FUNDACION LA MAQUINISTA DE LEVANTE

MEDIDAS Y PROCEDIMIENTOS RGPD

PROTOCOLO DE SEGURIDAD

Este documento recoge las obligaciones de la empresa responsable del tratamiento y de los encargados del tratamiento, los contratos recomendados para regular la relación con sus clientes, proveedores, empleados, así como empresas que nos presten servicios en relación a la normativa de protección de datos de carácter personal. Además, se incluye el registro de actividades de tratamiento y recomendaciones sobre las medidas de seguridad a adoptar. Una vez cumplimentado podrá obtener un documento de auditoría, con resultados y recomendaciones en caso de respuesta negativa.

FUNDACION LA MAQUINISTA DE LEVANTE

ÍNDICE DE APARTADOS:

Introducción

En este documento se incluye información y ayuda en relación a la nueva normativa de protección de datos, partiendo del Reglamento General de Protección de Datos (RGPD) en vigor desde mayo de 2016 pero aplicable desde mayo de 2018.

La documentación se genera con la información que se haya introducido previamente en la aplicación a3ASESOR|rgpd y va dirigida a empresas con tratamientos de datos que no sean de categoría especial (salud, origen étnico o racial, datos genéticos, datos biométricos, etc.) y que supongan un escaso riesgo para los derechos y libertades de las personas físicas.

En concreto se incluyen las obligaciones de la empresa responsable del tratamiento y de los encargados del tratamiento, los contratos recomendados para poder regular la relación con encargados de tratamiento, clientes, proveedores o potenciales empleados y empresas que nos presten determinados servicios en relación a la normativa de protección de datos de carácter personal.

Además, se incluye el registro de actividades de tratamiento y un anexo con diferentes recomendaciones para la empresa sobre las medidas de seguridad a adoptar.

Si se cumplimenta, también se puede obtener un documento de auditoría, con resultados y recomendaciones en caso de respuesta negativa.

En el caso de que se realicen imágenes captadas por cámaras de videovigilancia, en el anexo se puede disponer de una serie de recomendaciones.

1. Empresa responsable del tratamiento

1.1. Identificación

- ✓ NIF: G30854343
- ✓ Nombre o razón social: FUNDACION LA MAQUINISTA DE LEVANTE
- ✓ Dirección: CL SAGUNTO, 1, C.P. 30360 LA UNION (MURCIA) ESPAÑA.
- ✓ Teléfono: +34 646 47 93 43
- ✓ Correo electrónico: fundacionmaquinistalevante@gmail.com

1.2. Obligaciones generales

Dentro de las diversas obligaciones que establece la normativa de protección de datos, la empresa, como responsable del tratamiento de los datos personales que custodia y utiliza dentro del ejercicio de su actividad, deberá responsabilizarse del cumplimiento de una serie de principios generales y deberá ser capaz de demostrarlo (lo que se entiende como «responsabilidad proactiva»).

Es por ello que la empresa debe procurar que estos datos personales sean:

a) Tratados de manera lícita, leal y transparente en relación con el interesado.

b) Recogidos con fines determinados, explícitos y legítimos, y no deberán ser tratados posteriormente de manera incompatible con dichos fines.

c) Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

d) Exactos y, si fuera necesario, actualizados. Por ello se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin demora los datos personales que sean inexactos con respecto a los fines para los que se tratan.

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.

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.

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el

tratamiento para los derechos y libertades de las personas físicas, la empresa deberá determinar cuáles son las medidas técnicas y organizativas apropiadas.

La empresa debe aplicar estas medidas tanto en el momento de determinar los medios que utilizará como en el momento del propio tratamiento con el objetivo de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento General de Protección de Datos (RGPD) para proteger los derechos de los interesados y garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

Estas medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Debe considerarse que la adhesión a códigos de conducta o a algún mecanismo de certificación reconocido se podrá utilizar como argumento para demostrar el cumplimiento de las obligaciones por parte de la empresa.

2. Encargado del tratamiento / asesoría

2.1. Identificación

- ✓ NIF: 15482865R
- ✓ Nombre o razón social: VIOLETA ALBALADEJO YEBENES
- ✓ Dirección: CL MAYOR, 75 1 B. 30360 LA UNION. MURCIA.
- ✓ Teléfono: 968542000
- ✓ Correo electrónico: violeta@jlasconi.com

2.2. Obligaciones

El encargado del tratamiento, generalmente una asesoría, que presta sus servicios al responsable que se identifica en este documento garantiza que dispone de las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento General de Protección de Datos (RGPD) y garantiza la protección de los derechos de los interesados que han cedido sus datos personales.

La asesoría no podrá recurrir a otro encargado u otra asesoría sin la autorización previa por escrito, específica o general, de la empresa responsable de los datos.
En este último caso, la asesoría informará a la empresa de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así a la empresa responsable la oportunidad de oponerse a dichos cambios.

El tratamiento por la asesoría se regirá por un contrato u otro acto jurídico con arreglo a derecho y vinculará a la asesoría respecto de la empresa responsable y establecerá el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Dicho contrato estipulará, en particular, que la asesoría encargada del tratamiento:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas de la empresa responsable.

b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

c) Tomará todas las medidas de seguridad necesarias y adecuadas según normativa.

d) Respetará las condiciones indicadas para recurrir a otro encargado del tratamiento.

e) Asistirá a la empresa responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

f) Ayudará al responsable a garantizar el cumplimiento de sus obligaciones establecidas, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.

g) A elección de la empresa responsable, suprimirá o retornará todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes.

h) Pondrá a disposición de la empresa responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. La asesoría informará inmediatamente al responsable si, en su opinión, una instrucción infringe la normativa.

Cuando una asesoría recurra a otra para llevar a cabo determinadas actividades de tratamiento por cuenta de la empresa responsable, se impondrá a esta otra, mediante contrato u otro acto jurídico, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre la empresa responsable y la asesoría principal, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del RGPD. Si esa otra asesoría secundaria incumple sus obligaciones de protección de datos, la asesoría principal inicial seguirá siendo plenamente responsable ante la empresa responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones de la secundaria.

La adhesión de la asesoría a un código de conducta o a un mecanismo de certificación reconocido podrá utilizarse como elemento para demostrar la existencia de las garantías.

El contrato constará por escrito, inclusive en formato electrónico.

Si la asesoría infringe el RGPD al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

La asesoría como encargado del tratamiento y cualquier persona que actúe bajo la autoridad de la empresa responsable o de la asesoría y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones de la empresa responsable.

3. Documentación Legal

3.1. Anexos contractuales

- **CLIENTES, DONANTES, PATROCINADORES O MECENAS**

Plantilla de anexo contractual a incorporar en los formularios que se utilicen para solicitar datos personales de clientes.

- ✓ NIF: G30854343
- ✓ Nombre o razón social de la empresa: FUNDACION LA MAQUINISTA DE LEVANTE
- ✓ Dirección: CL SAGUNTO, 1, C.P. 30360 LA UNION (MURCIA) ESPAÑA.
- ✓ Teléfono: +34 646 47 93 43
- ✓ Correo electrónico: fundacionmaquinistalevante@gmail.com

En FUNDACION LA MAQUINISTA DE LEVANTE se van a utilizar sus datos personales para poder realizar informarle de las actuaciones que con sus donaciones se realizan en la Entidad.

Los datos personales facilitados se tratarán y mantendrán mientras exista relación comercial o durante los años necesarios para cumplir con las obligaciones legales correspondientes. Los datos no se cederán a terceros salvo que exista una obligación legal. (La cesión de datos es referida a Administraciones Públicas y fuerzas de seguridad del Estado).

Le recordamos que, como interesado, dispone de una serie de derechos, entre ellos el derecho a conocer si en nuestra empresa FUNDACION LA MAQUINISTA DE LEVANTE tratamos sus datos personales, y si es así tiene derecho de acceso a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

Finalmente FUNDACION LA MAQUINISTA DE LEVANTE necesita y por ello solicita su autorización expresa para poder enviarle comunicaciones de los proyectos, cursos e investigaciones que se vayan realizando y que le podrían interesar al aportar su donación.

Marque si autoriza el tratamiento de datos: ☐ SI ☐ NO

- **CANDIDATOS**

Plantilla de anexo a incorporar en los formularios que se utilicen para solicitar datos personales de candidatos.

- ✓ NIF: G30854343
- ✓ Nombre o razón social de la empresa: FUNDACION LA MAQUINISTA DE LEVANTE
- ✓ Dirección: CL SAGUNTO, 1, C.P. 30360 LA UNION (MURCIA) ESPAÑA.
- ✓ Teléfono: +34 646 47 93 43
- ✓ Correo electrónico: fundacionmaquinistalevante@gmail.com

En FUNDACION LA MAQUNISTA DE LEVANTE se van a utilizar sus datos personales con el objetivo de informarle de posibles vacantes en puestos de trabajo que se pudieran producir en nuestra empresa.

Los datos personales que no facilite se tratarán y mantendrán hasta que se seleccione la persona que cubrirá dicho puesto de trabajo o hasta que usted ejerza su derecho de cancelación. Los datos no se cederán a terceros salvo que exista una obligación legal.

Le recordamos que, como interesado, dispone de una serie de derechos, entre ellos el derecho a conocer si en FUNDACION LA MAQUINISTA DE LEVANTE tratamos sus datos personales y, si es así tiene derecho de acceso a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

- **PROVEEDORES**

Plantilla de anexo contractual a incorporar en los formularios que se utilicen para solicitar datos personales de los proveedores.

- ✓ NIF: G30854343
- ✓ Nombre o razón social de la empresa: FUNDACION LA MAQUINISTA DE LEVANTE
- ✓ Dirección: CL SAGUNTO, 1, C.P. 30360 LA UNIONB (MURCIA) ESPAÑA.
- ✓ Teléfono: +34 646 47 93 43
- ✓ Correo electrónico: fundacionmaquinistalevante@gmail.com

En FUNDACION LA MAQUINISTA DE LEVANTE utilizamos sus datos personales para solicitarle y realizar pedidos con sus correspondientes facturas.

Nuestra empresa va a conservar los datos personales que nos proporcione mientras no nos solicite el cese de la relación contractual y de la actividad y siempre respetando el plazo necesario para cumplir las obligaciones de la normativa vigente.

Los datos no se cederán a terceros excepto cuando exista una obligación legal.

Le recordamos que, como interesado, dispone de una serie de derechos, siendo el primero de ellos conocer si en FUNDACION LA MAQUINISTA DE LEVANTE tratamos sus datos personales, y si es así le recordamos que también dispone del derecho de acceso a sus datos personales, a rectificar los datos inexactos o a solicitar su supresión cuando los datos ya no sean necesarios para la finalidad que fueron recogidos.

3.2. Contratos

A continuación se relacionan varias plantillas con los textos propuestos en cada caso para incluir como anexos en las relaciones contractuales que se formalicen entre la empresa responsable de los datos personales y las diferentes empresas encargadas de tratamiento con las que se van a compartir estos datos.

Estos documentos servirán como base para el cumplimiento de las obligaciones que deben cumplir los diferentes encargados de tratamiento en relación a la normativa de protección de datos.

Los documentos que se incluyen son:

- CON LA ASESORÍA QUE VA A TRATAR LOS DATOS PERSONALES DE NUESTROS EMPLEADOS EN RELACIÓN A LA PROTECCIÓN DE DATOS PERSONALES.

RELACIÓN CONTRACTUAL CON LA ASESORÍA QUE VA A TRATAR DATOS PERSONALES DE NUESTROS EMPLEADOS EN RELACIÓN A LA PROTECCIÓN DE DATOS PERSONALES

LA EMPRESA RESPONSABLE DE LOS DATOS

De una parte, la empresa responsable de los datos FUNDACION LA MAQUINISTA DE LEVANTE con NIF G30854343 y con domicilio profesional/social en CL. SAGUNTO, 1, C.P. 30360 LA UNION (MURCIA) ESPAÑA. representada por la persona autorizada que firma el documento.

LA ASESORÍA/ ENCARGADO DEL TRATAMIENTO

De otra parte, VIOLETA ALBALADEJO YEBENES con NIF 15482865R y con domicilio profesional/social en CL MAYOR, 75 1 B. 30360 LA UNION. MURCIA. representada por la persona autorizada que firma el documento.

AUTORIZACIÓN COMO ENCARGADO DEL TRATAMIENTO

Ambas partes, conocedoras de la legislación vigente en materia de Protección de Datos de Carácter Personal, están interesadas en regular con carácter general, el tratamiento de Datos de Carácter Personal que en el curso de la prestación de los servicios que siguen pudieran producirse.

Por ello, se autoriza a VIOLETA ALBALADEJO YEBENES, con dirección en CL MAYOR, 75 1 B. 30360 LA UNION. MURCIA. y NIF 15482865R como encargado del tratamiento para tratar por cuenta de FUNDACION LA MAQUINISTA DE LEVANTE, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifica.

El tratamiento consistirá en Servicio de asesoria

La empresa responsable del tratamiento para poder realizar la prestación de servicios entregará a la asesoría encargada los datos personales necesarios.

Esta entrega no exime a la empresa responsable de sus obligaciones como serán la de procurar, tanto de forma previa como durante todo el tratamiento, el cumplimiento del RGPD por parte de la asesoría y, dentro de sus posibilidades, supervisar el uso de estos datos por parte de la misma.

DURACIÓN Y DATOS PERSONALES

La duración de esta relación contractual será de , con renovación automática al finalizar cada plazo salvo denuncia por alguna de las partes.

Cuando acabe la relación contractual o finalice la prestación de los servicios de tratamiento la asesoría, a elección de la empresa responsable, suprimirá o devolverá todos los datos personales y suprimirá las copias existentes.

Si la empresa responsable de los datos lo estipula el encargado del tratamiento deberá transmitir estos datos al nuevo encargado que haya sido designado por aquella, aunque podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas.

OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

La asesoría como encargado del tratamiento y el personal empleado de la misma que tenga autorización para tratar los datos personales de los clientes tienen una serie de obligaciones:

- Adoptar todas las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y estabilidad de los sistemas utilizados y servicios de tratamiento (equipos informáticos, redes, periféricos, etc.).

- Tratar los datos personales únicamente siguiendo instrucciones documentadas de la empresa responsable y sólo hacerlo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

- Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las normas de seguridad establecidas. Adicionalmente, se deberá tener a disposición de la empresa responsable la documentación necesaria que acredite el cumplimiento estas obligaciones y servirá también para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

- Procurar que las personas autorizadas reciban una formación adecuada en materia de protección de datos.

- No ceder ni facilitar los datos a terceras personas, salvo que cuente con la autorización expresa de la empresa responsable del tratamiento. Si la asesoría quiere subcontratar a otra asesoría debe informar al responsable y solicitar su autorización.

- Mantener el deber de secreto respecto a los datos de carácter personal que esté tratando por esta relación contractual, incluso después de que finalice el contrato.

- Asistir a la empresa responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que esta pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados, como son los derechos de acceso, rectificación, supresión y

oposición, limitación del tratamiento y portabilidad de datos. Si se ejercen ante la asesoría, ésta debe comunicarlo por correo electrónico a la dirección que indique el responsable. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

- La asesoría deberá llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la empresa responsable, que contenga:

  a) El nombre y los datos de contacto de la asesoría y de la empresa responsable de los datos personales.

  b) Las categorías de tratamientos efectuados por cuenta de la empresa responsable.

  c) Una descripción general de las medidas técnicas y organizativas de seguridad que se vayan a aplicar.

  d) El registro será por escrito, aunque puede ser en formato electrónico.

- En caso de finalización de la relación contractual, devolver a la empresa responsable los datos de carácter personal y, si procede, los soportes donde se guarde la información. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por la asesoría, aunque se podrá conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades por la prestación del servicio de asesoría.

- Notificación de violaciones de la seguridad de los datos: La asesoría notificará a la empresa responsable, sin demora injustificada y a través de la dirección de correo electrónico que le indique la empresa responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.
  La notificación deberá, como mínimo:

  a) Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
  b) Comunicar el nombre y los datos de la persona de contacto con la que pueda obtenerse más información.
  c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
  d) Describir las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin retrasos indebidos.

LA EMPRESA	LA ASESORÍA
Firmado (Representante legal)	Firmado (Representante legal)

4. Registro de Actividades de Tratamiento

Responsable del tratamiento. Datos de la empresa:

- NIF: G30854343
- Nombre o razón social: FUNDACION LA MAQUINISTA DE LEVANTE
- Dirección: CL SAGUNTO, 1, C.P. 30360 LA UNION (MURCIA) ESPAÑA.
- Teléfono: +34 646 47 93 43
- Correo electrónico: fundacionmaquinistalevante@gmail.com

Datos del tratamiento

Tipo o nombre del tratamiento: **Clientes**

Descripción o finalidad del tratamiento: Gestión de la relación con los clientes

Descripción de las categorías de clientes y de las categorías de datos personales:

Categorías de interesados:

Clientes.- Son las personas o empresas con las que la empresa mantiene una relación comercial para venderles productos o servicios de forma regular.

Se tratan las siguientes categorías de datos personales necesarios para el mantenimiento de la relación comercial:

De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail
Datos bancarios: para la domiciliación de pagos

Los datos se van a utilizar para:

Prestación de servicios
Facturar

Plazos previstos para la supresión de los datos:

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos serán los previstos por la normativa y legislación fiscal respecto a la prescripción de responsabilidades.

Datos del tratamiento

Tipo o nombre del tratamiento: **Empleados**

Descripción o finalidad del tratamiento: Gestión de la relación laboral con los empleados.

Descripción de las categorías de empleados y de las categorías de datos personales:

Categorías de interesados:

Empleados.- Personas que trabajan para la empresa responsable del tratamiento.

Se tratan las siguientes categorías de datos personales necesarios para el mantenimiento de la relación comercial:

De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail
Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad
Datos académicos
Datos profesionales
Datos bancarios: para la domiciliación de pagos

Los datos se han obtenido de:

Los han facilitado los interesados

Los datos se van a utilizar para:

Gestionar sus nóminas
Formación
Mantenimiento de la relación laboral

Plazos previstos para la supresión de los datos:

Cuando sea posible, los plazos previstos por la legislación fiscal y laboral en relación a la prescripción de las responsabilidades.

Datos del tratamiento

Tipo o nombre del tratamiento: **Candidatos**

Descripción o finalidad del tratamiento: Gestión de la relación con los candidatos a ser trabajadores de la empresa.

Descripción de las categorías de candidatos y de las categorías de datos personales:

Categorías de interesados:

Candidatos.- Personas que quieren trabajan para la empresa responsable del tratamiento.

Se tratan las siguientes categorías de datos personales necesarios para gestionar los currículums de posibles futuros empleados de la empresa:

De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail
Datos académicos
Datos profesionales

Los datos se han obtenido de:

Los han facilitado los interesados en formato papel

Plazos previstos para la supresión de los datos:

Cuando sea posible, el plazo para la supresión de los datos será de un año desde la presentación de la candidatura.

Datos del tratamiento

Tipo o nombre del tratamiento: **Proveedores**

Descripción o finalidad del tratamiento: Gestión de la relación con los proveedores de la empresa.

Descripción de las categorías de proveedores y de las categorías de datos personales:

Categorías de interesados:

Proveedores.- Personas o empresas a las que se les compran mercancías o servicios y con las que se mantiene, normalmente, una relación estable.

Se tratan las siguientes categorías de datos personales necesarios para mantener la relación mercantil:

De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail
Datos bancarios: para la domiciliación de pagos

Los datos se van a utilizar para:

Facturación
Realizar pedidos

Plazos previstos para la supresión de los datos:

Cuando sea posible, el plazo para la supresión de los datos será el previsto por la normativa fiscal para la prescripción de responsabilidades.

5. Recomendaciones sobre Medidas de Seguridad

Introducción

En este apartado se detallan las normas y los procedimientos recomendados para aplicar las medidas de seguridad en tratamientos de bajo nivel de riesgo por lo que no va dirigido a tratamientos de categorías especiales de datos personales **(*)**.

En los diferentes apartados, se relacionan algunas medidas que se consideran obligatorias para garantizar una seguridad mínima de los datos y después se añaden diferentes medidas como recomendaciones y será cada empresa la que deberá decidir cuáles se adaptan mejor a su organización siempre con vistas a garantizar el nivel de seguridad adecuado para los datos personales.

Las medidas que decida la empresa, deberán ser conocidas por el personal con acceso a los datos de carácter personal y afectarán a los sistemas e instalaciones que contienen los datos, y tienen como objetivo aplicar de forma efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento General de Protección de Datos (RGPD) y proteger los derechos de los interesados.

Las medidas de seguridad deberán ser revisadas de manera permanente y periódica y cualquier modificación relevante deberá comunicarse al personal afectado.

El RGPD determina la necesidad de establecer las medidas de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de datos, la destrucción o el daño accidental. El principio de responsabilidad proactiva que incorpora la nueva normativa conlleva la obligatoriedad de establecer medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la necesidad de demostrar que estas medidas se han llevado a la práctica.

En casos de encargar el tratamiento a otra empresa, para garantizar el cumplimiento del RGPD respecto del tratamiento que lleve a cabo el encargado, la empresa responsable al asignar actividades de tratamiento debe recurrir a encargados que ofrezcan suficientes garantías para la aplicación de medidas de seguridad adecuadas para el tratamiento. La adhesión del encargado a un código de conducta o mecanismo de certificación aprobado puede servir para demostrar el cumplimiento de las obligaciones por parte de la empresa. Una vez finalizado el tratamiento por cuenta de la empresa, el encargado debe, a elección de aquella, devolver o suprimir los datos personales, salvo que la normativa obligue a conservar los datos.

(*****) *Tratamiento de categorías especiales de datos personales*:

Son los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

ÁMBITO DE APLICACIÓN Y TIPOS DE MEDIDAS

La aplicación de las medidas de seguridad que se definen en el presente documento alcanza a todos aquellos recursos que de alguna manera participan en el tratamiento de los datos personales de la empresa, y pueden incluir:

- Personas que intervienen en el tratamiento de datos tanto de forma directa como indirecta (personal de limpieza, seguridad, etc.).
- Servidores, equipos o dispositivos periféricos y extraíbles.
- Entorno de comunicaciones, sistemas de información o redes.
- Locales en los que se ubican los datos, en que se accede a la información o se almacenen soportes que los contengan.

Todas las personas que tengan acceso a los datos personales, ya sea través de una aplicación informática específicamente diseñada para acceder a los mismos, bien a través de cualquier otro medio de acceso a los ficheros (otras herramientas informáticas, internet, etc.) o bien de forma directa en el caso de documentos, se encuentran obligadas por la normativa a velar por la seguridad de los datos que se tratan y están sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Cada persona autorizada a acceder a los datos personales deberá tener conocimiento de sus obligaciones y, será requisito obligatorio para poder acceder a esos datos el haber dado fe del conocimiento de dichas obligaciones.

Todo esto debe permitir que los datos personales sean tratados de un modo que se garantice una seguridad y confidencialidad adecuadas para dichos datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo o sistema de información utilizado en el tratamiento.

DERECHOS DE LOS INTERESADOS/TITULARES DE LOS DATOS PERSONALES

La empresa debe comunicar a todas las personas que tengan acceso a los datos personales la forma de los derechos que tienen los interesados o titulares de los datos personales y, por consiguiente, la empresa debe definir claramente cómo se pueden ejercer estos derechos (por correo electrónico, correo postal, etc.), y la forma y el procedimiento en que se deben atender dichos derechos.

Los interesados que soliciten ejercer sus derechos deberán presentar su documento nacional de identidad (DNI), pasaporte o documento similar que le identifique.
La respuesta por parte de la empresa no debe demorarse sin una causa justificada.

Los derechos que se pueden ejercer son:

- Derecho de acceso: La empresa deberá facilitar al interesado confirmación de si se están tratando o no sus datos personales y, en tal caso, le deberá facilitar la siguiente información: a) los fines del tratamiento; b) los datos personales que se tienen; c) la identidad de los destinatarios de los datos; d) los plazos de conservación de los datos personales o criterios para determinar este plazo; e) la identidad de la empresa responsable para poder ejercer el derecho a solicitar la rectificación o supresión de datos personales o la limitación del tratamiento, o a oponerse a dicho tratamiento; f) información sobre el derecho a presentar una reclamación ante la AEPD; y g) cuando los datos personales no se hayan obtenido del interesado, información sobre su origen.
- Derecho de rectificación: La empresa está obligada a rectificar los datos de los interesados que fueran inexactos o incompletos que le conciernan.
- Derecho de supresión: La empresa debe eliminar los datos de los interesados si estos manifiestan su negativa u oposición al tratamiento de datos por parte de la empresa y no exista normativa legal que lo impida.
- Derecho de portabilidad: El interesado tendrá derecho a recibir los datos personales que le incumban y que nos haya facilitado, en un formato estructurado, de uso común y lectura mecánica, y tiene derecho a que se le transmitan a otro responsable del tratamiento o empresa. La empresa lo facilitará si el interesado le facilita los datos del nuevo responsable.
- Derecho a la limitación del tratamiento: El interesado tendrá derecho a obtener de la empresa la limitación del tratamiento cuando este impugne la exactitud de los datos personales (durante un plazo que permita a la empresa verificar la exactitud de los mismos), cuando la empresa ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones, y cuando el interesado se haya opuesto al tratamiento mientras se verifica si los motivos legítimos de la empresa responsable prevalecen sobre los del interesado.

OBLIGACIONES DEL PERSONAL CON ACCESO A LOS DATOS PERSONALES

La empresa deberá informar al personal con acceso a los datos personales de sus obligaciones en relación al tratamiento de datos que va a realizar.

Las personas afectadas, por lo tanto, deberán conocer estas obligaciones y sería recomendable dejar constancia del conocimiento de dichas obligaciones mediante firma del oportuno documento.
Las actuaciones de cada persona se limitan al tratamiento de datos en el equipo informático/ordenador asignado utilizando las herramientas de gestión disponibles.
No deberían, en principio, tener acceso directo a los datos, salvo el personal informático autorizado que deberá cumplir de igual forma con todas las medidas de seguridad que se detallan aquí.

Cumpliendo con el deber de confidencialidad de los datos, cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicarlo a su responsable e inmediatamente después proceder a cambiarla.

Se recomienda no compartir contraseñas ni dejarlas anotadas en un lugar de acceso común al que puedan acceder personas distintas del usuario o personas sin derecho de acceso.

Se establece que cada persona será responsable de su puesto de trabajo y garantizará que la información que muestra su dispositivo en pantalla no pueda ser visible por personas no autorizadas. El concepto de puesto de trabajo va más allá de la ubicación «física» donde el usuario desempeña sus funciones diarias. Dentro de esta definición podemos incluir elementos con relación directa con la seguridad de los datos: equipos de trabajo, smartphones (móviles), tabletas, dispositivos de almacenamiento extraíbles, impresoras, escáneres, documentación, archivadores, etc.

Será recomendable que, tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo, se encuentren físicamente ubicados en lugares que garanticen la confidencialidad de la información.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su jornada laboral, deberá dejarlo en un estado que impida la visualización de los datos personales, ya sea cerrando la sesión de trabajo o con bloqueo de la pantalla mediante un protector de pantalla que impida la visualización de los datos.

La reanudación del trabajo implicará la desactivación de la pantalla protectora mediante la introducción de la contraseña correspondiente.

Es recomendable que los empleados guarden los documentos ofimáticos de datos personales en los servidores de ficheros corporativos en lugar de en los equipos individuales.

Los empleados pueden disponer de buzones o carpetas personales dentro de la misma red corporativa. En estas carpetas se almacena información que, si bien tiene relación con su trabajo, no

necesariamente es compartida por otros miembros del equipo. Es importante que el empleado tenga conciencia de que toda esta información almacenada ocupa un espacio y que, si es carente de valor será mejor eliminarla una vez se haya utilizado para evitar que la capacidad de almacenamiento se vea desbordada innecesariamente.
Es recomendable, que la configuración de aplicaciones y sistemas operativos en los puestos de trabajo desde los que se tiene acceso al fichero sólo pueda ser cambiada bajo la autorización de la empresa o persona autorizada por ella.

El personal con acceso a los datos personales no debe comunicar estos datos ni cualquier información relacionada a terceros. Se debe tener especial precaución en no divulgar datos personales protegidos durante llamadas telefónicas, correos electrónicos, chats, etc…

En el caso de documentos físicos, cuando el responsable del puesto deba ausentarse, deberá asegurarse de que los documentos que esté utilizando se guarden en sitio seguro (armarios o salas con acceso restringido) y lejos del alcance de personas no autorizadas a acceder a ellos. Se recomienda aplicar la política de “mesas limpias”.

En el caso de las impresoras se evitará dejar documentos impresos en la bandeja de salida que contengan datos personales. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

El personal empleado debe notificar a la empresa cualquier incidente de seguridad relacionado con su puesto de trabajo, ya sea en la propia empresa o en el exterior y que pueda afectar a los datos personales.
Como ejemplo, el empleado debería notificar:

- Si ha recibido alertas de virus/malware generadas por el antivirus.
- Si ha recibido llamadas sospechosas solicitando información sensible.
- Si ha recibido correos electrónicos que contengan virus.
- Si ha extraviado dispositivos móviles (portátiles, smartphones o tabletas) o dispositivos externos de almacenamiento (USB, CD/DVD, etc.).
- Si ha borrado o alterado accidentalmente datos personales.
- Si ha encontrado información de datos personales en ubicaciones no autorizadas para ello.
- Si tiene evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (sala de servidores, despachos, almacenes,…).
- Si evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros.

Para finalizar, cabe recordar que el deber de confidencialidad persiste aunque finalice la relación laboral o contractual entre el trabajador y la empresa responsable de los datos.

MEDIDAS A ADOPTAR EN LA EMPRESA EN RELACIÓN AL ACCESO A LOS DATOS PERSONALES

La empresa responsable deberá garantizar el nivel de seguridad adecuado de los datos personales. En niveles de riesgo bajo, la empresa debe decidir las medidas adecuadas teniendo en cuenta que el nivel de complejidad siempre será inferior al que debería adoptar si la empresa tuviera un nivel de riesgo elevado.
A continuación se relacionan una serie de medidas para ayudar a la empresa en el cumplimiento de sus obligaciones y se añaden una serie de recomendaciones útiles para la empresa si se dispone de los recursos.

CONTROL DEL ACCESO A LOS DATOS PERSONALES: PERMISOS Y PERFILES

En primer lugar, la empresa debería tener claro el tipo de datos personales que se tratan (contabilidad, recursos humanos/nóminas, contabilidad, clientes/facturación, marketing, producción, etc.) y, a continuación, determinar qué personas pueden acceder a cada tipo de información.

La asignación de permisos sobre los equipos o recursos que contienen la información puede realizarse individualmente o por perfiles de usuarios.
Si se hace de manera individual se obtiene flexibilidad pero la dificultad crece mucho a medida que el número de personas o usuarios aumenta.
Si la empresa tiene la posibilidad de optar por perfiles de usuario, inicialmente se deberá hacer un esfuerzo inicial mayor para definir los perfiles pero después la gestión de permisos será más rápida y eficiente.

Es especialmente recomendable el uso de perfiles para aquellos casos en que el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y para uso personal ya que de esta forma se mantendrán separados los usos profesional y personal del ordenador.
Es altamente recomendable disponer de algún perfil con derechos de administrador para temas específicos de instalación y configuración del sistema. De esta forma en caso de ciberataque será más complicado el obtener privilegios para acceder a nuestro sistema operativo.
Los principales sistemas operativos permiten asignar y gestionar este tipo de permisos.
Una vez hemos establecido quién y cómo debe acceder a qué información y quién y cómo debe autorizar ese acceso, es importante comprobar que esto se cumple.

CONTROL DEL ACCESO A LOS DATOS PERSONALES: GESTIÓN DE CONTRASEÑAS

Se recomienda una gestión de contraseñas adecuada para evitar extravíos de las mismas o accesos no deseados.

La empresa se encargará de que los sistemas informáticos de acceso a los datos personales tengan

su acceso restringido mediante un código de usuario y una contraseña. Las contraseñas deben ser robustas y, como ejemplo, deberán tener al menos 8 caracteres, y deberá contener números, letras y, preferentemente, algún signo o carácter especial (+, /, *, etc.).

Es recomendable obligar a cambiar la contraseña de forma periódica (por ejemplo, cada seis meses). También se recomienda que en caso de que el usuario realice varios intentos de acceso fallidos (por ejemplo, cinco) se proceda a bloquear la contraseña.
Asimismo, cuando accedan varias personas a los datos, la empresa se cuidará que todos los usuarios autorizados a acceder a los datos tengan un código de usuario que será único y que estará asociado a la contraseña correspondiente que sólo conocerá el propio usuario (lo que se conoce como identificación inequívoca).
Se deberá garantizar la confidencialidad de las contraseñas, evitando que se puedan exponer a terceros.

Se recomienda establecer alguna medida de revisión periódica de permisos, para comprobar que estos sean los adecuados prestando atención a los usuarios que han sido eliminados o modificados. Una comprobación con periodicidad anual sería correcta.

Si se ha optado por crear perfiles, en la revisión se debe tener en cuenta la composición de los perfiles y las personas asociadas a cada uno de ellos.

Si existe una empresa encargada de tratamiento que presta sus servicios en los locales de la empresa, esta debe asegurarse que el personal del encargado del tratamiento cumple las mismas medidas de seguridad previstas para el personal con acceso a los datos personales. En el caso de que el tratamiento de datos se realizara en los locales del encargado del tratamiento, se deberán cumplir las mismas medidas de seguridad que el personal empleado de la empresa responsable.

Adicionalmente, la empresa adoptará las medidas adecuadas para limitar el acceso del personal a datos personales para la realización de trabajos que no vayan relacionados con el tratamiento de datos personales.

CONTROL DEL ACCESO A LOS DATOS DE FORMA REMOTA Y SEGURIDAD DE LA RED

Actualmente, en casi todas las organizaciones se dispone de una red que conecta todos los equipos de la empresa.

Es muy importante que sea segura ante cualquier circunstancia y debería estar protegida ante ataques externos. Por ello habitualmente, la conexión a la red de la empresa estará restringida por defecto.

Se deben definir responsabilidades y procedimientos de trabajo para la gestión del equipamiento de red. Si es posible, es positivo disponer de una persona con funciones de administrador de la red.

Si el servidor de datos está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso a estos datos, la empresa o el administrador de la red deberá asegurarse de que este acceso no se permita a personas no autorizadas mediante algún sistema de seguridad. Debemos asegurarnos que cualquier nuevo equipo o dispositivo que se conecte a la red corporativa esté correctamente configurado y con el software antimalware actualizado.

Se debe realizar un control del uso de dispositivos móviles y medios de almacenamiento externo como USB, discos duros portátiles, etc., ya que son una puerta habitual de entrada de malware o virus en la red y que pueden ser una importante causa de fuga de información.

Es recomendable evitar la navegación por internet a sitios no seguros para evitar la exposición a virus y otras amenazas que puedan hacer vulnerable nuestra red, poniendo especial atención a las conexiones a redes sociales y P2P.

Se deben eliminar las cuentas y contraseñas que por defecto puedan dar lugar a posibles ataques de ciberdelincuentes.

En organizaciones grandes puede ser útil realizar una segmentación de la red para impedir que un posible ataque o un malware pueda propagarse de forma indiscriminada por la red. Si se realiza, la división en dominios de red hay que definir adecuadamente las posibilidades de interconexión controlada entre ellos.

Actualmente en casi todas las empresas se dispone de redes WiFi, y habitualmente están desprotegidas o mal configuradas, lo que puede permitir el acceso a nuestros sistemas desde el exterior.

Para aumentar la seguridad de las mismas se recomienda cambiar el usuario y la contraseña de acceso a la configuración del router, pues suelen ser contraseñas por defecto que son de conocimiento público.

También aumenta la seguridad modificar y cambiar regularmente la contraseña de acceso a la red wifi que viene configurada de fábrica en el router por otra personalizada que cumpla los requisitos mínimos de seguridad.

Si ocultamos el nombre de la red wifi (SSID) de la empresa, para que esta no sea «visible» por dispositivos ajenos a la empresa dificultaremos los intentos de conexión indeseados.

Otra recomendación sería la de proteger la red wifi utilizando cifrado en las comunicaciones (activando cifrado WPA/ WPA2) y permitir acceder a la red únicamente a los dispositivos de trabajo (esto se puede hacer activando el filtrado de direcciones MAC).

Deben tenerse en cuenta también los accesos desde el exterior ya sea por correo electrónico o con sistemas de acceso remoto de usuarios a través de red virtual (VPN).

Cabe destacar el peligro que suponen las conexiones realizadas por los dispositivos móviles desde el exterior, ya que pueden acceder a sistemas y recursos internos de la empresa desde redes wifi públicas abiertas o sin las debidas garantías de seguridad, como son wifis de cortesía de restaurantes, hoteles, aeropuertos, etc. Hay que intentar evitar el uso de estas redes pero si se utilizan se deben extremar las medidas de seguridad, adoptando sistemas de cifrado de datos y comunicaciones, haciendo uso de una Red Privada Virtual o VPN (del inglés Virtual Private Network) o utilizando conexiones 3G/4G.

Si la empresa tiene recursos para ello, existe la posibilidad de implantar sistemas de registro o monitorización del tráfico de nuestra red para guardar lo que está ocurriendo, y que nos permita protegerla tanto de manera preventiva como reactiva. Si es así como ejemplos del tipo de información que se puede registrar y analizar para poder detectar de manera preventiva situaciones anómalas serían: los accesos autorizados o rechazados a la red, equipos o a las aplicaciones; los cambios en la configuración de los sistemas; el uso de privilegios especiales; y las alarmas o avisos que se puedan generar en nuestra red. Toda esta información serviría también para, en caso de sufrir un incidente de seguridad, poder analizar qué es lo que ha ocurrido y así identificar posibles fallos de seguridad.

El acceso a los logs o registros de actividad de nuestra red y nuestros sistemas debe estar controlado, para evitar que alguien los deshabilite o manipule.

Si es posible, se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos personales, en directorios protegidos y bajo el control del administrador de la red. Si se realiza esto se mantendrán copias de esos correos durante un período mínimo determinado por la empresa (por ejemplo, un año).

Cuando los datos vayan a ser enviados por correo electrónico o sistemas telemáticos a través de redes públicas o no protegidas se tienen que enviar encriptados de forma que sólo puedan ser leídos e interpretados por el destinatario.

CONTROL DE ACCESO FÍSICO A LOS DATOS PERSONALES

En los centros de trabajo y en los locales de la empresa donde se ubiquen los ordenadores o dispositivos que contengan los datos personales o que tengan acceso a los mismos y, en su caso, los documentos que contengan esos mismos datos, se debe disponer de especial protección para garantizar la disponibilidad y confidencialidad de los datos personales, especialmente si el fichero está ubicado en un servidor con acceso a través de una red.

Sería recomendable el poder contar con medidas de control de acceso a los locales de la empresa que permitan la entrada únicamente a las personas con permiso o autorización, tales como tornos de entrada, tarjetas RFID, guardias de seguridad o videovigilancia.

Se intentará evitar dar permiso de entrada a personas que no sean indispensables pero como el día a día de la empresa hace necesario que personas accesorias (limpieza, seguridad, mensajerías, comerciales, etc.) accedan a dichos locales se debería cuidado en que no puedan acceder a terminales con acceso a los datos personales.

Se deberá contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del fichero o documento que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

COPIAS DE SEGURIDAD

El dispositivo o soporte escogido para la realización de copias de seguridad depende del sistema de copia elegido, de la fiabilidad necesaria y de la inversión que se quiera realizar.

La empresa debe analizar la información que desea incluir en la copia y debe descartar aquella información que no se necesite, que ya esté guardada o que no tenga relación con lo que se quiere guardar o respaldar.

A continuación, se debe definir una política de copias de seguridad que significa definir la periodicidad y el número de copias que se van a almacenar, que va a depender de la necesidad del negocio y de la capacidad de almacenamiento.

En períodos de mucho uso se recomienda hacer una copia diaria (salvo los días que no se trabaje) y hacerla en un dispositivo diferente del que se utilice para el trabajo diario. Se guardarán las copias el tiempo que establezca la empresa (por ejemplo, durante un mes) y sería recomendable guardar la última copia del mes durante un año.

La empresa se encargará de verificar periódicamente (por ejemplo, cada seis meses) la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de seguridad y posible recuperación de los datos. Es importante hacer pruebas periódicas de restauración de datos sobre todo si no se suelen recuperar habitualmente (el proceso debe estar documentado para agilizar el proceso ante contingencias). Las pruebas de verificación se realizarán en un soporte diferente al que se utiliza para las copias de seguridad diarias.

GESTIÓN DE SOPORTES O DISPOSITIVOS DE ALMACENAMIENTO DE LA INFORMACIÓN

El primer paso en la gestión segura de la información es realizar una clasificación de la información y garantizar un almacenamiento adecuado.

Los dispositivos de almacenamiento constituyen una parte importante en cualquier sistema o instalación informática. Cada día son de más capacidad y, por tendencia de mercado, más rápidos, fiables, económicos y de menor tamaño por lo que son fácilmente transportables, reproducibles o copiables (discos duros, cd, dvd, pen drives, etc.). Es evidente, por lo tanto, la importancia que para

la seguridad de los datos tiene el control de estos medios. Por ello, es recomendable realizar un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables y la información contenida.

Se recomienda que los dispositivos que contengan los datos, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, estén claramente identificados con una etiqueta externa con la información necesaria.

La empresa deberá guardar en lugar seguro, distinto del lugar en que se encuentren los datos originales, las copias de seguridad realizadas, para así permitir la recuperación de los datos personales en caso de pérdida de la información en caso de incendio, inundación, robo o rastreo de redes.

Existen empresas de custodia que garantizan la seguridad de los soportes, aunque en caso de que se guarden en otro tipo de empresa se recomienda que los datos estén cifrados.

Es recomendable también controlar cualquier operación realizada sobre un soporte, ya sea mantenimiento, reparación o sustitución.

Si la información almacenada en las copias es confidencial (por ejemplo, facturación, planes de negocio, beneficios de la empresa, etc.), debemos valorar la opción de cifrar los datos para evitar las consecuencias de robo o extravío de soportes. Debe considerarse, como contrapartida negativa, que en caso de pérdida de las claves de acceso no se podría acceder a la información. Por ello, quizás fuera preferible que el cifrado se realice solamente sobre archivos específicos y no de forma general.

Cuando se vaya a desechar cualquier dispositivo por llegar al final de su vida útil la información debe ser eliminada mediante procedimientos de borrado seguro, adoptándose las medidas necesarias para evitar accesos indebidos a la información o su recuperación posterior. En el caso de dispositivos de almacenamiento los medios eficaces que evitan completamente la recuperación de los datos contenidos en estos son: la desmagnetización, la destrucción física (por ejemplo, con una trituradora de papel) y la sobrescritura en la totalidad del área de almacenamiento de la información.

Aquellos medios que sean reutilizables, y que hayan contenido copias de datos de los ficheros deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables. Alternativamente existe la opción de recurrir a alguna empresa especializada.

El traslado o la salida de soportes informáticos, dispositivos portátiles en definitiva dispositivos de almacenamiento que contengan datos de carácter personal, incluidos los adjuntos a correos electrónicos, a instalaciones externas a las de la empresa, ya sea para traslado o para tratar datos fuera de los locales de la empresa, deberá ser expresamente autorizada por esta y se deberá asegurar que la cadena de custodia de los mismos sea la que corresponde para evitar fuga de información.

En el transporte de dispositivos se deben adoptar medidas para evitar la sustracción, pérdida o acceso indebido a la información.

Sería recomendable mantener un libro de registro de entradas y salidas de dispositivos, soportes o documentos para un mejor control de los movimientos. Si se lleva registro, estos libros permitirán, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y la hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

La salida de dispositivos que contengan datos personales debería valorarse la posibilidad de realiza cifrado de los datos o, en su defecto, utilizando otro mecanismo que garantice que la información no sea accesible ni manipulable durante el tiempo en que estén fuera de los locales de la empresa.

Servicios de almacenamiento en la nube: Es posible utilizar servicios de almacenamiento en la nube como medio de almacenamiento externo, para compartir la información generada o para realizar copias de seguridad. Un caso particular de almacenamiento es el asociado a la contratación de servicios externos como servicios de backup o alojamiento web. Debe tenerse en cuenta al contratar servicios en la nube que se deben seguir los mismos criterios de seguridad de la empresa para la información asociada a los servicios contratados, reflejándolo en los contratos de servicio que se firmen con los proveedores.

Es recomendable que la empresa disponga de una política sobre limitación de uso de servicios de almacenamiento online. Este tipo de servicios, denominados habitualmente «cloud», son muy útiles para almacenar copias de la información corporativa, facilitar el trabajo en equipo y permitir el trabajo desde fuera de la oficina. Es recomendable que la empresa dé de alta perfiles de usuarios exclusivos corporativos para el manejo de información corporativa, que prohíba utilizar el perfil de usuario corporativo para uso privado, que se utilice algún mecanismo de cifrado antes de subir la información importante y que el uso de este tipo de servicios venga autorizado por el personal de informática o administrador de la red o sistema.

GESTIÓN DE DOCUMENTOS FÍSICOS CON INFORMACIÓN DE DATOS PERSONALES

Los dispositivos de almacenamiento de los documentos, generalmente archivadores, armarios, cajas o estructuras parecidas, que contengan datos de carácter personal, deberán estar provistos de una cerradura o algún sistema similar que dificulte la apertura de los mismos.

Si las características físicas de los dispositivos de almacenamiento no permiten dotarlo de cerradura o sistema alguno de apertura controlada, una persona autorizada por la empresa, deberá impedir el acceso de personas no autorizadas al armario, archivador o dispositivo en general.

Los armarios, archivadores, cajas u otros elementos en los que se guarden documentos con datos de carácter personal, deberán encontrarse en áreas con acceso protegido con puertas dotadas de sistemas de apertura mediante llave u otro dispositivo similar.

Si, debido a las características del local o locales de trabajo la empresa no pudiera posible cumplir lo comentado antes, se deberá mantener el dispositivo de almacenamiento de documentos en el lugar que resulte más adecuado para que la seguridad de los datos sea la máxima posible.

Mientras la documentación no se encuentre archivada por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá proceder a su custodia e impedir, en todo momento, que cualquier persona no autorizada pueda acceder a dicha documentación.

Cuando se generen copias o reproducciones de los documentos se pondrá especial cuidado en vigilar el destino de copias realizadas mediante impresiones, escaneados, etc. para que nadie sin autorización pueda acceder a esta documentación.

Tal como se ha comentado antes, deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

El acceso a la documentación estará controlado por la empresa y se limitará exclusivamente al personal autorizado.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE COPIAS DE SEGURIDAD

La seguridad de los datos personales no sólo supone mantener la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos.

En caso de fallo del sistema con pérdida total o parcial de los datos se debe evitar actuar de forma precipitada. Las acciones sobre los dispositivos que se realicen en un intento desordenado de recuperación pueden llevar a la destrucción definitiva de los datos.
Por ello, se recomienda no reiniciar constantemente el dispositivo, ya que esto puede agravar el daño que sufra en caso de que éste tenga algún fallo físico de funcionamiento.

Se debería dedicar un tiempo a analizar los datos perdidos y a analizar el coste y decidir si es mejor iniciar un proceso de restauración del sistema o volver a entrar de nuevo los datos perdidos.
Si se decide restaurar el sistema, como es lógico, se partirá de la última copia de respaldo para proceder a reconstruir los datos hasta el estado en que se encontraban en el momento del fallo.
Si se realiza, el proceso de recuperación de los datos deberá ser autorizado por la empresa y sería recomendable dejar constancia de las manipulaciones que hayan debido realizarse para dichas recuperaciones.

OTRAS MEDIDAS TÉCNICAS A ADOPTAR POR LA EMPRESA

Mantener los equipos informáticos de una empresa correctamente actualizados es una actividad compleja pero absolutamente imprescindible que requiere de varias tareas que se han de ejecutar periódicamente. Debemos tener en cuenta que estas tareas no sólo son necesarias para asegurar un correcto funcionamiento de nuestros equipos, sino que además nos facilitarán el camino a la hora de resolver incidentes de seguridad complejos.

GESTIÓN DE ACTUALIZACIONES AUTOMÁTICAS DEL SOFTWARE DE ORDENADORES, EQUIPOS Y DISPOSITIVOS

Como primer paso se recomienda disponer de un inventario de todos los equipos y dispositivos de la empresa y mantenerlo actualizado. En este inventario se podrán anotar las características técnicas de todos los equipos, sistemas operativos, versiones, licencias y aplicaciones instaladas.

Para poder llevar a cabo un mantenimiento adecuado de los niveles de seguridad de los sistemas, es necesario estar informados de la aparición de las últimas versiones de las aplicaciones que tenemos instaladas, y de las vulnerabilidades que pueden afectarles.

La gran mayoría de los ciberataques buscan y aprovechan vulnerabilidades conocidas que afectan a las aplicaciones o a los sistemas a los que pertenecen. Aprovechando esas vulnerabilidades o fallos de seguridad los ciberdelincuentes pueden llegar a tomar el control de los sistemas. Con ese objetivo

rastrean la web buscando sistemas y equipos desactualizados, para poder atacarlos utilizando vulnerabilidades conocidas.

Por ese motivo, es muy importante que la empresa procure, dentro de lo posible, de que todos los sistemas operativos y las aplicaciones dispongan de las últimas versiones y parches de seguridad.

A día de hoy, estas tareas se pueden automatizar y con una buena organización y configuración, se pude facilitar enormemente esta gestión sin un gasto de recursos excesivo. Pero, a pesar de esto, siempre debe hacerse una revisión periódica de que todo se realiza en su tiempo y funciona correctamente.

Es imprescindible, que dentro del software obligatorio en los equipos se incluya un cortafuegos o firewall para evitar accesos remotos indebidos a los datos personales.
Se debe tener un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

Es recomendable que la empresa determine cuál es el software autorizado en la empresa, y filtrar el acceso por internet a sitios web potencialmente maliciosos.

En resumen, es recomendable si queremos asegurar la correcta actualización de nuestros sistemas deberíamos:

- Mantener permanentemente vigilado el estado de actualización de todos los dispositivos y aplicaciones con los que contamos en nuestra empresa.
- Configurar los sistemas para que las actualizaciones se instalen de manera automática en un horario en el que no afecte al trabajo de los empleados.
- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores, programas antivirus y cortafuegos.
- Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

Si la empresa dispone de recursos, también es recomendable periódicamente realizar un análisis de capacidad de los servidores y dispositivos de la organización para detectar consumos excesivos de recursos que pueden identificar problemas de seguridad, rendimiento o funcionalidad.

GESTIÓN Y CONTROL DE SISTEMAS ANTIVIRUS / MALWARE

Debe aplicarse a la totalidad de los equipos y dispositivos de la empresa, incluidos los dispositivos móviles y los medios de almacenamiento externo como USB, discos duros portátiles, etc., y deben contar con las medidas necesarias para prevenir, detectar y contener cualquier tipo de amenaza a la que se vea expuesta nuestra empresa.

Es útil considerar la instalación de software dedicado especializado que utilice una combinación de técnicas proactivas (para posibles amenazas desconocidas) y reactivas (para amenazas conocidas) para la detección e interceptación de código malicioso que pueda ser potencialmente peligroso para nuestros sistemas y actividades, y que pueda prevenir o limitar el daño que nos pueda causar. Debemos asegurar y verificar que en los equipos y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá del sistema de antivirus corporativo que garantice en la medida posible el robo y destrucción de la información y datos personales.

Es habitual programar en los antivirus análisis periódicos de todos los equipos de la empresa para evitar posibles infecciones. El sistema de antivirus también se deberá programar para que se actualice de forma periódica y así asegurarnos de que la base de datos del sistema está al día.

En resumen, la implantación de un sistema antimalware debe pasar por la instalación de software dedicado y especializado que detecte y neutralice todo tipo de amenazas. Como resumen, se recomienda que cumpla las siguientes características:

- Que disponga de actualizaciones automáticas.
- Es recomendable programar y planificar análisis periódicos (aunque la mayoría de antivirus disponen de análisis en tiempo real).
- Que no sea posible desactivar el antivirus por parte del usuario final.
- Debe incluir la funcionalidad de análisis de páginas web y correo electrónico.

VIOLACIONES DE SEGURIDAD DE DATOS PERSONALES

En caso de violación de la seguridad de los datos personales, la empresa la debe notificar a la Agencia Española de Protección de Datos (AEPD) sin retraso indebido y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos del retraso.

El encargado del tratamiento notificará sin demora indebida a la empresa responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

La notificación se realizará por medios electrónicos a través de la sede electrónica de la AEPD y deberá contener la información mínima marcada por la normativa.
Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin demora indebida.
La empresa documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.