COMPROMISO EMPRESARIAL
FISCAL · CONTABLE · LABORAL · JURÍDICO

COMPROMISO EMPRESARIAL CONSULTORES SL

POLÍTICA DE SEGURIDAD APLICADA AL TRATAMIENTO DE DATOS PERSONALES

V.00

ÍNDICE

1. OBJETO DEL DOCUMENTO

Desde COMPROMISO EMPRESARIAL CONSULTORES SL valoramos la privacidad y somos conscientes de la importancia de proteger los datos personales de todos aquellos interesados con los que nos relacionamos. Por ello, tratamos los datos personales con el máximo respeto a las disposiciones establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Con tales fines, la presente política se ha elaborado con el objetivo de regular los aspectos básicos que deben regir a la hora de gestionar cada uno de los tratamientos de datos personales de nuestra entidad. Estos aspectos deben ser respectados por cada uno de nuestros empleados, contratistas y subcontratistas, y deben servir para evidenciar nuestra proactividad y responsabilidad en el cumplimiento de nuestras obligaciones como Responsables o, en su caso, Encargados del Tratamiento.

Mediante las correspondientes políticas y protocolos especializados, se desarrollarán de forma más amplia las pautas y procedimientos a seguir para asegurar el debido cumplimiento de la normativa de protección de datos.

Las medidas y procedimientos de seguridad que mediante el presente documento se recogen, han sido desarrollados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como en atención a las guías y recomendaciones efectuadas por las correspondientes Autoridades en la materia. Todo ello, con la finalidad de asegurar la información de acuerdo a los riesgos asociados a los niveles de criticidad y sensibilidad de la información tratada por la organización.

2. ÁMBITO DE APLICACIÓN

El presente documento resulta de aplicación tanto a las actividades de tratamiento, como a los ficheros que contienen datos de carácter personal y que se hallan bajo la responsabilidad del Responsable del Tratamiento, tanto cuando actúa como tal o como Encargado; incluyendo los sistemas de información, comunicación, soportes, equipos y resto de recursos empleados para el tratamiento de datos de carácter personal. Por tanto, esta Política debe ser aplicada en todas las unidades de negocio, procesos y sistemas en todos los países en los que la Organización lleva a cabo sus negocios y realiza transacciones u otras relaciones comerciales con terceros.

3. RESPONSABILIDAD

Con el objeto de cumplimiento de las finalidades anteriormente señalas, la Dirección de la Organización en coordinación con el Responsable de seguridad o, en su caso, el personal

designado a los efectos expuestos, serán los responsables de promover y mantener las condiciones y medios necesarios para garantizar el cumplimiento del presente manual de seguridad.

Por su parte, cada uno de los usuarios con acceso a información confidencial o que contenga datos de carácter personal, ya sea en formato físico o digital, debe velar por el íntegro cumplimiento del presente manual de seguridad, siendo responsabilidad del propio personal garantizar el cumplimiento de las directrices mediante la presente dispuestas.

4. RECURSOS PROTEGIDOS

Con las finalidades anteriormente expresadas, se exponen, a continuación, los recursos protegidos:

- Centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan.
- Puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso a datos personales.
- Servidores y el entorno del sistema operativo y de comunicaciones en el que se encuentran ubicados los ficheros que contienen datos personales.
- Sistemas informáticos y/o aplicaciones establecidos para realizar el tratamiento de
- los datos personales.
- Cualquier otro recurso que, sin estar aquí individualizado, se utilice para tratar datos personales.

5. POLÍTICA BÁSICA DE PROTECCIÓN DE DATOS PERSONALES

5.1. Glosario de términos

DATOS PERSONALES: Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

ENCARGADO DEL TRATAMIENTO: La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

INTERESADO: Cualquier persona física que facilite sus datos personales, ya sea cliente, proveedor, empleado o cualquiera tercero.

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

SEUDONOMIZACIÓN: La seudonimización es un procedimiento de gestión de datos donde se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos.

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES: Suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)

TRATAMIENTO DE DATOS PERSONALES: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

VIOLACIÓN DE SEGURIDAD: significa una violación de seguridad que conduce a la destrucción, pérdida, alteración, comunicación no autorizada o acceso no autorizado o accidental de datos personales transmitidos, almacenados o tratados de otra manera.

5.2. Marco normativo básico

- Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

5.3. Principios relativos al tratamiento

Los principios relativos al tratamiento de datos personales se encuentran regulados en nuestro ordenamiento jurídico por el art. 5 del RGPD y por los arts. 4 y ss. de la LOPDGDD. Estos principios constituyen el pilar fundamental en el que se debe basar todo tratamiento de datos personales en nuestra entidad y, por lo tanto, deberán ser conocidos por todos y cada uno de los empleados que, en el ejercicio de sus funciones, deban tratar datos personales de empleados, clientes, proveedores o cualquier otra persona física o interesado.

El artículo 5.1 del RGPD lista los siguientes principios:

"1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado ***(«licitud, lealtad y transparencia»);***

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ***(«limitación de la finalidad»);***

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ***(«minimización de datos»);***

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan ***(«exactitud»);***

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; 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, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ***(«limitación del plazo de conservación»);***

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, 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 ***(«integridad y confidencialidad»).*** *"*

5.3.1. Principio de licitud, lealtad y transparencia

El principio de licitud, lealtad y transparencia viene regulado en el art. 5.1.a) del RGPD mediante el cual se establece que los datos deberán ser tratados de manera lícita, leal y transparente. En este sentido, el art. 6 del RGPD dispone que, para que un tratamiento se pueda considerar **lícito**, este deberá basarse en alguna de las bases legitimadoras del art. 6.1 del RGPD:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su ***consentimiento*** *para el tratamiento de sus datos personales para uno o varios fines específicos;*

b) 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;*

c) el tratamiento es necesario para el cumplimiento de una ***obligación legal*** *aplicable al responsable del tratamiento;*

d) el tratamiento es necesario para proteger ***intereses vitales del interesado o de otra persona física****;*

e) 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;***

f) el tratamiento es necesario para la satisfacción de ***intereses legítimos perseguidos por el responsable del tratamiento 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."*

Por lo que respecta a la lealtad y transparencia del tratamiento, se deberá cumplir con lo dispuesto en los arts. 13 y 14 del RGPD y 11 de la LOPDGDD en referencia a la información que se deberá facilitar a los interesados sobre el tratamiento de sus datos personales. En este sentido, y siempre que sea de aplicación la LOPDGDD, el Responsable del Tratamiento podrá facilitar la información en dos capas:

En la **"primera capa",** el art. 11 de la LOPDGDD establece que será necesario informar de los siguientes puntos:

- Datos del Responsable del Tratamiento y de su representante, en su caso.
- La finalidad del tratamiento.
- La posibilidad de ejercer los derechos reconocidos en los arts.15 y ss. del RGPD.
- Información en el caso de que se lleve a cabo un perfilado con sus datos.

En caso de que los datos no procedan directamente del interesado, se deberá informar además de lo siguiente:

- Las categorías de datos personales objeto del tratamiento.
- Las fuentes de las que proceden los datos.

Una vez se haya transmitido la información en la primera capa, se deberá facilitar al interesado un medio para acceder al resto de información exigida por los arts. 13 y 14 del RGPD en la **"segunda capa".** Asimismo, en caso de que no sea de aplicación la legislación española (LOPDGDD), se deberá informar tal y como disponen los mencionados artículos del reglamento, sin perjuicio de la aplicación de la regulación especial en materia de protección de datos que sea de aplicación por criterio de aplicación territorial.

En esta segunda capa, siempre y cuando los datos personales sean facilitados por el propio interesado, se deberá informar de los siguientes aspectos (Art. 13 del RGPD):

- La identidad y los datos de contacto del responsable y, en su caso, de su representante.
- Los datos de contacto del delegado de protección de datos, en su caso.
- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Cuando el tratamiento se base en el artículo 6.1.f) del RGPD, los intereses legítimos del responsable o de un tercero.
- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- La existencia de Transferencias Internacionales de Datos.
- El plazo de conservación de los datos.
- La posibilidad de ejercer los derechos reconocidos en los arts.15 y ss. del RGPD.
- La posibilidad de retirar el consentimiento para el tratamiento de los datos.
- El derecho a presentar una reclamación ante la AEPD.
- La existencia de cesiones de datos previstas a terceros.

- La existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Por otro lado, cuando estos datos provengan o los facilite un tercero distinto al propio interesado, el Responsable del Tratamiento, además de todo lo mencionado anteriormente, deberá informar adicionalmente de lo siguiente (Art. 14 del RGPD):

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

En este supuesto del art. 14 del RGPD, se deberá facilitar toda la información mencionada, una vez obtenidos los datos y en un plazo máximo de un mes. Sin embargo, cuando estos datos facilitados por un tercero, se usen para contactar con el interesado, se le deberá informar en ese mismo momento. En el caso de que se comuniquen los datos a otro tercero, se le deberá facilitar toda la información anterior en ese mismo momento.

Por último, es especialmente relevante facilitar toda la información mencionada de forma concisa, fácilmente accesible y fácil de entender, y utilizando un lenguaje claro y sencillo. Esta información podrá facilitarse por medios electrónicos, siendo esta una opción especialmente relevante en los casos en los que, debido a la complejidad tecnológica de ciertos tratamientos, sea difícil para el interesado saber y comprender si se están recogiendo sus datos, por quién y con qué finalidad.

5.3.2. Principio de Limitación de la finalidad

El art. 5.1.b) del RGPD regula el principio de limitación de la finalidad, el cual impide que se lleven a cabo tratamientos de datos con finalidades distintas para con las finalidades por las que fueron recabados.

Así pues, y tal y como hemos visto en apartado anterior sobre la información a facilitar al interesado, cuando se vaya a realizar un tratamiento de datos personales, se deberá determinar la finalidad del tratamiento de forma explícita, quedando totalmente prohibido tratar o usar los datos con finalidades ulteriores incompatibles con la finalidad para la que se recabaron. Asimismo, se deberá informar al interesado, y en su caso, recabar el consentimiento, siempre y cuando se decida tratar los datos con finalidades distintas a las originales.

5.3.3. Principio de Minimización de Datos

El principio de minimización viene recogido por el art. 5.1.c) del RGPD y consiste en recabar únicamente los datos personales que sean estrictamente necesarios para cumplir con la finalidad para la que fueron recabados.

Se deberá determinar qué datos son indispensables para cumplir con la finalidad del tratamiento que se persiga, excluyendo todos aquellos que puedan considerarse excesivos o innecesarios.

5.3.4. Principio de exactitud

El principio de exactitud, que se encuentra regulado en el art. 5.1.e) del RGPD, obliga a los Responsables y Encargados del Tratamiento a que tomen cuantas medidas sean necesarias para garantizar la exactitud de los datos objeto de tratamiento. En este sentido, se deberán suprimir, rectificar sin dilación indebida todos los datos que sean inexactos para con los fines que persiguen.

Este principio de exactitud viene íntimamente relacionado con los derechos de rectificación y supresión reconocidos tanto por el RGPD como por la LOPDGDD. El derecho de rectificación del art. 16 del RGPD consiste en el derecho que tiene todo interesado a solicitar que se rectifiquen o amplíen sus datos personales cuando estos estén sean erróneos o incompletos para con las finalidades para las que se recabaron.

Por último, en lo que respecta al derecho de supresión del art. 17 del RGPD, este se describe como el derecho de todo interesado a solicitar la supresión de sus datos personales al responsable, quedando este obligado a suprimirlos, sin dilación indebida, cuando concurra alguna de las siguientes circunstancias:

- El interesado retira el consentimiento que otorgó para el tratamiento de sus datos personales.
- El interesado ejerce su derecho de oposición y no prevalecen otros motivos legítimos para continuar con el tratamiento de sus datos.
- Los datos personales han sido tratados ilícitamente.
- Los datos personales deben suprimirse en cumplimiento de una obligación legal.
- Los datos personales se han obtenido en relación con servicios de la sociedad de la información (e-Commerce, redes sociales, etc.).

5.3.5. Principio de limitación del plazo de conservación

El principio de limitación del plazo de conservación está regulado en el art. 5.1.f) RGPD, el cual, como regla general, dispone que los datos objeto del tratamiento no se podrán conservar durante más tiempo del necesario para cumplir con las finalidades para las que se recabaron los mismos.

Esta regla general se complementa con el resto de plazos de conservación legales que procedan de otras leyes o cuerpos normativos, tal como comentaremos de nuevo más adelante.

Por otro lado, el mismo artículo 5.1.f) del RGPD ya prevé una serie de excepciones al plazo general. En el caso de los datos recabados con finalidades de archivo público, fines de investigación científica o histórica o fines estadísticos, se podrán conservar dichos datos durante plazos más extensos mientras continúe en vigor la finalidad que justifica su conservación.

5.3.6. Principio de integridad y confidencialidad

Este principio hace referencia a la seguridad de los datos personales en todas y cada una de las fases de su tratamiento. El art. 5.1.g) del RGPD establece que los datos deberán ser tratados de forma que se garantice su seguridad, incluyendo la protección contra el acceso no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
El RGPD regula la seguridad del tratamiento y las medidas de seguridad a aplicar desde la perspectiva de la proactividad y la privacidad desde el diseño y por defecto. Esto significa que el RGPD no ofrece un repertorio de medidas de seguridad a aplicar tal y como hacia la normativa anterior, sino que será el Responsable del Tratamiento quién deberá elaborar e implementar las medidas de seguridad necesarias para salvaguardar la confidencialidad, integridad y disponibilidad de los datos antes de realizar el tratamiento en cuestión.

Por su parte, el art. 32.1 del RGPD sobre la seguridad del tratamiento dispone lo siguiente:

> *"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y 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, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
> *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento"*

En el apartado a) del artículo se establecen las dos únicas medidas de seguridad que el RGPD ofrece para garantizar la seguridad de los datos, es decir, el cifrado y la seudonimización de los mismos. En cuanto al resto de apartados: en los b) y c) se dispone la mencionada obligación de garantizar la confidencialidad, integridad y disponibilidad de los datos; y, en el apartado d), se requiere que las medidas de seguridad implementadas sean revisadas y auditadas para comprobar su eficacia.

6. USO Y TRATAMIENTO DE DATOS PERSONALES

Vista la dimensión teórica de los principios que rigen todo tratamiento de datos sometido al ámbito de aplicación del RGPD, se procede al desarrollo en los próximos apartados de las normas de uso y tratamiento básicas por parte COMPROMISO EMPRESARIAL CONSULTORES SL, así como de sus Encargados de tratamiento que, en su caso, participen en el proceso.

A los efectos oportunos, COMPROMISO EMPRESARIAL CONSULTORES SL ha designado un Responsable de Protección de Datos en la entidad a disposición de los empleados y proveedores con la finalidad de resolver cualquier duda acerca de la política de la entidad en materia de datos personales, así como sobre el tratamiento de los mismos. Sus datos de contacto son los siguientes:

NOMBRE:
DEPARTAMENTO:
CORREO ELECTRÓNICO:
TELÉFONO:

Asimismo, se ha designado a un Delegado de Protección de Datos que sirva como punto de apoyo para todos los miembros de COMPROMISO EMPRESARIAL CONSULTORES SL, resolviendo cualquier duda y supervisando el cumplimiento de la normativa en protección de datos.

Datos de contacto del Delegado de Protección de Datos designado:

SEGURIDAD Y PRIVACIDAD DE DATOS, S.L.
Edificio Aqua Multiespacio, C/ Menorca 19, piso 17 (46023) Valencia
infodpo@forlopd.es
963 122 868

6.1. Categorías y tipología de datos que tratamos

En COMPROMISO EMPRESARIAL CONSULTORES SL tratamos diferentes tipologías y categorías de datos personales según la actividad, departamento o área en la que actuemos. A estos efectos, se deberá entender como dato personal toda información sobre una persona física identificada o identificable, y como identificable cualquier persona física cuya identidad se pueda conocer mediante una clave o dato personal, o su combinación, como, por ejemplo: Nombre, Apellidos, Teléfono, IP, Fotografía, etc.

El tratamiento de cada categoría y topología de datos conllevará unas obligaciones diferentes, que exponemos a lo largo de esta política, y que deberán cumplir los usuarios que actúen o lleven a cabo cualquiera de las actividades de tratamiento de datos personales por razón de las funciones encomendadas y durante todo el ciclo de vida de los datos personales.

Pueden consultarse las categorías y tipologías de datos personales, así como el significado de los distintos tratamientos que pueden llevarse a cabo sobre los referidos datos consultando el Anexo I de esta Política.

6.2. Tratamiento lícito, leal y transparente de los datos

Los datos personales que tratados en el ejercicio de las funciones encomendadas, deberán regirse en todo momento por cada uno de los principios desarrollados a lo largo del apartado *«.3. Principios relativos al tratamiento»* De este modo, se deberá cumplir en todo momento con las siguientes obligaciones:

- Recabar o solicitar el **consentimiento** para el tratamiento de datos personales cuando sea necesario hacerlo. El consentimiento siempre se debe recabar por escrito o por cualquier otro medio que deje prueba fehaciente de ello. De no ser necesario el consentimiento, se deberá conocer qué otra base legal es la que legitima el tratamiento de datos del interesado. A modo de recordatorio, las bases legales que podremos aplicar a parte del consentimiento, son:

  - necesario para **ejecutar un contrato** o para aplicar medidas precontractuales.
  - necesario para cumplir con una **obligación legal**.
  - necesario para la satisfacción de **intereses legítimos.**
  - necesario para el cumplimiento de una misión realizada en **interés público** o en el **ejercicio de poderes públicos.**
  - necesario para proteger **intereses vitales.**

- Verificar que la persona o interesado propietaria de los datos personales reciba toda la información que le corresponde y que se encuentra detallada en el apartado 5 de esta Política.

- En el caso del tratamiento de categorías especiales de datos, se deberá tomar especial cautela en su tratamiento.

- Cuando se recaben datos personales con el objetivo de realizar publicidad de los productos o servicios que ofrece COMPROMISO EMPRESARIAL CONSULTORES SL, se deberá recabar el consentimiento expreso del interesado siguiendo con lo dispuesto en el art. 20 de la LSSICE.

6.3. La finalidad del tratamiento

Todo tratamiento deberá tener una finalidad clara y concreta que vendrá determinada por COMPROMISO EMPRESARIAL CONSULTORES SL. Queda prohibido usar los datos personales con finalidades distintas a las originales para las que fueron recabados, y tratar los datos de forma incompatible con las finalidades que se pretenden cumplir.

Por ejemplo, no podríamos usar el correo electrónico que recabamos para enviar la factura por un servicio con el objetivo de enviar comunicaciones comerciales.

En el caso que sea necesario o quiera dar otras finalidades distintas a los datos recabados por cualquier motivo, **se deberá informar a los interesados sobre estas nuevas finalidades y, además, recabar el consentimiento expreso en caso de que sea necesario.**

6.4. Minimización en el tratamiento de datos

En concordancia con el principio de minimización, debemos tener en cuenta que únicamente podremos tratar los datos personales de los interesados que sean estrictamente necesarios para cumplir la finalidad del tratamiento que se esté llevando a cabo.

Por ejemplo, cuando se pretenda tratar datos personales con intención de gestionar el pago de unos servicios, sería excesivo recabar datos relativos a la salud del cliente, ya que se considerarían datos innecesarios para llevar a cabo el tratamiento.

6.5. Exactitud de los datos tratados

En el ejercicio de nuestras funciones deberemos ser proactivos en cuanto a la verificación de la exactitud de los datos personales que tratemos. Cuando, en el ejercicio de nuestras funciones, detectemos o tengamos indicios de que alguno de los datos personales tratados sea erróneo o inexacto, deberemos dar aviso a nuestro responsable, y en su caso, solicitar la rectificación del dato personal al interesado.

Asimismo, si por cualquier motivo se recibiese un ejercicio de derechos, ya sea de rectificación, supresión o cualquier otro de los reconocidos en RGPD, se deberá actuar de conformidad con lo establecido en apartado «6.*10. Ejercicios de derecho de los interesados*».

6.6. Plazos de conservación de los datos

En el tratamiento de datos personales, es de vital importancia asegurar que la conservación de los datos que estén bajo nuestra custodia no supere los plazos legales establecidos en el ordenamiento jurídico.

De forma general y, como ya se ha hecho mención anteriormente, la regla general para la conservación de los datos es el cumplimiento de la finalidad para la que se recabaron. No obstante, podrán existir excepciones y otros plazos previstos en normas que establezcan una prescripción o caducidad distinta.

A estos efectos, deben consultarse los plazos de conservación aplicables a nuestra entidad consultando el documento "***POLÍTICA DE RETENCIÓN DE DATOS PERSONALES***".

6.7. Transferencias internacionales de datos personales

En caso de que fuera necesario realizar transferencias internacionales de datos, se verificará el grado de protección del país de destino y se adoptarán las garantías exigidas por la normativa. En primer lugar, se comprobará si existe una decisión de adecuación aprobada por la Comisión. A falta de la misma, se optará por cualquiera de los mecanismos recogidos en el artículo 46 RGPD, siendo preferible la firma de unas cláusulas contractuales tipo. Tan solo en supuestos excepcionales será alegada una de las excepciones contenidas en el artículo 49 RGPD. En todo caso nada de esto será aplicable cuando la transferencia sea necesaria en un proceso de cooperación internacional con organismos de terceros países y fuera de aplicación cualquier tratado o convenio internacional así como la Directiva (UE) 2016/680 y los artículos 43 a 47 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

6.8. Registro de las actividades de tratamiento

De conformidad con lo establecido por el artículo 30 RGPD, deberá llevarse un registro de las actividades efectuadas bajo la responsabilidad de la organización, debiéndose mantener actualizado frente a los cambios que se sucedan. Dicho registro deberá contener toda la información indicada a continuación:

a) 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;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país u organismo internacional, incluida la identificación del país u organismo y la garantía aplicada;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Asimismo, cuando se actúe como Encargado del tratamiento igualmente se llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organismo internacional, incluida la identificación del país u organismo y la garantía aplicada;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Dichos registros constarán por escrito, inclusive en formato electrónico.

6.9. Incidentes de seguridad

El RGPD define, de un modo amplio, las "violaciones o brechas de datos personales" como "*todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

Por contra, no tendrán consideración de brecha de datos personales sujetas a los artículos 33 y 34 del RGPD aquellos incidentes que:

- No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

Cualquier organización que trate datos personales se encuentra expuesta a sufrir una brecha de datos personales que pueda repercutir en los derechos y libertades de las personas físicas, y por tanto está obligada a preverlas y gestionarlas adecuadamente. A estos efectos, el RGPD establece en su artículo 33 la obligación de notificar las brechas de los datos personales que puedan suponer un riesgo para los derechos y libertades de las personas físicas a la Autoridad de Control competente y, en su caso a los interesados afectados, estableciendo para ello un plazo máximo de 72 horas para proceder a su notificación.

Por ello y con el fin de transmitir a cada integrante de la Entidad de una forma clara, concreta y precisa el protocolo a seguir ante este tipo de eventos, se ha desarrollado el documento "***PROCEDIMIENTO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD*"** con la finalidad de gestionar con éxito la respuesta frente a un incidente de seguridad y/o, en su caso, una violación de la seguridad de los datos, incluyendo las obligaciones relacionadas con la notificación a la Autoridad de Control Competente y cuando proceda, a los afectados, tal como lo exige el RGPD.

Asimismo, se establece que todo evento, incidente o violación debe ser registrada por el Responsable establecido a tal efecto, en el correspondiente "***REGISTRO DE INCIDENTES DE SEGURIDAD***".

6.10. Ejercicios de derecho de los interesados

La normativa de protección de datos permite a los interesados ejercer ante el responsable del tratamiento los derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

A estos efectos, la entidad ha habilitado los canales que, a continuación se exponen, para que los interesados remitan las correspondientes solicitudes de ejercicio de derechos:

CORREO POSTAL DE LA ORGANIZACIÓN: MARIA TUBAU Nº 5-5 (28050) MADRID
E-MAIL DE LA ORGANIZACIÓN: crispe@compromisoempresarial.es

CORREO POSTAL DEL DPD: C/ MENORCA Nº 19 - PISO 17º, ED. AQUA MULTIESPACIO (46023) VALENCIA
E-MAIL DEL DPD: infodpo@forlopd.es

Asimismo, con el objetivo de regular y establecer de forma detallada el protocolo de actuación ante el ejercicio de los derechos, la entidad ha desarrollado el documento "***PROTOCOLO DE RESPUESTA ANTE EL EJERCICIO DE DERECHOS***".

Dicho protocolo de actuación informa acerca del procedimiento establecido para atender los derechos de los interesados y resulta de aplicación tanto a los empleados autorizados a gestionar las solicitudes de derechos interpuestas por los interesados y el personal a su cargo, así como a otros terceros con acceso a datos y a aquellos encargados del tratamiento de la organización, incluido el personal a su cargo, quedando todos ellos sujetos a lo establecido en el citado protocolo, debiendo actuar en todo momento siguiendo las instrucciones establecidas.

7. NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

El Responsable del Tratamiento ha establecido las siguientes normas y procedimientos de seguridad de obligado cumplimiento, por parte de todo el personal que integra la organización. Dichas normas y procedimientos serán trasladadas al personal mediante le documento

"***MANUAL DE MEDIDAS DE SEGURIDAD APLICADAS AL TRATAMIENTO DE DATOS PERSONALES***":

7.1. Uso adecuado de los recursos de la organización

7.1.1. Dispositivos tecnológicos que el Responsable del Tratamiento pone a disposición del personal

Las tabletas, ordenadores, portátiles, móviles, teléfonos y cualquier otro dispositivo que sirva para el tratamiento, transporte y/o almacenaje de información que el Responsable del Tratamiento ponga a disposición del personal para realizar las labores encomendadas, deberá ser custodiado por la persona a la cual se haya asignado, debiendo cumplir con todas las medidas de seguridad que vengan impuestas por la empresa.

Dichos dispositivos no podrán emplearse con fines ajenos a la actividad laboral. Si el trabajador o la trabajadora necesita utilizarlo con fines ajenos a la actividad laboral, deberá contar con la autorización previa y por escrito de la organización.

Se debe tener especial cuidado cuando el dispositivo se encuentra en vehículos (incluyendo automóviles propios y/o de conocidos), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas, todas ellas exteriores a las instalaciones de la organización. El personal que utilice dispositivos fuera de las instalaciones deberá cumplir las siguientes reglas:

- No utilizar otros dispositivos informáticos diferentes a los suministrados.
- El dispositivo que contenga información importante, sensible, crítica o datos especialmente protegidos por el RGPD no debe ser desatendido, quedando en lo posible resguardado bajo llave. De igual forma se adoptarán, en su caso, trabas especiales para asegurarlo.
- Firmar y aceptar las condiciones de uso, contempladas en el documento «Registro *de Dispositivos*».
- No conectar a internet los dispositivos corporativos utilizando redes WIFI públicas sin utilizar el acceso VPN corporativo.
- Cuando se utilice equipamiento de computación móvil en lugares públicos, se deberá tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.

- Los dispositivos deberán contar con las últimas instalaciones de parches y actualizaciones del sistema operativo, de acuerdo con las actualizaciones periódicas previstas por el desarrollador del sistema.

- Las configuraciones de seguridad deberán venir predeterminadas por el responsable informático de la empresa.

- La protección contra códigos maliciosos debe estar instalada y configurada para que se actualice de forma automática.

- Como regla general, ningún dato de carácter personal deberá ser almacenado en soportes extraíbles. Si llegara a ser necesario utilizar cualquier tipo de soporte extraíble, se deberá solicitar autorización a la persona Responsable del Sistema, quien deberá registrar dicho soporte en el registro de soportes extraíbles.

- La persona que utiliza el "soporte" fuera de las instalaciones es la responsable de realizar periódicamente copias de seguridad de los datos.

- La información sensible, incluyendo los datos de carácter personal que se encuentra en ordenadores portátiles, deben estar encriptados o seudonimizados.

- Como regla general, los soportes no pueden ser desatendidos. En caso de que, de forma excepcional, el soporte sea desatendido, se deberán aplicar las reglas para equipamiento de usuario desatendido, de acuerdo con las normas establecidas en el apartado «*7.3. Política de pantallas limpias*».

- En caso de extravío, robo, hurto o acceso no autorizado al dispositivo, el personal deberá comunicar el acontecimiento de forma inmediata a la persona Responsable.

7.1.2. Internet y redes WIFI

Todo el personal debe procurar un uso seguro y legal, tanto de Internet como de las redes WiFi de la organización, por lo cual, bajo ningún pretexto podrán:

- Acceder a páginas web que supongan una actividad ilegal, o de contenido no relacionado con el trabajo, así como también el acceso a páginas de dudosa procedencia.

- Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma, material ilegal, como por ejemplo: pornografía, material amenazante, fraudulento, discriminatorio, difamatorio, ofensivo, obsceno, insultante o contrario a la moral y las buenas costumbres.

- Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma material de cualquier tipo que esté protegido por el secreto comercial o por patentes vigentes.

- Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma cualquier archivo de tipo musical, de lectura o filmográfico, sin tener los derechos de propiedad intelectual correspondientes.

- Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.

- Enviar mensajes no solicitados, cualquier tipo de virus, código malicioso o ataques internos o externos a la red.

- Dañar de cualquier forma equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red, tanto de la organización como de terceros.

- Interceptar, recopilar o almacenar datos sobre terceros que no estén relacionados con la actividad laboral y sin su conocimiento y consentimiento expreso.

- Obtener acceso no autorizado a equipos, sistemas o programas tanto dentro como fuera de la red.

- Conectarse a la red reservada para invitados.

- Conectarse a redes públicas sin utilizar el acceso VPN corporativo.

- Realizar cualquier otro tipo de acción, tanto de forma directa como indirecta, que ponga en riesgo la disponibilidad, integridad y/o confidencialidad de la información, como la seguridad e integridad de los sistemas que utiliza la organización.

7.1.3. Terminales y líneas telefónicas

Los terminales, tanto fijos como móviles, tarjetas SIM y líneas telefónicas contratadas, no pueden utilizarse para fines ajenos a los relacionados con la actividad laboral que el personal desempeña para el Responsable del Tratamiento.

Solamente podrán utilizarse para fines personales, los equipos señalados, en caso de emergencia familiar, o cuando el Responsable le autorice a ello, aunque en ningún caso podrán almacenarse en los mismos datos personales que puedan individualizar a una persona.

Queda también prohibido la manipulación de los terminales para lograr privilegios superiores a los otorgados por la organización, grabar llamadas, duplicar tarjetas SIM y en general cualquier actividad contraria a los mandatos mediante la presente expuestos.

Respecto de la instalación de aplicaciones, deberá cumplir con lo indicado en el apartado «*7.5. Instalación de programas por cuenta propia*» del presente documento.

7.1.4. Correo electrónico

Respecto al uso de la cuenta de correo electrónico profesional asignado al persona de la entidad, se establecen las siguientes obligaciones:

- Queda prohibido el envío de correos electrónicos en el que se adjunten bases de datos personales o bien se copie el contenido de las mismas dentro del cuerpo del correo electrónico. Si, por razones del trabajo debe enviarse este tipo de información, la misma deberá enviarse únicamente mediante un archivo adjunto y dicho archivo deberá estar cifrado. La clave, en ningún caso, se transmitirá por correo electrónico.

- Queda prohibido enviar o reenviar mensajes en cadena o con fines comerciales o publicitarios sin el consentimiento expreso del destinatario.

- Queda prohibido configurar la cuenta de correo electrónico profesional en cualquier dispositivo sin la autorización previa y por escrito de la dirección.

- Queda prohibido permitir el acceso al contenido de su cuenta de correo electrónico profesional a cualquier persona, ya sea personal interno como externo a la organización; sólo podrá tener acceso a su contenido a quien la dirección indique y por razón fundada.

- Respecto de la contraseña, deberá cumplir con lo indicado en el apartado 7.4 del presente documento.

- No podrá utilizarse la cuenta de correo personal, bajo ningún pretexto, para la realización de la actividad laboral.

- El correo electrónico corporativo solo podrá ser utilizado para los fines correspondientes a la actividad laboral y en ningún momento con fines propios o privados quedando totalmente prohibido el envío o la recepción de correos ajenos a las funciones laborales con contenido personal.

- Para el envío de un correo electrónico a varias personas, queda totalmente prohibido la remisión mediante la funcionalidad CC, debiéndose utilizar, en todo caso, para los emails con múltiples destinatarios la casilla CCO (con copia oculta).

7.1.5. Uso de herramientas basadas en sistemas de Inteligencia Artificial

El uso de sistemas de inteligencia artificial en la empresa queda sujeto a la previa autorización por parte de la dirección o el departamento responsable designado. Esta autorización se concederá considerando factores como la viabilidad técnica, los riesgos potenciales, el impacto en la privacidad y los derechos fundamentales, así como los beneficios esperados. El personal que desee utilizar sistemas de inteligencia artificial deberá presentar una solicitud que incluya la descripción de la finalidad y los objetivos del uso propuesto.

El uso de sistemas de dichos sistemas deberá cumplir estrictamente con las leyes y regulaciones aplicables en materia de protección de datos personales y privacidad. A estos efectos, queda expresamente prohibido introducir datos personales. Asimismo, queda prohibido introducir o generar información que pueda afectar a la confidencialidad y los secretos empresariales, así como a derechos de propiedad intelectual.

7.2. Política de escritorios limpios

Con miras a proteger la información contenida en los puestos de trabajo, deben llevarse a cabo las directrices que, a continuación, se establecen:

- Debe asegurarse de que el área de trabajo se encuentre limpia y ordenada, de forma que, tanto los documentos impresos, como los soportes removibles de almacenamiento de datos -tales como memorias USB, discos duros externos y tarjetas de memoria- sean retirados del escritorio, así como de los correspondientes puertos, con la finalidad de evitar el acceso no autorizado a los mismos. Asimismo, cuando la información sea especialmente sensible, confidencial o de naturaleza análoga, deberá incrementarse su seguridad, almacenándola en un lugar seguro y bajo llave o, en su caso, utilizando contraseñas seguras o métodos de cifrado o encriptación.

- Cuando se realicen labores de reprografía de documentos mediante la utilización máquinas reproductoras y análogas -tales como impresoras, equipos de fax, fotocopiadoras y escáneres- resulta esencial para garantizar la seguridad de la información, la retirada inmediata de la documentación. Asimismo, debe verificarse que no existan tareas pendientes en la cola de impresión.

- Los dispositivos móviles corporativos -tales como tables, teléfonos móviles y notebooks- deben ser igualmente retirados del escritorio y almacenados en un lugar seguro, a fin de evitar su hurto o uso indebido.

- Toda aquella información obsoleta almacenada de forma física debe ser destruida de manera confidencial y en el modo establecido en el apartado «*7.9. Gestión de soportes».*

- Queda prohibido colocar sobre los escritores y mesas de trabajo, recipientes o envases que contengan líquidos y cuyo cierre no sea hermético, con el fin de evitar su vertido encima de los equipos informáticos y/o cualquier otro tipo de soporte que pueda verse afectado por el vertido.

7.3. Política de pantallas limpias

Con el propósito de proteger la información contenida en los diversos dispositivos informáticos, debe procederse según las siguientes instrucciones:

- La ubicación de los puestos de trabajo y la colocación de las pantallas dentro de la Entidad está organizada de tal forma que sólo la persona que utiliza la misma puede leer lo que se plasma en la pantalla, evitando miradas indiscretas.

- Todos los dispositivos utilizados para el ejercicio de las funciones encomendadas, deberán contar con credenciales de acceso. Las contraseñas deberán ser lo suficientemente robustas. Las claves y sus combinaciones deberán conformarse siguiendo las directrices establecidas en el apartado «*7.4. Política de contraseñas*». Dichas claves no deberán ser expuestas ni comunicadas.

- En el caso de que el personal se ausente del puesto de trabajo, especialmente cuando se retire de las instalaciones de la Organización y al final de su jornada laboral, deberá quitar toda la información sensible de la pantalla y bloquear el acceso a todos los sistemas para los cuales la persona tiene autorización.

  En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se deberá implementar finalizando la sesión en todos los sistemas o bloqueando la pantalla mediante la función de bloqueo de equipo realizando la de la siguiente combinación: [Tecla Windows + L] o mediante la creación de otro atajo personalizado, con igual resultado. En el caso de una ausencia por un período más prolongado, se deberá finalizar la sesión en todos los sistemas, apagando el ordenador.

  Asimismo, con la finalidad de garantizar el cumplimiento de lo antedicho, se deberá configurar el bloqueo de pantalla automático de sesión, estableciendo un periodo de 10 minutos para que se active el modo de inactividad en el equipo correspondiente.

- Toda aquella información obsoleta almacenada en soporte digital debe ser destruida de manera confidencial y en el modo establecido en el apartado «*7.9. Gestión de soportes*» del presente documento.

7.4. Política de contraseñas

El manejo diario de la información de la entidad requiere el acceso a diversos servicios, dispositivos y aplicaciones para lo cual utilizamos el par de credenciales: usuario y contraseña.

Para garantizar la salvaguarda de la información, resulta necesario que dichas credenciales de autenticación se generen, actualicen y revoquen de forma óptima y segura. A estos efectos, la organización ha establecido un procedimiento para garantizar un control de acceso seguro a los distintos dispositivos, servicios y aplicaciones de la entidad, que, a continuación, se detalla:

- La contraseña deberá tener, al menos, 8 caracteres.
- Deberán combinarse letras mayúsculas y minúsculas, números y símbolos.
- No podrá utilizar la misma contraseña en diferentes servicios.
- No podrá utilizar aquellas contraseñas que utilice en su vida privada, por ejemplo, la de acceso al banco, a su cuenta de red social, etc.
- No podrá reutilizar contraseñas que ya haya utilizado previamente.
- No podrá utilizar patrones de teclado, por ejemplo: “qwerty” o “uiop” o “1qaz” “2wsx” o “3edc” ni la combinación de estas, ni palabras sencillas en cualquier idioma, nombres propios, fechas, lugares o datos de carácter personal.
- No utilizar las contraseñas dadas por defecto.
- No hacer uso del recordatorio de contraseñas.
- Las contraseñas tienen un período de vigencia de 3 meses.
- Una vez creada la contraseña, deberá asegurar su correcta gestión y almacenamiento, por lo cual, deberá seguir las siguientes directrices:

    - No apuntar la contraseña en notas y pegarlas en el escritorio, pantalla u ordenador.
    - No utilizar la opción de “recordar contraseña” que ofrecen los navegadores.
    - No almacenar la contraseña, dentro de su ordenador, en archivos sin cifrar y que estén a la vista de cualquier usuario y que lleven nombres que permita su fácil identificación, por ejemplo: “listado de contraseñas”, “contraseñas”, “pass”, “password”, etc.
    - Queda prohibido divulgar, compartir y/o entregar, tanto a personal interno como externo de la organización, las contraseñas que sean de su responsabilidad.
    - En aquellos casos en los que se tenga que recordar un gran número de contraseñas, se permite el uso de gestores de contraseñas siempre que dicho gestor cifre las credenciales y cuente con doble factor de autenticación para acceder al mismo.

7.5. Instalación de programas por cuenta propia

El personal no puede instalar ningún tipo de software por cuenta propia sin la autorización previa y por escrito del Responsable del Tratamiento.

En el caso que el proceda a la instalación sin autorización ni conocimiento por parte de la organización del Responsable del Tratamiento, el usuario quedará vinculado y será responsable en caso de daños ocasionados al equipo informático y/o a la información en él contenida como consecuencia de dicha instalación.

Antes de instalar un programa, el personal autorizado deberá comprobar que se cuenta con la licencia y derechos de uso del programa; con la certificación del programa para su compatibilidad con el sistema operativo y los demás aplicativos; con la garantía del código para evitar la posible presencia de virus, troyanos y otros programas espías.

En todo caso, cualquier tipo de software que se instale, deberá mantenerse actualizado siguiendo las indicaciones del desarrollador del software en cuestión.

7.5.1. Pruebas con datos reales

Las pruebas anteriores a la implantación y/o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales.

En el caso de resultar necesario utilizar datos reales con el fin de poder realizar la prueba de forma positiva, deberá asegurarse el nivel de seguridad correspondiente al tipo de tratamiento y a los datos de carácter personal afectados para que los mismos no sean objetos de una brecha de seguridad.

7.6. Control de accesos

El personal sólo puede acceder a aquellos datos y dependencias que sean necesarias para el correcto desarrollo de sus funciones.

7.6.1. Entrada y salida de las instalaciones de la organización

Es responsabilidad del personal asegurar que las dependencias, despachos, armarios y cajoneras con llaves, permanezcan cerrados cuando finalice la jornada laboral o se ausenten de su puesto de trabajo, siendo responsable de la custodia de las llaves, tarjetas de identificación y/o claves que la organización le entrega, no pudiendo entregarla a terceras personas.

Queda prohibido realizar copias de las llaves al igual que distribuir las mismas sin autorización expresa del Responsable del Tratamiento. Tampoco se podrá ceder o prestar las mismas a terceras personas sin autorización expresa del Responsable del Tratamiento.

En caso de extravío, el personal responsable deberá comunicarlo sin dilación indebida al Responsable del Tratamiento o a aquella persona que designe el Responsable del Tratamiento.

7.6.2. Cuarto del servidor

Únicamente el Responsable de Seguridad y/o el personal autorizado por este, están autorizados para acceder a las dependencias en las que se encuentren los sistemas de información que corresponden al servidor y a las copias de respaldo.

Es responsabilidad de quienes tengan asignadas llaves, o en su caso, las claves de acceso, la custodia de las mismas, al igual que la comunicación de su extravío al Responsable del Tratamiento o a aquella persona que designe el Responsable del Tratamiento.

Queda prohibido realizar copias, al igual que distribuir, o ceder las laves o claves de acceso, sin autorización expresa del Responsable del Tratamiento.

7.6.3. Acceso a datos personales e información confidencial

Para proteger la información es esencial controlar quien accede a la información de la cual es responsable la organización. Con esta finalidad de gestionar el control de acceso a los datos, la entidad ha establecido permisos en los servicios y aplicaciones utilizadas para el desarrollo de las funciones que le son propias. Así pues, se han llevado a cabo las siguientes acciones:

- Definición de los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.
- Asignación de permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso.
- Gestión de las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.
- Procedimiento de creación/modificación/borrado de cuentas de usuario con permisos.
- Establecimiento de mecanismos de autenticación.
- Revisión periódica de los permisos concedidos a los usuarios.
- Revocación de permisos y eliminación de cuentas de usuario una vez finalizada la relación contractual.

7.7. Régimen de trabajo fuera de los locales de la organización

El tratamiento de datos de carácter personal, fuera de los locales de la organización, deberá ser autorizado expresamente por el Responsable del Tratamiento, teniéndose en consideración las funciones que realiza el personal en la organización.
En el caso de que se autorice el tratamiento de datos fuera de los locales de la organización, el personal que los trate, los usuarios deberán cumplir con todas las medidas de seguridad indicadas en el presente documento y con todas aquellas que establezca la organización para el caso concreto.

7.8. Copias de respaldo y recuperación

La organización debe copias de seguridad de forma habitual y sistemática. El personal deberá acatar las indicaciones que vengan impartidas por el Responsable o, en su caso, por el departamento informático de la empresa.

7.9. Gestión de soportes

7.9.1. Utilización de soportes extraíbles

Por regla general, el personal no podrá disponer fuera de la entidad de ningún soporte con datos de carácter personal en los que la entidad actúe como Responsable o Encargado del Tratamiento. El personal laboral que lo desee deberá solicitar una autorización previa para el tratamiento de datos en relación con las salidas y/o entradas de soportes del centro de trabajo. En este caso, se deberá llevar un registro adecuado que contemple la fecha de entrega, el dispositivo y el personal al que se asigne.

Únicamente el Responsable del Tratamiento, o a quién éste designe, podrá autorizar la salida de datos de carácter personal en soportes extraíbles de la organización.

7.9.2. Disposición final de soportes

La destrucción de la documentación, ya sea en soporte papel o digital, que se genera como consecuencia del desarrollo de las funciones inherentes al puesto de trabajo, sobre todo cuando contenga datos personales, tiene una labor previa que si no se realiza correctamente puede derivar en un incumplimiento de la normativa de protección de datos.

Por lo expuesto, no pueden tirarse los documentos ni soportes, de ningún tipo, directamente a la basura, ni aunque se rompan en trozos. La disposición final de los mismos se realizará de la siguiente forma:

- Si se va a desechar el soporte, por ejemplo, un ordenador, portátil o móvil, discos duros, DVD’s, CD’s, memorias USB, cintas o cualquier otro tipo de dispositivo digital; por mal funcionamiento, antigüedad, inutilidad, etc., el empleado deberá ponerlos a disposición del Responsable del Tratamiento o de la persona designada por este a tal, para que dicha persona proceda a su desechado.

- Si se va a desechar información contenida en papel, el trabajador deberá arrojarlos a los contenedores habilitados a tal fin.

7.10. Política de borrado seguro de documentación electrónica

El objetivo de borrar y destruir los soportes de información no es solo proteger la distribución de la información confidencial de una organización, sino también proteger la difusión de información personal.

Por ello, en aras de garantizar las finalidades antedichas, y en suma a lo expuesto en el apartado anterior, resulta de vital importancia gestionar los recursos que ya no van a ser utilizados, esto es, destruir la información confidencial, así como los datos de carácter personal contenidos en los archivos electrónicos almacenados en los dispositivos, evitando así el acceso a dicha información y su recuperación posterior.

Con estos fines, cuando un archivo pierda su utilidad, inmediatamente deberá procederse a la supresión del mismo. No obstante, hay que tener en cuenta que cuando se utilizan métodos de borrado proporcionados por el propio sistema operativo, como la opción «eliminar» o la tecla «Supr» o «Delete», el borrado se produce exclusivamente en la "Lista de archivos" sin borrar realmente el contenido del mismo, el cual sigue permaneciendo en la zona de almacenamiento. Por tanto, toda aquella acción que no conlleve la eliminación total no garantiza la destrucción segura de la información. Por esta razón, será necesario borrar los archivos y carpetas eliminados de la papelera de reciclaje.

Para ello se deberán seguir los siguientes pasos:

1.- Buscar el icono de papelera de reciclaje en el escritorio.
2.- Hacer clic en el botón secundario y seleccionar «Vaciar papelera de reciclaje». Alternativamente: acceder a la papelera de reciclaje haciendo doble clic y volver a hacer clic en el botón «Vaciar papelera de reciclaje».

Este proceso deberá realizarse de forma diaria, al final de cada jornada laboral.

8. HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción del cambio
V.00	01-06-2023	Primer ejemplar.

ANEXO I

CATEGORÍAS Y TIPOLOGÍAS DE DATOS PERSONALES

Identificativos: Nombre y apellidos; DNI / CIF / documento identificativo; Dirección; Correo electrónico; Teléfono; Fax; Nº de registro de personal; Nº seguridad social / mutualidad; Tarjeta sanitaria; Firma; Firma electrónica; Nombre de usuario; Huella; Imagen; Carné de conducir; Datos de geolocalización; Datos de tráfico de red de telecomunicaciones; Datos de navegación del usuario que pueden identificarle; Carné de Identidad; IP; Voz.

Características personales: Sexo; Estado civil; Nacionalidad, Edad; Fecha y lugar de nacimiento; Lengua materna; Altura; Peso; Características antropométricas; Marcas físicas; Aptitudes; Comportamientos; Gustos y / o preferencias; Aficiones.

Circunstancias familiares y sociales: Número de hijos; Edad de hijos; Permisos, licencias y autorizaciones; Filiación; Inscripciones en foros, clubes o asociaciones; Ayudas y subvenciones; Permiso de residencia.

Detalles de empleo: Puesto/cargo; Categoría o grupo profesional; Departamento; Empresa; Datos no económicos de nómina; Datos de baja; Datos de contacto corporativos; Permiso de trabajo

Académicos y profesionales: Titulaciones; Formación; Experiencia profesional; Historial de estudiante; Datos de colegios profesionales.

Judiciales y administrativos: Procedimientos administrativos; Reclamaciones y recursos; Sanciones; Registros; Solicitudes; Expediente o historial judicial; Procedimientos judiciales.

De control de presencia: Fecha / hora de entrada y salida; Motivo de ausencia; ID de control de presencia.

Económicos, financieros y de seguros: Ingresos; Rentas; Inversiones; Créditos; Préstamos; Avales; Deducciones impositivas; Baja de haberes correspondiente al puesto de trabajo anterior; Retenciones; Datos bancarios; Datos de actividad económica y solvencia; Bienes patrimoniales; Herencias; Impuestos; Planes de pensión y jubilación.

Información comercial: Actividades y negocios; Licencias comerciales; Subscripciones a publicaciones o medios de comunicación; Creaciones artísticas, literarias, científicas o técnicas.

Relativos a condenas e infracciones penales: certificado de antecedentes penales, certificado de delitos de naturaleza sexual, demandas y sentencias penales, etc.

Categorías especiales: Origen étnico o racial; Opiniones políticas.; Convicciones religiosas o filosóficas; Afiliación sindical; Datos genéticos; Datos biométricos; Datos relativos a la salud; Datos relativos a la vida o la orientación sexual.

SIGNIFICADO DE LOS DISTINTOS TRATAMIENTOS

- **Acceso:** posibilidad de acceso al sistema o dispositivo en el que se encuentra registrada la información que contiene datos de carácter personal.
- **Consulta:** búsqueda de información que contiene datos personales en el sistema o dispositivo en el que se encuentra registrada.
- **Recogida:** captura de información que incluye datos de carácter personal
- **Extracción:** obtención de información desde un sistema o dispositivo para su traspaso a otro sistema.
- **Registro:** inscripción o grabado de información que contiene datos de carácter personal en sistemas o dispositivos automatizados o no, para su posterior tratamiento.
- **Utilización:** uso de la información para una finalidad concreta.
- **Organización o estructuración:** ordenar y estructurar la información que contiene datos personales con la finalidad de facilitar su tratamiento.
- **Comunicación:** comunicar información que contiene datos personales a otro destinatario
- **Comunicación por transmisión:** enviar información que contiene datos personales a otro destinatario a través de un dispositivo a través de medios electrónicos.
- **Adaptación o modificación:** alterar o modificar la información que contiene datos personales.
- **Conservación/Servicio Cloud:** mantener la información durante un tiempo determinado/ prestar el servicio de conservación de la información que contiene datos personales utilizando computación en la nube.
- **Interconexión:** conexión física, lógica y funcional de las bases de datos utilizadas por los mismos o diferentes operadores de información que contiene de datos personales, de manera tal que los usuarios de estas bases de datos puedan comunicarse entre sí.
- **Cotejo:** comparación y examen de datos de carácter personal para apreciar sus semejanzas y diferencias.
- **Limitación:** limitar los tratamientos de los datos personales que hasta ahora se estaban llevando a cabo de conformidad con lo dispuesto por el artículo 18 RGPD.
- **Supresión:** eliminación de la información que contiene datos de carácter personal del dispositivo, sistema o soporte en el que se encuentre registrada.
- **Destrucción:** inutilizar el soporte físico para el acceso a la información.