# Política de Datos Personales

## Departamento de Ciberseguridad y Delegado de Protección de Datos

## Políticas de Seguridad de la Información

| | |
|---|---|
| **Código del documento** | SEG-PY-XXX |
| **Versión** | 3.0 |
| **Fecha de aprobación** | 16-12-2020 |

| Elaborado | Revisado | Aprobado |
|---|---|---|
| Nombre:<br><br>Departamento Ciberseguridad | Nombre:<br><br>Departamento: Delegado de Protección de Datos | Nombre:<br>Departamento: Comité de Privacidad |

# Índice

# 1. Control de Versiones

| | | | |
|---|---|---|---|
| **Versión actual** | 1.0 | | |
| **Historial de Cambios** | **Fecha de modificación** | **Versión** | **Comentarios del cambio** |
| | 28-02-2019 | 1.0 | Versión inicial |
| | 31-08-2020 | 2.0 | Revisión DPD |
| | 16-12-2020 | 3.0 | Aprobado DPD |

# 2. Introducción

El Reglamento General de Protección de Datos (en adelante, RGPD), en vigor desde el 25 de mayo de 2016 y en aplicación dos años más tarde, supone un complejo cambio legislativo sobre las actividades de tratamiento de datos personales y la privacidad. Este cambio desarrollado por el Parlamento Europeo supone aumentar el nivel de protección de los derechos de los ciudadanos que se encuentren en la Unión Europea (en adelante, UE). Cualquier entidad que trata datos personales (incluidos los sitios web, aplicaciones móviles, etc.) con personas físicas que estén en la UE o si las actividades de tratamiento se realizan desde la UE, se verán afectadas por este reglamento.

Por tanto, la presente Política de Protección de Datos Personales complementa, en sus aspectos específicos, a la Política General de Sistemas de Información de Grupo Masmovil (en adelante, Grupo) y dará una serie de directrices generales para tratar los aspectos principales del RGPD, centrada en exponer las cuestiones fundamentales que plantean los principios de protección de datos y el uso de datos personales conforme a las bases jurídicas de la normativa de protección de datos que con más asiduidad se dan en el ámbito de la empresa.

Para tratamientos específicos y para ahondar en el contenido de los conceptos esbozados en este documento, los Comités de Privacidad y de Ciberseguridad, apoyados por el Delgado de Protección de Datos deberán realizar un esfuerzo adicional para asegurar que el tratamiento datos es siempre conforme con la normativa vigente en cada momento.

# 3. Objetivo

Uno de los objetivos y requisitos clave de RGPD es mantener a los ciudadanos de la UE informados sobre cómo las empresas recopilan, utilizan, comparten, protegen y procesan sus datos personales. Por tanto, es fundamental que el Grupo esté al tanto de esta legislación y sea de aplicación para todo su personal.

# 4. Alcance

Por su carácter de Política General, va dirigida, en primer lugar, a los Responsables de Tratamientos a quienes resulte aplicable el RGPD, así como a los profesionales que contribuyen, ya sea dentro del Grupo o bien como Encargados de Tratamiento con el fin de cumplir de forma eficiente las obligaciones que les incumben en virtud del Reglamento. Finalmente, incluye, también, a todas las herramientas informáticas que se encarguen, o bien, de almacenar, o bien, de tratar dichos datos.

# 5. Descripción

## Información básica sobre protección de datos

Con el fin de concienciar al empleado/a del Grupo sobre la importancia de cumplir con el nuevo Reglamento General de Protección de Datos (RGPD), se dará una introducción de la materia.

### ¿Qué es un dato personal?

1. Se considera dato personal cualquier dato sobre personas físicas identificadas o identificables, incluyendo por tanto los datos del personal, clientes o proveedores del Grupo. Estos pueden ser nombre y apellidos, fecha de nacimiento, dirección postal o de correo electrónico, número de teléfono, DNI, imagen, voz…, y muchos otros datos[1] que puedan llegar a identificar y aportar información sobre una persona identificada o identificable, como una dirección IP, número IMEI, dirección MAC, un número de teléfono -fijo o móvil-, una matrícula de coche, etc .se usan a diario constituyen información valiosa que podría permitir identificar a una persona, ya sea directa o indirectamente.

2. Se incluyen dentro de los datos personales, los datos de contacto empresarial: es habitual pensar que el RGPD no se aplica sobre datos de personas físicas que representan a personas jurídicas o de personas físicas que actúan en calidad de empresario individual. Sin embargo, el RGPD no excluye estos datos de su ámbito de aplicación y, por tanto, quedan sometidos a las obligaciones que impone el RGPD.

   Confidencialidad y protección de datos: las obligaciones de confidencialidad no son las mismas que las de protección de datos. Mientras que las primeras se centran fundamentalmente en impedir que un empleado o un tercero difunda cierta información (personal o no), la protección de datos abarca un campo mucho más amplio y se refiere únicamente a datos de personas físicas.

3. Habrá que tener un cuidado adicional en el caso de los llamados datos especialmente protegidos.

### ¿Qué es un dato de carácter especial?

4. Las categorías especiales de datos son aquellos datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

5. En particular nos referimos a datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación

[1] Ver Apéndice I. Tipos de datos personales

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 la orientación sexual de una persona física.

6. Tales datos personales no pueden ser tratados, a menos que se permita su tratamiento en situaciones específicas, incluidas en el art. 9 del RGPD. Sin perjuicio del resto de situaciones incluidas en el artículo 9, los dos supuestos que más virtualidad van a tener en la práctica de una empresa son:

7. Que el interesado haya dado su consentimiento explícito (ver apartado 2.2.4) para el tratamiento de dichos datos personales con uno o más de los fines especificados, salvo que una norma prohíba al interesado la posibilidad de dar su consentimiento en estos casos;

8. que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

**Conceptos importantes**

Los siguientes conceptos aparecen en varias ocasiones a lo largo del documento por lo que es importante que se tenga claro su significado:

9. **Interesado**: la persona titular de los datos personales.

10. **Responsable del tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

11. **Encargado de tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

12. **Tratamiento o actividad de tratamiento**: materialización de una finalidad sobre los datos personales de un determinado colectivo de personas. Así, una actividad de tratamiento puede ser la gestión de personal, la gestión de historias clínicas, la gestión de alumnos, la gestión de becas, la gestión de una biblioteca, la gestión de la agenda institucional de una organización.... Cada tratamiento incluirá una serie de operaciones como, por ejemplo, la recogida, registro, organización, estructuración, consulta o utilización de los datos.

13. **Registro de Actividades de Tratamiento**: documento que enumera las actividades de tratamiento de datos personales que lleva a cabo un responsable de tratamiento y las actividades de tratamiento que un encargado lleva a cabo en nombre de un responsable de tratamiento.

14. **Conceptos de cesión y acceso a los datos personales**: muchas veces la cesión de nuestros datos a otras organizaciones o el acceso a nuestros datos por otras organizaciones pasan desapercibidos, pero lo cierto es que se producen muy habitualmente, como ocurre en las cesiones de datos de empleados a la Seguridad Social o a Hacienda o el acceso a datos para la gestión de nóminas. La cesión implica transferir los datos a un sujeto externo, para que este los utilice con sus propias finalidades. El acceso implica transferir los datos a un sujeto externo, para que este nos preste un servicio, bajo las instrucciones y con las finalidades que se les marquen.

**¿Quién es el responsable de datos personales o DPD del Grupo?**

| | |
|---|---|
| **Denominación** | Delegado de protección de datos |
| **Dirección** | Avenida de Bruselas, 38 – 28108 Alcobendas |
| **Datos de contacto** | Alexandra Juanas |
| **Delegado de Protección de datos** | dpo@masmovil.com |

**¿Qué es el derecho fundamental a la protección de datos?**

15. Es la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él. Es un derecho reconocido en la Constitución Española y el Derecho Europeo y protegido por el RGPD.

16. Todos los usuarios que tengan un acceso a datos de carácter personal almacenados tanto en sistemas informáticos como en formato papel, deben cumplir las siguientes normas encaminadas a asegurar un buen cumplimiento de la normativa vigente. Es por ello que se precisa la colaboración e implicación de todo el personal que trabaja en el Grupo para aplicar correctamente todas las medidas que la ley exige.

**¿Qué derechos poseen los titulares de los datos en materia de protección de datos?**

17. Toda persona física, de la cual se dispongan datos de carácter personal tiene, por ley, potestad para ejercer sus derechos de acceso (conocer qué datos se tienen de él), rectificación (pedir su modificación), cancelación y oposición (pedir su baja total o parcial o restringir su utilización o posibles comunicaciones a terceros), limitación del tratamiento (conservándolos sólo para el ejercicio o defensa de reclamaciones), revocación (dejar sin efecto el consentimiento otorgado) y, en su caso, solicitar la portabilidad de sus datos.

18. Es obligación de todos los empleados del Grupo contribuir al ejercicio de dichos derechos, por lo que los usuarios deberán redirigir cualquier consulta de este tipo al Delegado de Protección de Datos (DPD), quien proporcionará a ese interesado todas las explicaciones necesarias dentro de los plazos de contestación establecidos al efecto.

19. En caso de que el empleado quiera ejercitar los derechos reconocidos en el *CAPITULO III del GDPR -acceso, rectificación, supresión, limitación, portabilidad, oposición y a no ser sujeto de toma de decisiones automatizadas-* deberá ponerse en contacto con el Responsable de Protección de Datos o el DPD para indicarle el proceso a seguir y añadir un escrito firmado con Ref. Protección de datos GDPR, en:

| | |
|---|---|
| Dirección correo | dpo@masmovil.com |

**¿Qué deben hacer los empleados en caso de tratar datos personales responsabilidad del Grupo?**

20. Los datos de carácter personal solo pueden ser comunicados a un tercero (persona física o jurídica, pública o privada u órgano administrativo distinta del Grupo) si se dispone del consentimiento del interesado. Por tanto, si para la realización de cualquier tarea, el usuario quisiera comunicar a un tercero datos de carácter personal, ya sea empresa, profesional o administración pública, deberá contactar previamente con el DPD para determinar su viabilidad y las especiales medidas jurídicas y de seguridad que, en su caso, hay que aplicar.

21. En caso de transmitir datos de carácter especial por correo electrónico, Internet u otro tipo de servicio de telecomunicaciones, el usuario deberá contactar previamente con el DPD para determinar las especiales medidas de seguridad que cabe aplicar.

22. En el caso de subcontratar a terceras empresas la realización de trabajos que impliquen la necesidad de que éstas traten datos de carácter personal de los que es responsable el Grupo, será preciso regular este proceso mediante la formalización de un contrato por lo que también en estos casos, deberá contactarse previamente con el DPD.

**¿Cómo se deben tratar los datos personales?**

23. Los datos de carácter personal deben ser adecuados, pertinentes y no excesivos en relación con la propia finalidad del tratamiento en el que se hallen recogidos. Es por ello que debe hacerse especial énfasis en el riesgo que pueden suponer cualquier tipo de dato de carácter personal que podría llegar a vulnerar la calidad y finalidad de la información, es decir, que vaya más allá de la finalidad, previamente establecida, del tratamiento tales como anotaciones subjetivas o incluso peyorativas.

**Transferencias internacionales de datos personales**

24. Todo tratamiento de información y/o datos, sujeto a la normativa de la Unión Europea que implique una transferencia de los mismos fuera del Espacio

Económico Europeo2, deberá llevarse a cabo dentro del estricto cumplimiento de los requisitos establecidos en la ley aplicable en la jurisdicción de origen.

25. El RGPD exige que las transferencias fuera del Espacio Económico Europeo se realicen solo si se han tomado previamente garantías adecuadas (art. 46 RGPD) para que los datos transferidos se mantengan bajo un entorno de seguridad equivalente al de la Unión Europea o que la transferencia se realice al amparo de alguna de las situaciones que enumera el art. 49 RGPD, entre ellas, que el interesado haya dado su consentimiento explícito cuando haya sido informado de los posibles riesgos de la transferencia al no existir garantías adecuadas en marcha.

**Principios sobre la contratación de encargados del tratamiento**

26. La contratación de terceros prestadores de servicios que en virtud de la actividad o servicio a prestar pudieran tener acceso a información sensible y/o a datos de carácter personal responsabilidad del Grupo, deberá ser verificada durante la vigencia de la relación contractual. La aptitud del prestador de servicios deberá ser confirmada, asegurándose que reúne las garantías necesarias y cumple con las medidas de seguridad exigibles.

27. Para el cumplimiento de las obligaciones que impone el RGPD en este punto, se debe consultar el Procedimiento de Compras y el documento Control de Servicios Externalizados, Anexo al mismo.

**Formación y Concienciación del personal**

28. La formación en materia de protección de datos de los empleados es crucial para el Grupo, por ello deben establecerse acciones formativas para aumentar los conocimientos, las habilidades y las actitudes de los empleados, con el objetivo de mejorar los tratamientos de información que contengan datos de carácter personal.

29. Es fundamental que los conocimientos que se adquieran no se queden obsoletos y para ello han de establecerse los medios necesarios para actualizar (periódicamente) los conocimientos y obtener por parte de cada empleado un trabajo eficaz y diligente en el manejo de datos de carácter personal.

[2] Espacio Económico Europeo

# 6. Directrices de tratamiento de datos de carácter personal

## Principios de tratamiento

El tratamiento de datos personales se rige por una serie de principios que deben tenerse en cuenta en todo momento, tanto al recoger los datos personales como durante el propio tratamiento. Es importante recordar que los principios no son meras declaraciones de intenciones o referencias teóricas para orientar el tratamiento de datos personales. Los principios tienen aplicaciones prácticas de crucial importancia e imponen obligaciones que se deben aplicar de forma transversal a toda actividad de el Grupo que conlleve el tratamiento de datos personales. El incumplimiento de cualesquiera de estos principios lleva aparejadas las sanciones más altas que impone el RGPD, las cuales pueden llegar hasta los veinte millones de euros o, tratándose de una empresa, de una cuantía equivalente hasta el cuatro por ciento como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

A continuación, se explica el contenido de cada principio y cuáles son las implicaciones prácticas que cada uno tiene.

### Principio de licitud, lealtad y transparencia

La principal implicación práctica de este requisito es la obligación de informar a los sujetos interesados de que el Grupo está tratando sus datos personales y la de explicarles qué se hace con ellos.

El RGPD obliga a los responsables del tratamiento a dar información detallada de lo que se hace con los datos personales de interesados. Los artículos 13 y 14 RGPD enumeran los extremos de los que se deberá informar a los interesados:

1. La identidad y los datos de contacto del responsable y, en su caso, de su representante;
2. los datos de contacto del delegado de protección de datos, en su caso;
3. los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
4. cuando el tratamiento se base en el interés legítimo del Grupo (ver apartado 2.2.5), los intereses legítimos del responsable o de un tercero;
5. los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
6. en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo,

del RGPD, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado;

7. el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
8. la existencia del derecho a solicitar al responsable del tratamiento 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;
9. cuando el tratamiento esté basado en el consentimiento, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
10. el derecho a presentar una reclamación ante una autoridad de control;
11. si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
12. la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4 RGPD, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado;
13. cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.

Además, cuando los datos se recojan de una persona distinta al interesado (cuando hayan sido cedidos por otro organismo, cuando hayan sido dados por un tercero o cuando provengan de fuentes accesibles al público), el Grupo deberá ofrecer la siguiente información adicional:

14. Las categorías de datos personales de que se trate; y
15. la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

La información debe ofrecerse de forma **concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo**.

Dar la información de forma concisa y transparente significa que se debe evitar dar información de una forma que propicie la fatiga informativa del interesado que recibe la información. Con este fin, es recomendable dar la información por capas, tal y como recoge la LOPDGDD. En una primera capa de información se puede ofrecer de forma sintética y resumida los aspectos principales del tratamiento, siendo la identidad del responsable del tratamiento y su representante, en su caso, la finalidad y la posibilidad

de ejercer los derechos reconocidos en el RGPD. En la segunda capa se incluirá la restante información con mayor grado de detalle. Para una más fácil comprensión de cómo funciona el método de la información por capas se puede utilizar la Guía para el cumplimiento del deber de informar de la AEPD.

Para que la información sea inteligible el Grupo debe hacer un esfuerzo previo para delimitar a qué audiencia dirige la información de modo que pueda ofrecerla de manera que sea sencilla de entender para un miembro medio de esta audiencia.

La información debe ofrecerse de tal manera que sea fácilmente accesible para los interesados, es decir, o bien que se ofrezca directamente o bien que sea inmediatamente aparente la ubicación donde puede encontrarse. En un formato electrónico y cuando la información se ofrezca por capas se podrá recurrir a un hipervínculo que lleve directamente a la información. Cuando se utilice un dispositivo de captación de datos que carezca de una interfaz de comunicación con el interesado, como una cámara de videovigilancia o un dispositivo del internet de las cosas, se puede utilizar una señal en la que se incluya la información básica y el lugar donde se pueda encontrar información adicional.

Finalmente, se debe utilizar un lenguaje claro y sencillo de modo que la forma de expresar la información sea lo más clara posible, huyendo de frases complejas y de estructuras de lenguaje complicadas. La información debe ser concreta y definitiva, es decir, debe evitarse ofrecer información abstracta y ambigua. En esta línea, es recomendable no utilizar fórmulas de lenguaje que expresen posibilidad cuando puedan evitarse, por ejemplo, “sus datos podrán ser transferidos fuera de la Unión Europea” o “es posible que tratemos sus datos con finalidades diferentes”. El interesado debe ser consciente de las consecuencias que el tratamiento de sus datos puede conllevar. Es recomendable utilizar sangrías para estructurar o jerarquizar la información de modo que se presente de forma más visual e intuitiva, no utilizar frases formuladas en oración pasiva, evitar el uso excesivo de nombres y de un lenguaje legal, técnico o especialista. Cuando se traduzca información al castellano es necesario asegurarse que el significado final es el mismo.

El principio de transparencia, en definitiva, debe entenderse desde la perspectiva de los interesados e implica que se deben realizar todos los esfuerzos que sean necesarios para que el interesado conozca qué se está haciendo con sus datos, adaptándose a las circunstancias que rodean a la recogida de sus datos personales.

**Principio de limitación de la finalidad**

El RGPD establece que los datos personales deben ser recogidos para finalidades específicas y legítimas y que, como regla general, no deberán ser usados con finalidades incompatibles. Este principio se solapa con la información que se debe ofrecer a los interesados, ya que en el momento en que se recogen los datos se debe informar sobre la finalidad para la que se pretende utilizarlos.

La implicación práctica fundamental de este principio es que los datos personales no deben utilizarse para finalidades diferentes a las que se hayan hecho explícitas al interesado en el momento de informarle sobre las cuestiones de protección de datos.

Con este objetivo, el Grupo debe tener identificadas en todo momento las finalidades para las que trata los datos personales. Para canalizar el cumplimiento de este principio el Grupo puede utilizar el Registro de Actividades de Tratamiento, donde tiene listadas las actividades de tratamiento que lleva a cabo y donde se debe incluir la finalidad para la que se usan los datos personales como un campo obligatorio.

El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial.

**Principio de minimización de datos**

Este principio implica que los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, es decir, en el momento de recoger los datos se deben solo pedir aquellos datos personales que sean necesarios para cumplir con la finalidad para la que se recogen.

Este principio exige que el Grupo emprenda una labor de reflexión sobre los datos personales que pide para desarrollar las actividades de tratamiento y sea responsable y coherente a la hora de pedir información. De nuevo se puede canalizar el cumplimiento de este principio a través del Registro de Actividades del Tratamiento pues en él deberán quedar listadas las categorías principales de los datos que se están utilizando.

**Principio de exactitud**

Los datos personales deben ser exactos y, por tanto, deberán ser puestos al día cuando resulte preciso.

La obligación fundamental derivada de este principio consiste en la puesta en marcha de medidas que permitan la actualización periódica de los datos personales, por ejemplo, a través de comunicaciones periódicas con los propios interesados.

Si el Grupo ha tomado medidas suficientes para asegurar la exactitud de los datos personales que utiliza, no será responsable de la inexactitud de datos personales obtenidos directamente del interesado, ni de aquellos suministrados al responsable por un mediador o intermediario cuando las normas aplicables al sector de actividad posibiliten su participación, ni de aquellos que provengan de otro responsable en virtud del ejercicio del derecho a la portabilidad por el interesado.

En definitiva, no solo es necesario informar al interesado de que debe ser responsable en el momento de dar sus datos de forma correcta y de que debe ponerse en contacto con el Grupo cuando los datos cambien, sino que se exige una labor proactiva del Grupo para garantizar que los datos son exactos. En la práctica, articularemos el cumplimiento de este principio de la siguiente manera:

16. Por un lado, en la información que se dé al interesado se debe incluir que este último debe dar los datos de forma exacta y que la inexactitud de los datos que se hayan obtenido directamente de él no será imputable a el Grupo. Asimismo, se debe informar al interesado que tiene el deber de comunicar cualquier modificación de los datos, para lo que se debe ofrecer una dirección de contacto accesible.

17. Por otro lado, el Grupo debe poner en marcha mecanismos para facilitar que los interesados actualicen sus datos de forma periódica. En función de las circunstancias concretas de cada caso se debe pensar la fórmula idónea para ofrecer al interesado esta posibilidad, sin que le pueda resultar molesto. Cuando el Grupo se deba poner en contacto con los interesados para cumplir con este deber, la comunicación debe establecerse por medios que sean eficaces para entrar en contacto con el interesado, por ejemplo, un correo electrónico o una notificación en su cuenta dentro de una aplicación, pero con una periodicidad amplia para evitar que resulte intrusivo para el interesado, por ejemplo, una vez al año si no es presumible que haya tenido lugar algún cambio en los datos.

**Principio de limitación del plazo de conservación**

El Grupo no debe conservar datos personales por un periodo superior al necesario. El plazo durante el que se deben conservar los datos personales depende de la finalidad para la que se hayan recabado; cuando los datos dejen de ser necesarios para cumplir con la finalidad para la que se recogieron, deberán ser eliminados.

Los periodos de conservación van a depender del tipo de datos personales y de la finalidad para la que se lleva a cabo el tratamiento. Las reglas que se deben adoptar para conservar los datos tienen que ser razonables y estar justificadas fehacientemente.

Nuevamente, el Registro de Actividades de Tratamiento sirve como herramienta para cumplir con este principio ya que es obligatorio incluir el plazo durante el que se conservarán los datos personales. Además, deberá informarse al interesado sobre el plazo concreto durante el que se utilizarán los datos personales cuando se le dé información sobre protección de datos. Cuando no sea posible establecer el periodo específico de almacenamiento de datos (p.ej. porque haga referencia a una relación indefinida entre el responsable del tratamiento y el interesado, como un contrato de trabajo), el responsable del tratamiento deberá determinar qué criterios utilizará para determinar el periodo de conservación de los datos.

El cumplimiento de este principio se trata con mayor detalle en el documento “PROCEDIMIENTO DE CONSERVACIÓN, BLOQUEO Y SUPRESIÓN DE DATOS”, del Grupo.

**Principio de integridad y confidencialidad**

El RGPD obliga a que los responsables del tratamiento apliquen las medidas necesarias para garantizar que se cumple con su contenido. Con este objetivo introduce un enfoque novedoso, basado en el riesgo, por el que los responsables del tratamiento deberán tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas, con carácter previo a la elección de las medidas finales.

De acuerdo con este enfoque, es **necesario realizar, con carácter previo al inicio de una actividad de tratamiento, una valoración de los riesgos de la actividad de tratamiento conlleva sobre la privacidad de los sujetos a los que pertenecen los datos**. Para ello habrá que realizar dos procesos de gestión de riesgos diferentes, en función del nivel de riesgo previsible de la actividad:

18. Si el riesgo previsible es alto, se debe realizar una evaluación de impacto de protección de datos.

19. Si el riesgo no es alto, se realizará un análisis básico de riesgos.

Estos dos procesos nos ayudan a escoger qué medidas de seguridad o qué medidas técnicas y organizativas son las más adecuadas para afrontar el riesgo asumido. Las medidas finalmente seleccionadas deberán listarse en el Registro de Actividades de Tratamiento.

Puede consultar información adicional sobre las obligaciones generales del responsable en la Guía del RGPD para responsables del tratamiento, de la AEPD y sobre la realización de análisis de riesgos en la Guía práctica de análisis de riesgos de la AEPD.

**Principio de responsabilidad proactiva**

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la manera en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

**El Grupo debe asegurarse de documentar todo esfuerzo que haga para el cumplimiento de la normativa de protección de datos**. Debe empezar por el Registro de Actividades de Tratamiento, como una foto general de los tratamientos que se hacen en el Grupo y como canal vivo para demostrar el resto de los principios de protección de datos. Llevar el Registro al día y trabajar en él de forma diligente es la mejor fórmula para cumplir con este principio.

**Principio de privacidad desde el diseño**

La privacidad desde el diseño implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada. Esto se consigue mediante una aplicación de medidas de protección de la privacidad en las etapas tempranas del proyecto, que contemple procesos y prácticas de negocio llevando a cabo una gobernanza de la gestión de los datos personales por parte de las organizaciones.

En la práctica, este principio se cumple atendiendo a las siguientes consideraciones:

20. **Proactividad, no reactividad**: se deben tomar medidas proactivas para anticipar las amenazas, identificando las debilidades de los sistemas para neutralizar o minimizar riesgos en lugar de las medidas correctivas para resolver un incidente ya sucedido.

21. **Privacidad como configuración predeterminada**: se persigue que los datos personales estén automáticamente protegidos en cualquier sistema, aplicación, producto o servicio. La configuración por defecto deberá quedar establecida desde el diseño a aquel nivel que resulte lo más respetuoso posible en términos de privacidad. Este principio se aprecia en la minimización de datos a lo largo de todas las etapas del tratamiento: recogida, uso, conservación y difusión. Se logra fijando los criterios de recogida que persigue el tratamiento, limitar el uso de los datos personales a solo las finalidades exactas, restringir accesos a datos personales a las partes implicadas en tratamientos, definir plazos estrictos de conservación y establecer mecanismos para que se cumplan de forma correcta.

22. **Privacidad desde la fase de diseño**: la privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña.

23. **Pensamiento "todos ganan"**: se debe encontrar el balance óptimo entre los diferentes intereses en juego (privacidad, funcionalidad, beneficio empresarial, seguridad, etc.) y no pensar en que los objetivos de privacidad se consiguen a costa del resto de objetivos. Con este objetivo, se deben establecer canales de comunicación colaborativos y de consulta a las partes interesadas con el objeto de comprender y hacer converger múltiples intereses, así como, en caso de que la solución propuesta plantea amenazas a la privacidad, buscar nuevas soluciones y alternativas para alcanzar las distintas funcionalidades e intereses perseguidos, pero siempre sin perder de vista que deben gestionarse adecuadamente los riesgos para la privacidad del usuario.

24. **Aseguramiento de la privacidad en todo el ciclo de la vida**: la privacidad debe nacer en el diseño, antes de que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida completo de los datos. La seguridad de la información impone confidencialidad, integridad, disponibilidad y resiliencia de los sistemas que los cobija. La privacidad garantiza además la desvinculación (unlinkability), la transparencia y la capacidad de intervención y control en el tratamiento por parte del sujeto del dato (intervenability). Para integrar la privacidad a lo largo de todas las etapas del tratamiento de datos, se deben analizar detenidamente las distintas operaciones implicadas (recogida, registro, clasificación, conservación, consulta, difusión, limitación, supresión, etc.) e implementar, en cada una de ellas, las medidas más adecuadas para proteger la información y entre las que cabe considerar:

    a. **Visibilidad y transparencia**: la transparencia en el tratamiento de datos se asienta como pilar para demostrar la diligencia y la responsabilidad proactiva ante la AEPD y como medida de confianza ante los sujetos cuyos datos son tratados. Fomentar la trasparencia y la visibilidad pasa por adoptar una serie de medidas como hacer públicas las políticas de privacidad y protección de datos que rigen el funcionamiento de el Grupo

o desarrollar y publicar cláusulas de información concisas, claras e inteligibles, que sean fácilmente accesibles y que permitan a los interesados comprender el alcance del tratamiento de sus datos, los riesgos a los que pueden verse expuestos, así como el modo de hacer valer sus derechos en materia de protección de datos.

b. **Mantener un enfoque centrado en el titular de los datos**: el Grupo debe diseñar procesos, aplicaciones, productos y servicios "con el usuario en mente", anticipándose a sus necesidades. La protección de estos datos pasa por una mejor implementación de configuraciones de privacidad por defecto "robustas" o proporcionar a los interesados acceso a sus datos y a información detallada de las finalidades del tratamiento y de las comunicaciones realizadas.

Puede consultar más información sobre la privacidad desde el diseño en la Guía de privacidad desde el diseño de la AEPD.

**Cuadro resumen**

| Principio aplicable | Contenido práctico |
|---|---|
| **Licitud, lealtad y transparencia** | 1. El Grupo debe ofrecer a los interesados información sobre cómo se tratan sus datos personales. La información tiene que incluir lo que se recoge en los arts. 13 y 14 del RGPD.<br>2. La información debe darse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje que sea claro y sencillo. |
| **Limitación de la finalidad** | 1. El Grupo debe saber, para cada actividad de tratamiento en marcha, cuál es la finalidad para la que se utilizan los datos. La finalidad se debe identificar antes de empezar a tratar los datos.<br>2. Se debe incluir la finalidad de cada actividad de tratamiento en el Registro de Actividades de Tratamiento.<br>3. Se debe informar al interesado, en el momento en que se recojan sus datos, de cuál es la finalidad para la que se utilizan sus datos. |
| **Minimización de datos** | 1. El Grupo no podrá recabar más datos de los que sean necesarios para cumplir con la finalidad para la que se hayan recogido. Para facilitar que no se recaben más datos de los necesarios, se puede incluir en el Registro de Actividades de Tratamiento los tipos de datos personales que se |

| | |
|---|---|
| | recaban para una determinada actividad de tratamiento, a fin de reflexionar y demostrar que se ha tenido en cuenta este principio. |
| **Exactitud** | 1. Se debe informar al interesado de que debe dar los datos de forma exacta y de que tiene el deber de comunicar cualquier modificación de los datos.<br>2. El Grupo debe poner en marcha mecanismos para facilitar que los interesados actualicen sus datos de forma periódica, por ejemplo, a través de una comunicación periódica. |
| **Limitación del plazo de conservación** | 1. Se debe definir el plazo durante el que se van a tratar los datos personales.<br>2. El Grupo debe informar al interesado de este plazo cuando recoja sus datos o, por lo menos, de los criterios que se utilizarán para determinar el mismo.<br>3. El plazo escogido debe incluirse en el Registro de Actividades de Tratamiento. |
| **Integridad y confidencialidad** | 1. Se deben poner en marcha las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos. Con el fin de seleccionar las medidas adecuadas, el Grupo deberá realizar una valoración de los riesgos que asume al tratar datos personales.<br>2. Las medidas finalmente seleccionadas se listarán en el Registro de Actividades de Tratamiento. |
| **Responsabilidad proactiva** | 1. Se debe guardar documentación de cualquier esfuerzo que demuestre el cumplimiento de la normativa de protección de datos. |
| **Privacidad desde el Diseño** | 1. Se debe tener en cuenta las consideraciones de privacidad a lo largo de todo el ciclo de vida de un proyecto, iniciativa o proceso. |

# 7. BASE JURÍDICA DEL TRATAMIENTO

La base jurídica del tratamiento es la cobertura legal que permite que se traten datos personales. Los datos personales solo se pueden utilizar en una serie de supuestos que enumera el RGPD. Fuera de estos supuestos el tratamiento será considerado ilícito y no podrá llevarse a cabo.

El RGPD, en su art. 6.1 establece que el tratamiento de datos personales solo será lícito si se cumple al menos una de las siguientes condiciones:

1. El interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos;
2. el tratamiento es necesario para la **ejecución de un contrato en el que el interesado es parte** o para la aplicación a petición de este de **medidas precontractuales**;
3. el tratamiento es necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento;
4. el tratamiento es necesario para **proteger intereses vitales del interesado** o de otra persona física;
5. 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;
6. el tratamiento es 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.

A continuación, vamos a tratar las bases jurídicas que con más asiduidad van a aparecer en el ámbito de la actividad del Grupo para conocer en qué consiste cada una y cómo se debe utilizar en la práctica.

### Consentimiento

El interesado puede prestar su consentimiento para que se traten sus datos personales. El consentimiento es la base típicamente necesaria para enviar comunicaciones comerciales a interesados a raíz de un contrato previo entre una empresa y una persona física. También es necesario para la transmisión de los datos de clientes o empleados a otras empresas dentro de un grupo de empresas, siempre que la transmisión no sea necesaria para la llevar a cabo el contrato o relación jurídica de que se trate.

**El consentimiento no es una herramienta que permita obtener cualquier tipo de dato personal para cualquier finalidad**. Su utilización queda condicionada al cumplimiento de los principios de protección de datos, de modo que, por ejemplo, no se podrá pedir cualquier dato sino solo los necesarios para la finalidad para la que se pida

el consentimiento (principio de minimización) y los datos solo serán conservados durante el tiempo necesario para cumplir con la finalidad que se haya comunicado al interesado. Además, para la utilización del consentimiento como base jurídica se deberá cumplir con los siguientes requisitos:

7. Que el consentimiento se haya obtenido válidamente, es decir, que sea libre, específico, informado e inequívoco. El contenido de este requisito se explica más adelante.

8. Que la Compañía sea capaz de demostrar que ha obtenido el consentimiento. Con este fin deberá poner en marcha alguna fórmula para guardar los consentimientos que ha obtenido y en los que sustenta actividades de tratamiento en marcha. En este registro de consentimientos se deben guardar pruebas para demostrar cómo se obtuvo el consentimiento, cuándo se obtuvo y qué información se dio.

9. Que el interesado sea capaz de retirar el consentimiento en cualquier momento, a través de un canal que asegure que el consentimiento se retira con la misma facilidad como fue dado. La retirada del consentimiento no puede llevar aparejado detrimento alguno en el interesado y, en particular, nunca debe llevar aparejado coste alguno. Se debe informar sobre este derecho en el momento de pedir el consentimiento.

10. La retirada del consentimiento obliga a la Compañía a paralizar el tratamiento de datos personales en las actividades de tratamiento ligadas a ese consentimiento. Si todas las actividades de tratamiento están ligadas al consentimiento, los datos personales deberán ser suprimidos3 o anonimizados.

11. En estos casos la Compañía puede optar por migrar la base jurídica a otra que sea aplicable, pero persistirá en todo caso el deber de informar al interesado sobre este cambio.

Para que el consentimiento sea válido debe ser libre, específico informado e inequívoco. Si los datos se tratan sobre la base de un consentimiento inválidamente otorgado, la Compañía estaría incumpliendo el RGPD y se expondría a multas de hasta veinte millones de euros o del cuatro por ciento de la cifra de negocio, optándose por la de mayor cuantía. A continuación, se explica con algo más de detalle el contenido de los requisitos de validez:

**Ejecución de un contrato o de medidas precontractuales**

Cuando para ofrecer un producto o prestar un servicio se necesite tratar datos personales de clientes, potenciales clientes, proveedores, socios de negocio o algún otro tipo de interesado, o cuando se establezca una relación jurídica con el interesado, por ejemplo, el contrato de empleo o la participación en un concurso, la base jurídica que se deberá utilizar es la ejecución de un contrato.

[3] Para la supresión de datos, consulte las *Directrices sobre Conservación de Datos de Carácter Personal*, parte integrante de la Política de Privacidad de [DENOMINACIÓN ABREVIADA].

Esta base jurídica permite tratar datos personales para cualquiera de las prestaciones que sean necesarias para ejecutar el contrato o relación jurídica de que se trate. También permite tratar los datos para emprender aquellas acciones necesarias para que el contrato se ponga en marcha (por ejemplo, toda la información que se solicite antes de cerrarse el contrato). El Grupo debe realizar una reflexión sobre qué es necesario y qué no para ejecutar o poner en marcha el contrato. Lo que sea necesario debe interpretarse en sentido estricto, de modo que solo será necesario aquello que es absolutamente imprescindible para poner en marcha la relación de que se trate. Así, por ejemplo, para la prestación de un servicio nunca va a ser necesario enviar comunicaciones comerciales al interesado ni para la gestión de un contrato de empleo va a ser necesaria la utilización de la imagen de un trabajador.

**Cumplimiento de una obligación legal**

Los datos personales de interesados pueden tratarse cuando sea necesario para el cumplimiento de una obligación legal de el Grupo.

Los casos más habituales aparecen en relación con obligaciones impuestas con finalidades fiscales o de seguridad social. Así, toda empresa debe ceder datos personales de sus trabajadores a la Agencia Tributaria para gestionar el IRPF a la vez que se ceden datos a la Seguridad Social para el alta y baja de trabajadores, gestionar la cotización del trabajador al sistema, la provisión de prestaciones sociales…

Numerosas normativas imponen obligaciones de este tipo. A modo de ejemplo, la legislación contra el blanqueo de capitales impone obligaciones de cesión de información al SEPBLAC, la investigación de delitos obliga la cesión a las fuerzas y cuerpos de seguridad del estado, la cesión a registros públicos, como el Registro Mercantil o de la Propiedad, la cesión a mutualidades para la gestión de bajas laborales, etc.

Aunque el tratamiento sea necesario para cumplir con una obligación legal, los principios de protección de datos se aplican íntegramente, sobre todo los deberes de información. El interesado debe ser informado, en consecuencia, de que sus datos se están tratando sobre la base de una obligación legal y de la finalidad y contenido de la obligación.

**Interés legítimo**

En determinadas situaciones, puede resultar útil y razonable para la Compañía utilizar datos personales de interesados con diferentes finalidades dirigidas en última instancia a que la actividad de la Compañía se desarrolle de la forma más eficiente posible. Esta utilidad se denomina interés legítimo y podrá utilizarse como base jurídica para el tratamiento de datos personales siempre que no prevalezcan los intereses o los derechos y libertades del interesado. Por tanto, esta base pone en equilibrio el interés de la empresa en conducir su actividad de la forma más eficiente posible con el derecho del interesado a la privacidad y a que sus datos personales sean solo utilizados de conformidad con la normativa de protección de datos.

Para determinar si debe prevalecer el interés de la Compañía o los derechos del interesado, se debe reflexionar, con carácter previo al uso de los datos personales, sobre las circunstancias del tratamiento que se quiere llevar a cabo, teniendo en cuenta

las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable.

En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, de la que se debe dejar constancia documental, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior.

La normativa de protección de datos establece un conjunto de tratamientos en los que puede prevalecer el interés legítimo de la Compañía. Estos son:

12. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude.
13. El tratamiento de datos personales con fines de mercadotecnia directa.
14. Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados.
15. El tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.
16. El tratamiento de datos de contacto de personas físicas que presten servicios a una persona jurídica (normalmente representantes de la persona jurídica) cuando se refiera únicamente a los datos necesarios para su localización profesional y cuando la finalidad del tratamiento sea únicamente mantener

relaciones de cualquier índole con la persona jurídica en la que el interesado preste sus servicios.

17. El tratamiento de datos de contacto de empresarios individuales cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con ellos como personas físicas.

Para aquellas actividades de tratamiento en las que se recurra al interés legítimo, se podrá utilizar el Registro de Actividades de Tratamiento como soporte para dejar constancia de que se han puesto en equilibrio los intereses de la Compañía con los derechos y libertades del interesado.

# 8. RGPD en la Seguridad de la Información

### Usuarios y contraseñas

18. Cada usuario es responsable de la confidencialidad de su contraseña o de proteger cualquier otro mecanismo de autenticación equivalente y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicarlo con la mayor brevedad posible al Responsable de Protección de Datos o al DPD para proceder inmediatamente a su cambio, así como para registrar la incidencia en el registro de incidencias JIRA Software.

19. En especial, queda prohibido escribir la contraseña en cualquier tipo de soporte físico (papel, etc.) o lógico (archivos).

### Puesto de trabajo

20. El usuario es responsable del puesto de trabajo desde donde realiza el acceso, y garantizará que ninguna otra persona no autorizada pueda ver la información sobre datos de carácter personal que muestren sus equipos informáticos.

21. Cuando el usuario deja su lugar de trabajo, debe cerrar la sesión de trabajo y apagar los equipos tecnológicos asociados al mismo (ordenador, pantalla, periféricos, etc.). El objetivo de esto es imposibilitar la visualización de los datos protegidos así como salvaguardar la confidencialidad de los mismos.

22. Finalmente, el usuario no podrá cambiar la configuración de las aplicaciones y sistemas operativos de su puesto de trabajo sin la autorización de los responsables o administradores de seguridad informática y no podrá utilizar ninguna herramienta o utilidad no autorizada para acceder a aquellos archivos que contengan datos de carácter personal.

### Datos y almacenamiento de ficheros

23. En relación con los archivos temporales, que son considerados por el Grupo como documentos de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento, se recuerda a los usuarios la obligación de almacenar en el Directorio Carpeta de Red correspondiente toda la información tratada durante el desarrollo de las funciones laborales, no estando permitido el almacenamiento de información en el disco duro de los ordenadores, tanto en los PC como en los ordenadores portátiles, salvo autorización previa y expresa del Responsable de Protección de datos o al DPD.

24. El usuario está obligado a borrar periódicamente los archivos localizados en los directorios de red una vez desaparecida la finalidad perseguida en la creación del documento que contenga datos personales de carácter básico y/o especial y siempre que no resulte necesaria su conservación.

25. En caso de que el usuario detecte que se han borrado por error, avería del sistema informático u otra razón datos, archivos, bases de datos, etc. que contuvieran datos de carácter personal tanto básicos como especiales, deberá comunicarlo de inmediato al Responsable de Protección de Datos o al DPD para que se proceda, en la medida de lo posible, a recuperar la copia de seguridad más reciente y para, inmediatamente después, proceder a actualizar manualmente los datos que no estuvieran en dicha copia y se hubieran perdido.

26. En lo relacionado con los documentos en soporte papel, mientras éstos no estén archivados por estar en proceso de tramitación o revisión, el usuario deberá custodiarlos e impedir en todo momento que puedan ser accedidos por personas no autorizadas (al finalizar la jornada laboral no deberán quedar a la vista documentos que contengan datos de carácter personal). En el momento en que hayan de ser eliminados deberá procederse a su destrucción de forma que se evite su recuperación posterior (mediante máquina destructora de papel o mecanismo equivalente). El responsable de Protección de Datos o el DPD velará por la correcta administración de estos documentos, en especial, los que contengan datos de carácter tanto básico como especial.

27. Respecto al uso de ordenadores portátiles, dispositivos móviles y otros equipos, si el usuario precisa copiar en ellos archivos informáticos que contengan datos de carácter personal, tanto básicos como especiales, solicitará la correspondiente autorización al Responsable de Protección de Datos o al DPD y velará, en la medida de lo posible, por su seguridad, controlando su ubicación y evitando su sustracción, además de utilizando siempre contraseñas de acceso al equipo u otros mecanismos equivalentes que eviten el acceso a los datos en caso de robo o pérdida accidental.
28. Por otra parte, el usuario velará por eliminar dichos archivos cuando no sean precisos y por volcarlos a los sistemas informáticos principales en caso de que realice modificaciones en ellos al menos una vez a la semana para garantizar que son incluidos en las copias de seguridad correspondientes.

**Gestión de incidencias**

29. La certeza o sospecha de que se ha producido una incidencia que entrañe riesgo para la seguridad de los datos personales debe ser comunicada al Responsable del Departamento con la mayor celeridad posible. Entre otras, se consideran incidencias los olvidos o conocimiento por parte de usuarios no autorizados de las contraseñas, la creación de archivos con datos de carácter personal no autorizados, la pérdida de información de una base de datos personales o los soportes que los contienen, la aparición de listados no controlados y, en general, cualquier incidencia que no permita acceder a los datos o permita acceder a los datos con un tipo de acceso teóricamente no permitido (o a datos a los que no se debería tener acceso).

## Tratamiento de datos personales

30. El usuario recibirá instrucciones sobre los tratamientos de datos personales que está autorizado a emplear, así como el tipo de acceso permitido (lectura, escritura, etc.) y la finalidad de los mismos.

31. El usuario sólo podrá utilizar esos tratamientos, plasmados en el registro de actividades de tratamiento del Grupo, y únicamente de acuerdo con la finalidad estipulada, procurando además que los datos personales contenidos en ellos estén siempre actualizados y cancelándolos cuando ya no sean necesarios o pertinentes para la finalidad para la cual hubieran sido recabados, puesto que la normativa en materia de protección de datos prohíbe expresamente el mantenimiento indefinido de los datos de carácter personal.

32. En el supuesto de que el usuario desee crear archivos propios o nuevos tratamientos con datos de carácter personal, incluso de carácter temporal, deberá hacerlo previa autorización del Responsable de Protección de Datos o al DPD, quien le informará de cualquier posible medida legal, técnica u organizativa que haya que adoptar.

# 9. Cumplimiento

33. El incumplimiento de cualquiera de las obligaciones contenidas en el presente documento comportará las consecuencias jurídicas y laborales derivadas del propio incumplimiento cometido. Quien creara ficheros que contuvieran datos de carácter personal o desarrollara o instalara aplicaciones que permitieran tratarlos sin la correspondiente autorización será considerado responsable del fichero o de su tratamiento, con las consecuencias legales que de ello se derivan.

34. Asimismo, con la firma del presente documento el trabajador confirma que ha leído y entendido el documento de Política de Datos Personales del Grupo Masmovil, y que se compromete a cumplir con lo establecido en este.

# 10. Responsables y Contacto

En caso de duda sobre esta Política, se indican los siguientes contactos clave:

| Nombre | Rol | Contacto |
|---|---|---|
| Daniel Martínez Ponce | CISO | daniel.martinez@masmovil.com<br>Telf.: 633 000 378 |
| Jorge Rivera Nebot | Manager | jorge.rivera@masmovil.com<br>Telf.: 633 000 059 |
| Miguel Ángel Cantero Pinilla | Analista | miguelangel.cantero@masmovil.com<br>Telf.: 633 000 108 |

En caso de dudas legales, los contactos clave son:

| Nombre | Cargo y Departamento | Contacto |
|---|---|---|
| TBD | DPO | TBD |

# 11. Glosario y Definiciones

1. Confidencialidad
   Carácter reservado de la información por el cual su acceso o conocimiento está limitado a las personas, entidades o procesos que han sido debidamente autorizados. Propiedad de un activo de información que establece que no debe ser transmitido o accedido por personas, entidades o procesos no autorizados.

2. Información
   Cualquier tipo de representación o comunicación de conocimientos tales como datos, hechos u opiniones, soportados en cualquier tipo de medio manual o automatizado (por ejemplo; impreso, electrónico o audiovisual). Por elemento de información se entiende cualquier ítem o parte de la misma.

3. Integridad
   Propiedad de un activo de información que garantiza su exactitud y completitud frente a su alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

4. Confidencialidad
   Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.

5. Dispositivo móvil
   Dispositivo de uso personal o profesional que permite la gestión de información y el acceso a redes de comunicaciones, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo Smartphone (teléfonos móviles inteligentes con mayores prestaciones), Tablet y agendas electrónicas (PDA), independientemente de sí disponen de teclado o pantalla táctil.

# 12. Referencias

1. UNE-ISO/IEC 27001/2013. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).
2. COBIT 5 para la Seguridad de la Información. Information Systems Audit and Control Association, ISACA.
3. Reglamento General de Protección de Datos. Agencia Española de Protección de Datos (AEPD).

# Apéndice I. Tipos de datos personales

| Verificaciones de antecedentes | Información familiar | Viajes y gastos |
|---|---|---|
| Historial criminal | Nombre de los hijos, padres o compañeros sentimentales | Detalle de gastos |
| Antecedentes penales | **Información laboral** | Detalle de reserva de viajes |
| Citaciones de tráfico | Departamento | Historial de viajes |
| Resultados del "Test de Drogas" | Compañía | **Información de cuentas de usuario** |
| Referencias | Tipo de contrato | Fecha de creación de la cuenta |
| Identificación personal | Tarjeta de crédito o débito corporativas | Número de cuenta |
| Edad | Acciones disciplinarias | Contraseña de la cuenta |
| Nombre completo | Fecha de extinción laboral y motivos | Contraseña de activación |
| Fecha de nacimiento | Información de salud y seguridad | Dirección MAC |
| Género | Detalles del puesto de trabajo | **Información de navegación web** |
| Estado civil | Localización en la oficina | Tiempo de navegación |
| Imágen | Salario | Información de cookies |
| Opinión política | Fecha de inicio de la relación laboral | Dirección IP |
| Religión | **Experiencia profesional y afiliaciones** | Logs del sistema |
| Origen racial o étnico | Experiencia profesional | Historial de webs |
| Orientación sexual | Membresía profesional | **Biométrica** |
| Firma | Cualificaciones/certificaciones | Reconocimiento facial |
| Grabación de voz | Afiliación sindical | Huella dactilar |

| **Información de contacto** | Formación y habilidades | Detector de retina |
|---|---|---|
| Dirección domicilio personal | Títulos académicos | Detector de voz |
| Email personal | Historial educativo | **Redes sociales** |
| Número de tarjeta de crédito | **Financiero** | Cuentas de redes sociales |
| Número de identificación personal y pasaporte | Información cuenta bancaria | Contactos |
| Carnet de conducir | Bonus | Historial de redes sociales |

# Apéndice I. Controles SEG-PY-XX

| Referencia[i] | Ámbito[ii] | Descripción[iii] | Responsables[iv] | Cumplimiento[v] | |
|---|---|---|---|---|---|
| | | | | Obligatorio | Recomendado |
| SEG-PR-XX-C.01 | Seguridad en datos personales | | | X | |
| SEG-PR-XX-C.02 | | | | X | |
| SEG-PR-XX-C.03 | | | | X | |

[i] Identificador del control en el procedimiento tratado.
[ii] Ámbito del control dentro del procedimiento tratado.
[iii] Descripción detallada del control.
[iv] Indica el área/departamento responsable de llevar a cabo el control.
[v] Grado de cumplimiento del control dentro del procedimiento tratado.