado o borrado seguro	
Se lleva a cabo un debido control de accesos lógicos de administradores y usuarios a los sistemas operativos y a aplicaciones o una debida segregación de funciones	
Se lleva a cabo un buen control de accesos lógicos a sistemas operativos y aplicaciones, contando para ello con políticas de contraseñas	
Cuenta con registro de los accesos realizados a aplicaciones y bases de datos de los usuarios	
Se realizan copias de seguridad y, en caso de que la contestación sea afirmativa, con qué frecuencia son realizadas esas copias de seguridad (indicar en comentarios)	
Se realizan pruebas de restauración de copias en función de los planes de acción previstos	
Se procede a la eliminación de ficheros temporales o en el caso contrario, no se cuenta con procedimientos o políticas de uso de medios que indiquen lo contrario	
Resiliencia: redundancia y recuperación	
Procedimientos de continuidad de negocio.	
Comunicaciones cifradas. Procesos de encriptación o cifrado de la información para lograr que sea ilegible.	
Auditoría técnica de sistemas	
Gestión de vulnerabilidades de sistemas y aplicaciones	
Cifrado en equipos y dispositivos móviles	
Seguridad en entornos de desarrollo y test.	
Medidas dirigidas a lograr la Seudoanonimización /Anonimización de datos personales. Por ejemplo, a través de Hash o del cifrado de datos.	
Test de intrusión a través de Pentesting.	
Otras medidas de seguridad	

# 2

## ***Corporate Defense – Modelo de Cumplimiento y Prevención Penal***



**Comunidad  
de Madrid**

**ASOCIACIÓN  
ÓPTICAS  
MADRID**



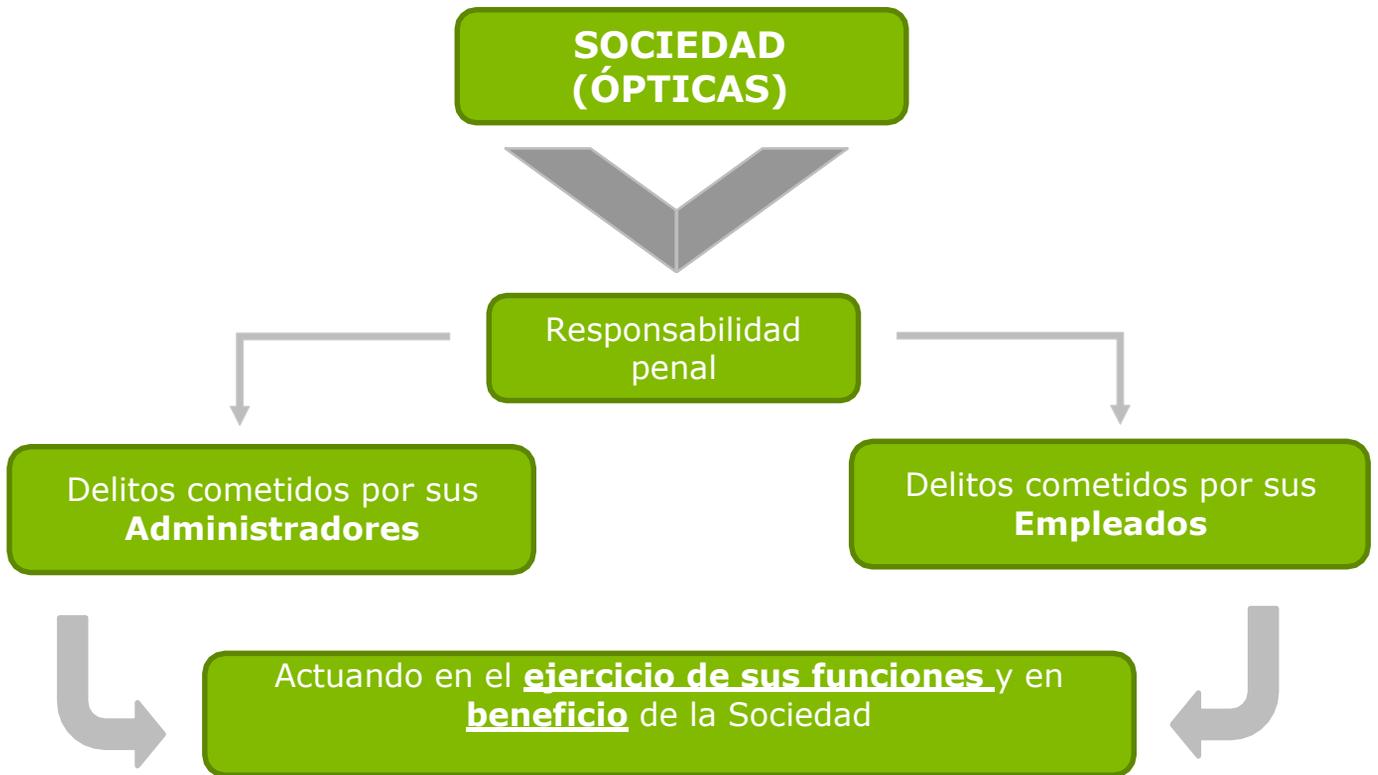
## **Corporate Defense - Modelo de Cumplimiento y Prevención Penal**

Octubre de 2018

# La responsabilidad penal de la persona jurídica



## ¿Qué es la responsabilidad penal de la persona jurídica?



**2010:** Se introduce la **responsabilidad penal de la persona jurídica** por la comisión de determinados delitos por sus directivos o empleados en el ejercicio de su cargo. La responsabilidad penal **se puede atenuar** si la empresa cuenta con medidas eficaces para prevenir y detectar delitos.

**2015:** **Ausencia de responsabilidad criminal** de la persona jurídica cuando haya adoptado **medidas de prevención de delitos**, no exista una omisión por parte del órgano de control y el autor haya infringido fraudulentamente los controles.



Modelo de  
Cumplimiento  
y Prevención  
Penal

# ¿Puede ser la persona física también responsable penal?

---

**Sí**

Responsabilidad penal para la persona jurídica **no exime a la persona física.**



Junto a la persona jurídica, **también es responsable la persona física autora del delito.**



# ¿Qué implica la condena penal de la persona jurídica?



## Persona física

- **Multa** por cuotas o proporcional
- **Penas de prisión**
- **Inhabilitación especial para licitar**
- **Inhabilitación especial para empleo o cargo público**
- **Inhabilitación especial para el ejercicio de industria o comercio**

- **Daños reputacionales**
- **Acciones por daños**
- **Ineficiencias empresariales y desviación de recursos**
- **Inseguridad jurídica**
- **Distorsiones en el funcionamiento del mercado**
- **Dificultades en el proceso de internacionalización**

## Otras consecuencias <sup>7</sup>

# ¿Puede evitarse la responsabilidad penal de la persona jurídica?

## CONDICIONES DE EXENCIÓN (31 bis 2,4)

### Si el delito lo comete un administrador o persona con capacidad de decisión, organización o control...

1. El órgano de administración haya ejecutado con eficacia, antes de la comisión del delito, **modelos de organización y gestión** con mecanismos idóneos de prevención de delitos.
2. La supervisión y funcionamiento del modelo haya sido confiada a un órgano con poderes autónomos de iniciativa y control o que legalmente tenga asignada la función de supervisión.
3. Los autores hayan eludido fraudulentamente el modelo.
4. No concurra una omisión o ejercicio insuficiente de las labores de supervisión por parte del órgano de control.

### Si el delito lo comete un empleado...

En este caso, la persona jurídica podrá **eximir su responsabilidad** también cuando haya **ejecutado un modelo eficaz de organización y gestión con medidas idóneas para prevenir delitos**.

**Modelo de organización y gestión o Modelo de Cumplimiento y Prevención Penal**

# ¿Puede evitarse la responsabilidad penal de la persona jurídica?

## REQUISITOS DE LOS MODELOS DE COMPLIANCE (31 bis 5)

Confiar la **supervisión y funcionamiento del Modelo a un órgano con poderes** autónomos de iniciativa y control.



**Identificar las actividades** en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos (evaluación del riesgo).



Imponer la obligación de informar de posibles riesgos e incumplimientos al órgano de vigilancia.



**Establecer los protocolos que concreten el proceso de formación de la voluntad de la persona jurídica**, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.



Establecimiento de un sistema **disciplinario** que sancione adecuadamente el incumplimiento del modelo.



Disponer de **modelos de gestión de los recursos financieros** adecuados para impedir la comisión de los delitos que deberán ser prevenidos.



**Realizar una verificación periódica del modelo** y su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización.

# Modelo de Cumplimiento y Prevención Penal



# Modelo de Cumplimiento y Prevención Penal

El **Modelo de Cumplimiento y Prevención Penal** establece el conjunto de elementos para prevenir, detectar y reaccionar ante la comisión de delitos en la organización mediante:



**ÓRGANO DE CONTROL INTERNO (COMITÉ DE PREVENCIÓN DE RIESGOS PENALES)**



**MAPA DE RIESGOS PENALES  
(MATRIZ DE RIESGOS Y DE CONTROLES)**



**CANAL DE DENUNCIAS**



**CÓDIGO ÉTICO  
POLÍTICA DE CUMPLIMIENTO  
Y PREVENCIÓN PENAL  
MANUAL DE CUMPLIMIENTO  
Y PREVENCIÓN PENAL**



**SISTEMA DISCIPLINARIO**



**PARTIDA PRESUPUESTARIA  
CONTROL FINANCIERO**



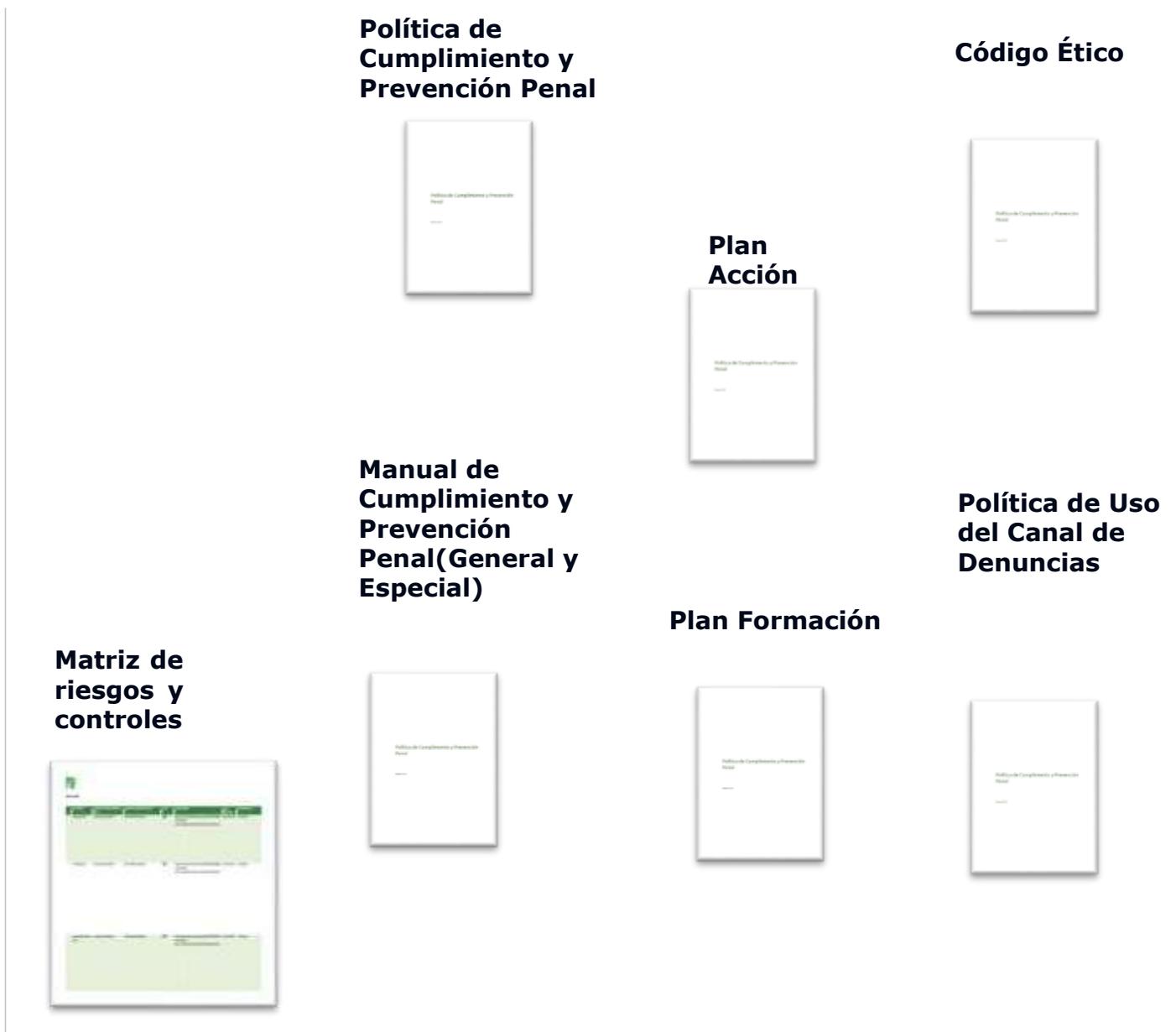
**PLAN DE SUPERVISIÓN  
PLAN DE VERIFICACIÓN**

¿Dónde está el Modelo de Cumplimiento y Prevención Penal?

# Modelo de Cumplimiento y Prevención Penal

El **Modelo de Cumplimiento y Prevención Penal** se configura, principalmente, a través de los siguientes documentos:

## Modelo de Cumplimiento y Prevención Penal



# Comité de Prevención de Riesgos Penales

---

## Principales características

Esencialmente, las características que debe reunir el Comité de Prevención de Riesgos Penales son las siguientes:



Conocimiento detallado de las actividades de la Sociedad.



Autoridad para asegurar el carácter vinculante de las decisiones.



Autonomía e independencia que garantice su credibilidad, evitando posibles situaciones de conflictos de interés.



Es recomendable que, en conjunto, el órgano cuente con expertos en: organización y gestión empresarial, asuntos legales, finanzas, etc.



Deben tratar la información a la que accedan con la máxima confidencialidad.

# Comité de Prevención de Riesgos Penales

---

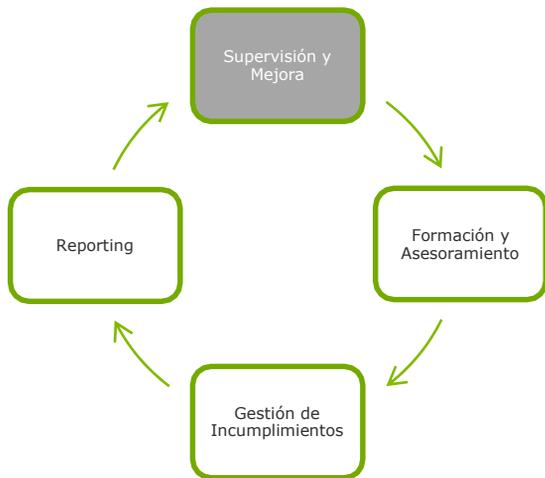
## Principales funciones

El **Comité de Prevención de Riesgos Penales**, formado por el equipo directivo o de administración, es el órgano responsable de:



# Comité de Prevención de Riesgos Penales

## Supervisión y Mejora

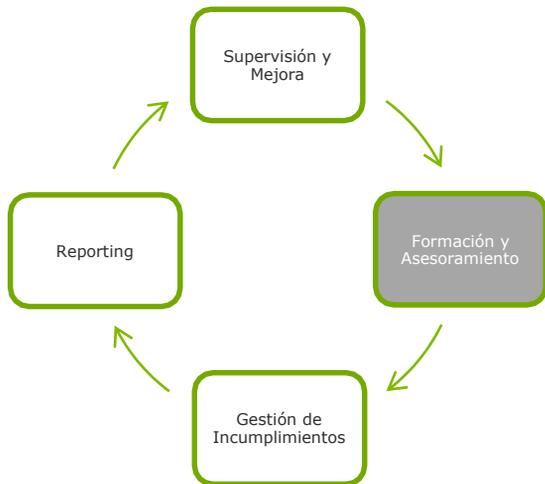


- **Vigilar el funcionamiento, eficacia y cumplimiento** del Modelo.
- Adoptar y/o coordinar la **adopción de medidas** para garantizar el cumplimiento del Modelo.
- Analizar las **modificaciones legislativas y demás novedades.**

# Comité de Prevención de Riesgos Penales

---

## Formación y Asesoramiento



- Garantizar la **difusión de los principios generales y éticos** de la Sociedad y promover la preparación e implementación de programas adecuados de formación.
- Asesorar en la **resolución de las dudas** que puedan surgir en la aplicación de los códigos y manuales o cualquier otro tipo de duda respecto del Modelo.

# Comité de Prevención de Riesgos Penales

---

## Gestión de Incumplimientos



- **Gestionar los posibles incumplimientos** del Modelo y comunicar de forma inmediata al Consejo de Administración las infracciones del Modelo.

# Comité de Prevención de Riesgos Penales

---

## Reporting



- Anualmente comunicar el **grado de cumplimiento al Consejo de Administración** y proponer las mejoras oportunas.

# ¿Qué hacer si creo haber detectado la comisión de un delito?

## Canal de Denuncias

### ¿Qué conductas se pueden denunciar?

- Aquellas que supongan un **riesgo de comisión de delito**...
- Aquellas **contrarias al Código Ético** de la Sociedad...

...que hayan sido **cometidos por cualquier empleado, directivo o miembro del Consejo** de Administración.

### ¿Cómo denunciar?

Acceso a la **plataforma** del Canal de Denuncias en la **intranet** y **completar el formulario**.



La denuncia deberá contener la siguiente información: (i) identidad del denunciante si queremos identificarnos, (ii) **identidad del denunciado**, (iii) **tipo de infracción cometida** y, en su caso (iv) **documentación soporte** en la que se basa la denuncia.

### ¿Quién recibe y gestiona las denuncias?

La Sociedad encarga la **gestión e investigación de las denuncias** recibidas al asesor externo que tiene la obligación de promover y preservar, entre otros, los siguientes aspectos:

- ✓ confidencialidad,
- ✓ fiabilidad y transparencia,
- ✓ rapidez y eficacia en la reacción,
- ✓ trazabilidad de las actuaciones.

**Recepción:** asesor externo

**Prohibición de represalias**

**Sanción a la denuncia falsa**

# Procedimiento disciplinario

## PROCEDIMIENTO DISCIPLINARIO

La existencia de normas, políticas y procedimientos es condición esencial para el éxito de una empresa. Corresponde a la Sociedad garantizar que se sigan para el funcionamiento correcto y eficaz de la organización. Los desvíos o incumplimientos pueden dar lugar a la aplicación de **medidas disciplinarias** que, cuando se apliquen, deben servir como **elemento reactivo y sancionador**, al mismo tiempo que **educador y creador de cultura**.

Por tanto, los empleados tienen la **obligación de conocer y cumplir las normas interna**. Todos los incumplimientos serán sancionados de acuerdo con el Convenio Colectivo aplicable a la Sociedad, la legislación laboral y el resto de obligaciones civiles y mercantiles que haya contraído el trabajador como consecuencia de su relación laboral.



**¿Sabías que.....?**

Como parte integrante de la Sociedad, estás obligado a:



**Cumplir las normas, políticas y procedimientos de la empresa**



**Denunciar situaciones irregulares o susceptibles de ser consideradas delito**



**Denunciar incumplimientos del Código Ético**

# 2.1

## *Listado compliance de Cumplimiento y Prevención Penal*



LISTADO COMPLIANCE	SI/NO	COMENTARIOS
¿Cuenta la Sociedad con un Modelo de cumplimiento y prevención penal?		
¿El Modelo de cumplimiento y prevención penal cuenta con un <b>mapa de riesgos penales</b> (matriz de riesgos y controles)?		
¿El Modelo de cumplimiento y prevención penal cuenta con un <b>código ético</b> interno de la sociedad?		
¿El Modelo de cumplimiento y prevención penal cuenta con una <b>Política de cumplimiento y prevención penal</b> ?		
¿El Modelo de cumplimiento y prevención penal cuenta con un <b>Manual de cumplimiento y prevención penal</b> ?		
¿Cuenta la Sociedad con una <b>partida presupuestaria</b> que permita llevar un <b>control financiero</b> ?		
¿Cuenta la Sociedad con un <b>canal de denuncias</b> interno?		
¿Se cuenta con un <b>sistema disciplinario</b> ?		
Con el fin de poder verificar y supervisar lo anterior, ¿La Sociedad tiene redactado un plan de verificación y supervisión?		



# 3

## ***Estrategias de Marketing Digital***

### ***SEO \$ SEM***

# ESTRATEGIAS DE MARKETING DIGITAL SEO & SEM



Más visibilidad para vuestros  
Centros Ópticos



**Comunidad  
de Madrid**



Si los clientes  
buscan tu producto no  
te encuentran.....



Crees que te pueden comprar

# ¿Cómo compraban los usuarios.....?



Estímulo  
(Televisión,  
medios de  
comunicación)



Primer  
momento de la  
verdad  
(estantería)



Segundo  
momento de la  
verdad  
(Experiencia)



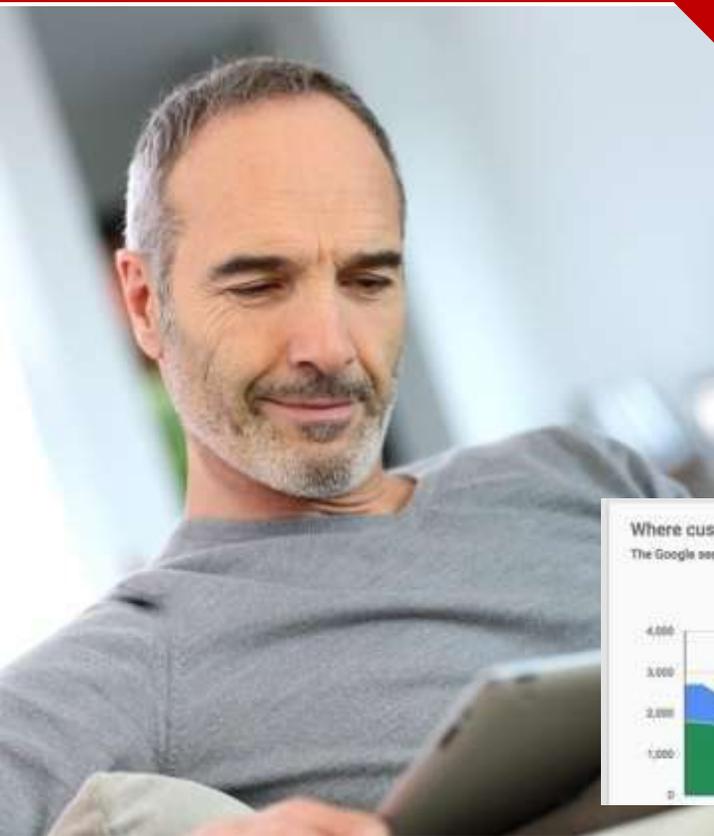
# ¿Cómo compran ahora.....?



Él es el protagonista.....  
Conocerlo es esencial



# La importancia para vuestro negocio



El 82 % de los consumidores utilizan motores de búsqueda para encontrar Información sobre empresas locales.  
(fuente Google)



# SEO LOCAL

## Esencial para vuestras Ópticas

BÚSQUEDAS  
GEOLOCALIZADAS

Ordenadores - IP

Móvil - GPS



# ¿Porqué Google da tanta importancia a las búsquedas locales?

Mejorar

la experiencia de búsqueda del usuario.



Búsqueda

Tiempo de carga

# Búsquedas Locales

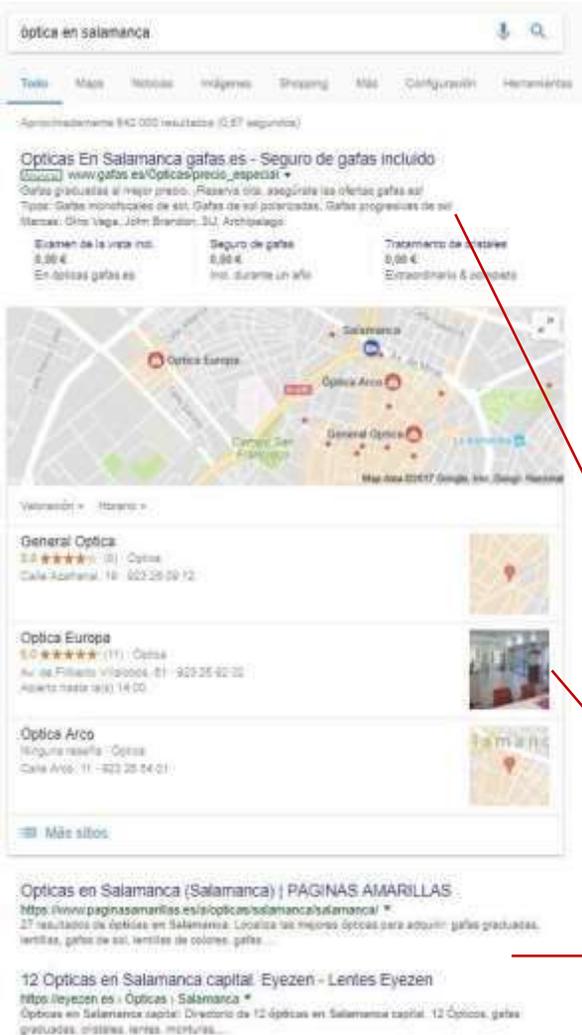
¿Cómo son...?

Al hacer una búsqueda en el buscador

■ Anuncios (SEM/PPC)

■ SeoLocal

■ Seoorgánico



# ¿Qué NECESITAS para tener posicionamiento Local?

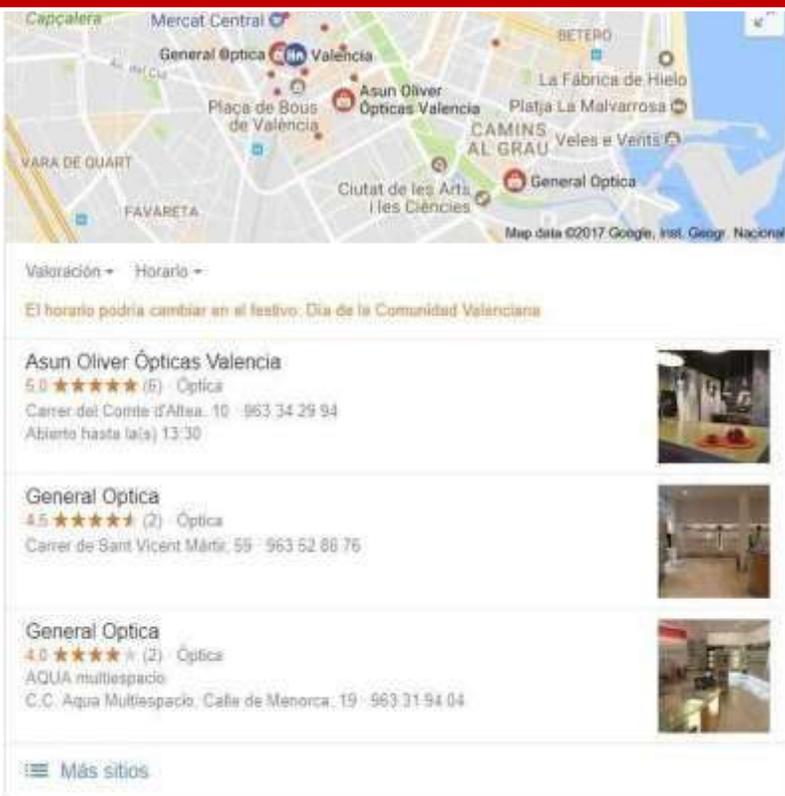
- Página Web

- Una cuenta asociada a servicios Google(gmail)

- Una cuenta en Google My Business



# Consejos para mejorar el Posicionamiento local

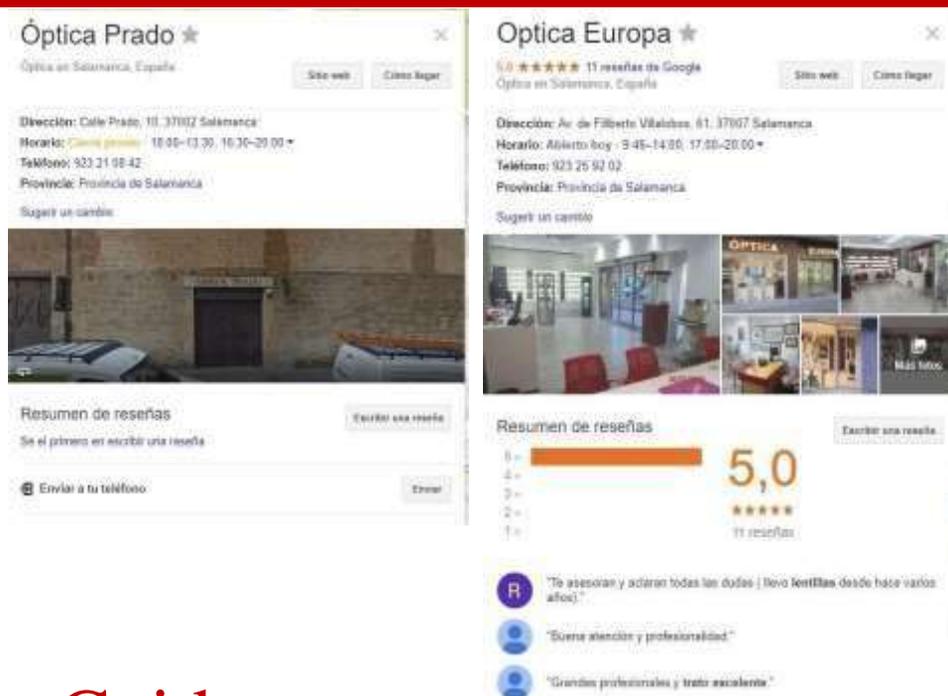


Especial atención a las valoraciones de clientes

- Generan confianza
- Mejoran el posicionamiento
- Mayor visibilidad

 **Contestar Reseñas**

# Consejos para mejorar el Posicionamiento local



¿Si fuerais el Usuario... a cuál iríais?

Cuidar y actualizar

- Subir Fotos
- Añadir publicaciones
- Mantener el horario
- Contestar reseñas

# ¿Qué NECESITAS para tener posicionamiento Local?

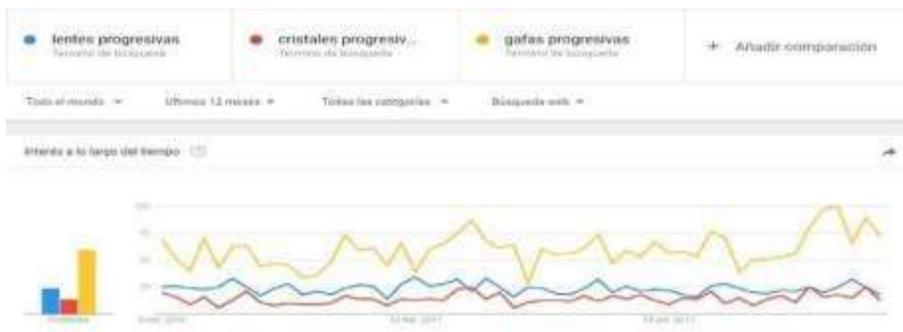


El contenido es el

# REY

## ¿Cómo lo aplico a mi centro óptico?

- El contenido necesita ser creado en el lenguaje adecuado, es decir, el lenguaje que tu usuario utiliza cuando emplea el buscador.
  - Identifica los temas de interés de tus usuarios.
    - Investiga qué palabras clave emplean para localizar esos contenidos en los buscadores.
    - No te olvides de las KWs long tail.
  - Investigación del contenido y las KWs



# Para atraer tráfico a tu óptica Se pueden hacer muchas cosas

## Generación de “leads”

- PPC
  - SEM:Adwords
  - Facebookads
  - Display
- Emailing
- SMS

## Conocimiento Marca(Branding)

- Generación de contenido
- Social Media
  - Blog
  - Facebook
  - Twitter
  - Pinterest
- Street Marketing

# Analizar las búsquedas

## Keyword research



- El usuario busca...
- Analizar la búsqueda y si es clave para el objetivo de negocio.
  - “He ido al oculista y me ha dicho que tengo presbicia”

# Focalizarse en las que generan objetivo de negocio



- Precio de gafas
- Precio de Gafas de Sol
- Precio Gafas de sol Tous
- Precio Gafas Sol TOUS  
STO943 09RG

# Objetivos / Priorizar

- Identificar tus objetivos
- Priorizar



# Focalizarse Keywords que generan objetivo de negocio



# Factores relevantes del seo

## Factores más relevantes:

- 1 Web rastreable.
- 2 Gestionar duplicados.
- 3 Velocidad de carga.
- 4 Estructura de URLs.
- 5 Móvil.



# Campañas PPC

Google  
AdWords



Pago por clic  
Modo subasta

# SEO vs. SEM

lentillas progresivas

3 Resultados de páginas (valor: 47,88%), gratis la mayoría de estos grupos de resultados. Ver [cómo comprar](#) para más opciones de compra.

Tudo Shopping Imágenes Videos Noticias Más Configuración Herramientas

Aproximadamente 233.000 resultados (0,25 segundos)

**Lentillas Gratis - Prueba las Lentes Air Optix - mejorconlentillas.com**  
[Accede](#) [www.mejorconlentillas.com/Air-Optixgratis](#)  
¡Llévate Gratis tu Primer Par! Siéntete la comodidad en tus ojos.  
Lentillas Gales (Gala) · Lentillas Air Optix Gratis · Consigue lentillas gratis.  
Consejos útiles · Encuentra tu óptica

**Lentillas Progresivas | Multifocales Online - Óptica Óptima**  
[Accede](#) [www.optica-optima.com](#)  
Visión de [optica-optima.com](#) 4.3 ★★★★★  
Compra Gafas de Sol de Primeros Marcos al Mejor Precio con Envío en 24 Horas.  
Gafas de Sol Camera 5003 · Gafas de Sol Tous · Gafas de Sol Camera · Gafas de Sol Oakley

**Lentillas Progresivas - LentesDeContacto365.es**  
[Accede](#) [www.lentesdecontacto365.es](#) · 911 41 32 18  
Lentes de Contacto 365 La Mayor Óptica Online de España  
Línea Apoyo 12 Horas Día · Garantía Satisfacción 100% · Envío Rápido · Stock 24h

**Lentillas progresivas - Ampio Stock Aquí - opticalens.es**  
[Accede](#) [www.opticalens.es/opticasaranda-de-quezo](#)  
Venta de Gafas para Mejorar Problemas de la Visión · Graduadas y sin Graduar.  
Productos competitivos · Telescopios y prismáticos · Lentes oftálmicas.  
Óptica Lats · Gafas Solares · Noticias · Productos · Contacto

**1. Lentillas Progresivas o Multifocales | Vision Direct**  
[www.visiondirect.es/contacto-lentes-multifocal-contacto-lentes](#)  
Compra Lentillas Progresivas online en Vision Direct. Precios bajos en lentes de contacto progresivas y envío rápido en VisionDirect.es.

Get Your results with free SEMrush account - Contact Us

1. 18 2. 375 3. 43,84 4. 3884 5. Apr 2007/10/18 6. active 7. inactive

8. Rank 5,87M 9. Air Day Ads 10. Pub Day Ads 8

**2. ¿Cómo adaptar lentillas progresivas? » Presbicia o vista cansada**  
[https://presbiciaovertacansada.com/adaptacion-lentillas-progresivas/](#)  
15 mar 2016 · En este artículo te mostramos cómo es la adaptación a las lentillas progresivas. Sus pros y sus contras. Pincha aquí: Presbicia · Lentillas.

**Comprar lentillas progresivas** Patrocinador

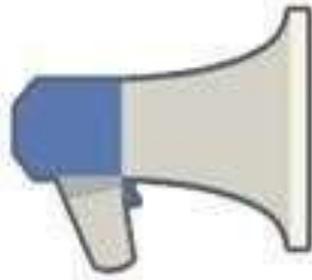
 Bionity Multifocal (3... 27,45 € VisionDirect.es ★★★★★ (53) De Google	 Lentillas Air Optix Aqua F... 15,00 € lentesexpress De Google	 Air Optix Aqua Multifocal (5... 43,90 € Lentes-de-conta... De Google
 Air Optix Aqua Multifocal (3... 21,25 € Óptica ESP Envío gratis De Google	 Acuvue Oasys (5 lentes) 18,20 € Lentes-de-conta... De Google	 Lentillas Soflene Daily 95 24,95 € lentesproec De Google
 Bionity Multifocal (3... 22,59 € Óptica ESP Envío gratis De Google	 Piscobar 1 Day Multifocal (3E... 19,50 € MoodOptic ES De Google	 Air Optix Aqua Multifocal (5... 42,70 € Lentillas.es ★★★★★ (66) De Google

# SEM: Campaña Adwords

- Se tienen en cuenta 2 costes:
  - Coste gestión de la campaña:
  - Inversión en Adwords
- Con la segmentación adecuada del Centro óptico (ubicación geográfica, potencial, nivel de inversión) se puede obtener buen nivel de visitas a tienda, o de llamadas
- En estos gabinetes, los resultados son inmediatos.

# FacebookAds

- Anuncios en Facebook
- Segmentación
- Alcance del Público



**facebook.** Ads

Crear nuevo

Usar un público guardado ▼

Públicos personalizados ⓘ

**Dirige tus anuncios a las personas que conocen tu negocio** ✕  
Puedes crear un público personalizado para mostrar los anuncios a tus contactos, visitantes del sitio web o usuarios de la aplicación.  
[Crear un público personalizado.](#)

Lugares ⓘ

Todas las personas en este lug... ▼

España

📍 España

📍 Incluir ▼ [Agrega lugares.](#)

[Agregar varios lugares...](#)

Edad ⓘ

65 ▼

- 65+ ▼

Sexo ⓘ

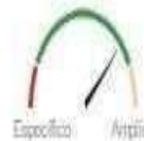
Todos

Hombres

Mujeres

Idiomas ⓘ

Tamaño del público



Tu selección de público es bastante amplia.

Tamaño total: 7.500 personas

Resultados diarios estimados

Alcance

950 - 2.500 (de 5.300)

Es solo una estimación. Los números que se muestran se basan en el rendimiento de tu campaña anterior, pero no garantizan resultados.

Segmentación detallada ⓘ

**INCLUIR** personas que cumplan al menos UNA de las siguientes condiciones ⓘ

Comportamientos > Usuario de dispositivo móvil > Todos los dispositivos móviles por marca > Apple

iPhone 7

[Agrega datos demográficos, intereses o comport...](#) [Sugerencias](#) [Explorar](#)

[Excluir personas](#) o [Aotar público](#)

Conexiones ⓘ

# Emailing



- Una manera de mantener activo al cliente online (y de ofrecer más)



## Caso práctico: Formación redes sociales

- 1. ¿Por qué me interesa la presencia digital y por dónde empezar?**
- 2. Principales redessociales**
  1. Twitter
  2. Facebook
  3. LinkedIn
  4. Instagram
- 3. Herramientas de trabajo**

# 1-¿Por qué me interesa la presencia digital y por dónde empezar?

## ALCANCE



- ✓ Dar a conocer tu mensaje
- ✓ Amplificar tu mensaje
- ✓ Aumentar tu red de contactos
- ✓ Atraer tráfico

## ACTIVIDAD



- ✓ Fomentar interacciones
- ✓ Persuadir la participación
- ✓ Clave el contenido
- ✓ Intercambio de información a tiempo real

## CONVERSIÓN



- ✓ Llamadas a la acción para involucrar a movilizarse

## DELEITE



- ✓ Construir relaciones de lealtad y compromiso
- ✓ Conoces a las personas a las que te diriges

Debemos tener **OBJETIVOS CLAROS** y, a partir de ahí, **CREAR LAS ESTRATEGIAS** correspondientes. Una buena estrategia se basa en investigaciones de marketing y en **CONOCER EL PERFIL** de nuestros clientes y dónde están en internet.

## 1-¿Por qué me interesa la presencia digital y por dónde empezar?

**“Tu marca personal es lo que dicen de ti cuando tú no estás delante”**

Jeff Bezos, CEO de Amazon

**“Céntrate en la identificación de tu público objetivo, comunicando un mensaje auténtico que él quiera y necesite, y proyéctate a ti mismo como un „experto“ dentro de tu nicho.” – KimGarst**

# 1-¿Por qué me interesa la presencia digital y por dónde empezar?

Estrategia, táctica y objetivos -ejemplo

OBJETIVO	ESTRATEGIA	TÁCTICA
Aumentar la cantidad de Seguidores	Sorteos	Sortear un premio entre los seguidores de Facebook 1 vez al mes
	Promociones	Lanzar un descuento del 10% en alguno de los servicios por 15 días , después del lanzamiento del curso
	Generar Contenido de Valor	Regalar 1 recurso al mes, crear videos, contenidos en el blog y compartirlos en las RRSS

# 1-¿Por qué me interesa la presencia digital y por dónde empezar?

Caso práctico

Actividad propuesta. Ahora es tu turno.

- Trazatu propio plan de comunicación en redes sociales.
- Ten en cuenta tus objetivos personales.
- Define tu estrategia y traza tu plan de acción para los próximos meses.

## 2-Principales redes sociales

### Twitter



- ✓ Definir el **NOMBRE** que tendrá tu perfil (nombre +apellido o un nombre nuevo).

### Apertura de perfil

- ✓ Definir las **PALABRAS CLAVES** que definen tu perfil.

- ✓ **MENSAJE** que quieres transmitir.
- ✓ **VALORES** que se transmitirán, esos que tienen que estar presente en el diseño de la nueva marca personal.
- ✓ El **TONO DE COMUNICACIÓN** que se empleará, si será formal o más bien coloquial.
- ✓ La **IMAGEN Y DISEÑO** que tendrá la marca personal: logos, tipografías, colores...
- ✓ Selección de las **REDES SOCIALES y CANALES** donde te interesa estar
- ✓ Creación de un **CALENDARIO DE CONTENIDOS** para redes sociales.



### Importancia de la biografía

- ✓ Foto desenfocada, de lejos, no se ve quien escribe, está oscuro.
- ✓ Bio inapropiada.
- ✓ 89 notificaciones sin leer
- ✓ Usuario difícil de recordar



- ✓ Foto de perfil nítida y clara
- ✓ Bio ordenada y descriptiva.
- ✓ Uso de hashtag en los que nos queremos posicionar.

## 2-Principales redes sociales

### Twitter



**Información  
a tiempo  
real**

Crea una  
RED DE  
CONTACTOS  
con usuarios  
de tu sector

Comparte  
CONTENIDO  
útil e  
interesante

No te FÍES de  
todo lo que se  
publica

Utiliza  
#HASHTAGS

Establece y  
fomenta  
conversaciones  
INTERACTÚA

Cuida tu  
presentación  
IMPORTANCIA  
DE LA  
BIOGRAFIA

HAZ  
LLAMADAS A  
LA ACCIÓN

ESCUCHA  
ANALIZA Y  
HABLA

TONO  
INFORMATIVO  
E INFORMAL

## 2-Principales redes sociales

### Facebook



#### Interacción con la comunidad

INTERACTÚA  
CON TUS  
FANS

EL  
CONTENIDO  
VISUAL ES  
MUY  
IMPORTANTE

MENOS ES  
MÁS  
(no publicar  
demasiado)

ALCANCE  
ORGÁNICO  
ESTÁ MUY  
LIMITADO

RESUELVE  
DUDAS

IMPORTANCIA  
DEL VÍDEO Y  
NUEVOS  
FORMATOS

HAZ  
LLAMADAS A  
LA ACCIÓN

ESCUCHA  
ANALIZA  
Y HABLA

TONO  
CERCANO Y  
EMOCIONAL



**Ampliar  
público  
joven**

EL  
CONTENIDO  
VISUAL  
Es muy  
importante

AMPLIAR  
PÚBLICO  
objetivo

Tono MÁS  
INFORMAL,  
PERSONAL,  
CERCANO Y  
EMOCIONAL

DAR LIKES Y  
SEGUIR  
para crecer

STORIES y  
contenido a  
tiempo real

AMPLIAR  
temáticas  
CONTENIDOS

Uso de  
#HASHTAGS

## 2-Principales redes sociales

LinkedIn



**Ampliar  
público con  
profesionales  
de tu sector**

Posiciónate  
como  
experto del  
SECTOR

OFRECE  
estudios,  
contenidos  
de interés

Tono MÁS  
PROFESIO  
NAL pero  
CERCANO

Información  
muy  
completa  
en el  
PERFIL de  
empresa

Trabaja la  
IMAGEN  
CORPORATIVA

Uso de  
#HASHTAGS

- Construcción de nuestra identidad en la red. ¿En qué redes sociales os interesa estar?
- Crea un perfil de Twitter, completa la biografía, establece una portada y empieza a tuitear y a seguir a las personas que te interesan.
- ¿Qué plan de contenidos y tono vas a usar?  
¿Cómo te quieres posicionar?

“Cada maestrillo tiene su librillo”

- **Gestión de redes:**

- **HOOTSUITE:** gestión global y monitorización de redes sociales todo en uno, que permite gestionar varias cuentas a la vez con un panel de control muy visual e intuitivo que nos ofrece infinidad de datos y funcionalidades interesantes.
- **TWEETDECK:** La eterna competencia de Hootsuite. Permite sólo la gestión de cuentas de Twitter.
- **SOCIALBRO:** Junto a las anteriores, cumple una gran función en Twitter, permitiendo filtrar contactos mediante la creación de listas, siguiendo, dejando de seguir, te permite conocer cuál es tu mejor hora para tuitear, y muchas otras funcionalidades que podéis probar en su versión gratuita.
- **MANAGER FILTER:** Aplicación muy completa para analizar tu actividad en Twitter: seguidores, quién no te sigue, usuarios inactivos, y muchísimas cosas más. De este modo, podemos mantener siempre nuestra cuenta en un estado óptimo, recibiendo información útil para llevar a cabo las necesarias limpiezas de usuarios que ya no nos interesa seguir. Podemos introducir un término o categoría de interés y nos devuelve una lista de usuarios a los que seguir.

- **Analítica de redes: “Lo que no se mide no existe”.**
  - **TWEETBINDER**: Mide el impacto de una campaña en Twitter, estadísticas, usuarios más activos, etc, ofreciendo un análisis muy fiable y pormenorizado. Es ideal para poner en valor el trabajo del Community Manager ante el jefe o cliente, y reivindicar con cifras concretas la importante labor que desempeña el gestor de comunidades online.
  - **SOCIALBAKERS**: Herramienta para la gestión integral de las analíticas de todas las redes sociales.
  - **GOOGLE ANALYTICS**: identificar lo que sucede con el tráfico que dirige a su sitio web o blog.
  - **FACEBOOK ANALYTICS**: el sistema de analítica de Facebook.
  - **TWITTER ANALYTICS**: el sistema de analítica de Twitter.
  - **LINKEDIN ANALYTICS**: el sistema de analítica de LinkedIn.
  - **INSTAGRAM ANALYTICS**: el sistema de analítica de Instagram.
  - **YOUTUBE ANALYTICS**: el sistema de analítica de Youtube.

- **Contenido:**

- **COPYSCAPE**: Detecta si hay en la red contenido duplicado de tu web o blog, es decir, podemos localizar dónde y quién ha copiado contenidos de nuestro sitio.
- **GOOGLE TRENDS**: Detectar las tendencias de búsqueda en Google en un momento o período determinado.
- **BITLY**: Acortador de URLs muy útil para ahorrar caracteres. Además, monitoriza los clics que se realizan a dichos enlaces y puedes organizarlos por carpetas, lo cual resulta muy práctico a la hora de sacar informes de clics por clientes.
- **FEEDLY**: Podemos gestionar los artículos que seguimos a través de los *feeds* a los que estamos suscritos.
- **SOCIAL MENTION**: Buscador de contenidos en diferentes Redes Sociales, permitiendo conocer dónde mencionan a la marca.

- **Herramientas de diseño:**
  - **CANVA**
- **Bancos de imágenes:**
  - **PIXABAY:** En él podemos encontrar multitud de fotografías, algunas de ellas de gran calidad, de muy diversos temas. No es necesario registrarse abriendo una cuenta para descargar nada y es muy fácil y rápido encontrar enseguida alguna imagen que se adapte a nuestras necesidades.
  - **PEXELS:** Si buscas necesitas fotografías diferentes y de calidad para alguna de tus redes sociales, esta herramienta permite adquirirlas sin abrirte una cuenta y sin preocuparte por los derechos de autor, ya que todas sus imágenes son libres.
  - **FREEPIK:** banco de vectores, imágenes y fotografías que se ha hecho muy popular es todo un *must* en las community herramientas. La mayor parte de su contenido es gratuito, pero también ofrecen algunas ventajas con la suscripción de pago a su servicio, como contenido exclusivo o la posibilidad de usar las imágenes sin necesidad de hacer mención.

- **Monitorización: ¿Qué se dice de nosotros?**
  - **BRANDWATCH**: Monitorización de todo lo que se dice de tu marca a tiempo real.
  - **BÚSQUEDA AVANZADA DE TWITTER**
  - **BÚSQUEDA AVANZADA DE IMÁGENES DE GOOGLE**
  - **BÚSQUEDA AVANZADA DE NOTICIAS DE GOOGLE**
  - **TRENDSMAP**
- **Mailings:**
  - **MAILCHIMP**
- **Concursos en redes sociales:**
  - **EASSYPROMOS**
  - **COOLTABS**

Aumentar comunidad en Twitter a través de seguir y dejar de seguir perfiles con la herramienta Manager Filter.

Fijar una estrategia de **generación de CONTENIDOS DE CALIDAD** que sirvan para atraer a nuestra comunidad ganándonos su confianza y reforzando nuestro prestigio como profesionales expertos en nuestra área.

**ANALIZAR** cada acción que emprendemos y los resultados que proporciona.

Debemos estar permanentemente estudiando qué acciones nos acercan a nuestros objetivos y cuáles no.



**SEGMENTAR** al detalle a nuestro público objetivo. Debemos conocerles con todo detalle: sus gustos, expectativas, necesidades... y por encima de todo debemos aportarles **SOLUCIONES**.

**CONSTANCIA Y PERSEVERANCIA:** todas estas técnicas ofrecen resultados a medio plazo.