Módulo de Formación Protección de Datos Personales

Persevera, S. L.

11 de noviembre de 2016

FVCV
FEDERACIÓN DE VELA
COMUNITAT VALENCIANA

Módulo de Formación

Este módulo de Formación se realiza con la finalidad de dar cumplimiento a lo dispuesto artículo 88.3.C del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal**,** el cuál regula que en el Sistema de Protección de Datos de Carácter Personal y dentro del Documento de Seguridad se incluya un apartado que incluya las funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

Si bien, el Documento de Seguridad de la **Federación de Vela de la Comunitat Valenciana** incluye este apartado, cumpliendo con lo enunciado en el artículo citado, este módulo es un complemento adecuado para un mayor conocimiento y sensibilización respecto de la normativa de protección de datos de carácter personal por las personas relacionadas con la **Federación de Vela de la Comunitat Valenciana.**

Política de seguridad

La Federación de Vela de la Comunitat Valenciana, en adelante, la Organización, consciente de la importancia y de la necesidad de garantizar la seguridad de los sistemas de información con datos personales, ha decidido llevar a cabo la implantación en la Organización de un Sistema de Protección de Datos de Carácter Personal, que sea eficaz y adecuado, con el fin de garantizar los requisitos exigidos por la legislación vigente en materia de Protección de Datos de Carácter Personal (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

Para ello, se promueve el concepto de Seguridad de la Información estableciéndose objetivos y responsabilidades para garantizar la seguridad, integridad y calidad de los procedimientos, tratamientos, manipulación, comunicaciones, consultas, interconexiones o transferencias de datos de carácter personal.

Es objetivo de esta Organización concienciar y formar a todos los miembros de la organización acerca de la necesidad de garantizar la protección de datos personales, y de convertir esta necesidad en una tarea colectiva, en la cual deben implicarse todas las personas de la organización.

Las directrices generales que se establecen son las siguientes:

Implantar en la Organización una Norma de Seguridad, anexa al Documento de Seguridad.

Establecer unos procedimientos sistemáticos que aseguren la exactitud y calidad de los Datos de Carácter Personal.

Asignar los Responsables que velen por el cumplimiento de la Norma.

Garantizar a los titulares de los datos de carácter personal el derecho a ejercitar sus derechos de acceso, rectificación, cancelación y oposición, de forma acorde con los requisitos y especificaciones establecidas en la normativa y legislación vigente aplicable.

Informar a todo el personal sobre la existencia de la Norma de Seguridad.

Formar a todo el personal que accede a los datos en las directrices y procedimientos reflejados en la Norma de Seguridad.

Velar por el cumplimiento de la legislación vigente y de la Norma de Seguridad.

La siguiente Norma de Seguridad interna se ha elaborado trabajando en el sistema para prevenir los fallos, y si aún así se dieran para implantar correcciones y medidas de mejora. La eficacia y aplicación de la misma es responsabilidad directa de toda la Organización.

El Sistema de Protección de Datos Personales incorpora uno o varios Administradores del Sistema. Si el Sistema incorpora ficheros de nivel de seguridad Medio y/o Alto, junto con los Administradores del Sistema habrá uno o varios Responsables de Seguridad. En estas personas recae la responsabilidad de supervisar la implantación; desarrollo, seguimiento y mantenimiento de la misma, evaluando su adecuación y correcta aplicación. Tanto unos o como los otros poseen la suficiente autoridad para intervenir en la Organización, en la medida que se estime conveniente, y para desempeñar un papel activo en la implantación de la Norma de Seguridad, identificando problemas, verificando su eficacia y coordinando las actividades que puedan verse afectadas.

Toda persona de la Organización cuya actividad pueda directa o indirectamente verse afectada por los requisitos descritos en esta Política de Seguridad, está obligada al cumplimiento estricto de la misma.

La Organización se compromete a desarrollar las directrices de la Norma de Seguridad, así como a la revisión periódica del contenido de la Política de Seguridad, para garantizar su adecuación a las necesidades de la organización y de la legislación vigente.

Para asegurar que todo el personal conoce, comprende y aplica esta Política de Seguridad, se hace entrega de la misma a todas las personas relacionadas con la organización. También estará a su disposición a través de los medios que se comunicarán.

Norma de seguridad

Esta Norma de Seguridad[1] será de obligado cumplimiento por parte de todas aquellas personas que presten servicio en la Organización, y que por razón de las funciones o tareas que tengan asignadas, precisen acceder a datos o recursos del Sistema de Información de la Organización, constituyendo su trasgresión una falta susceptible de ser sancionada.

Obligación de secreto

- Quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con la organización

- Si un usuario/a recibe visitas en su puesto de trabajo cuidará especialmente de que la información tratada, tanto en pantalla como impresa quede fuera del alcance visual del visitante.

- La forma de proceder ante cualquier solicitud para comunicar o ceder datos de carácter personal concernientes a cualquier persona será únicamente la establecida en el procedimiento para dar respuesta al ejercicio de los derechos de acceso, rectificación y/o cancelación de los datos de carácter personal.

Control de acceso a datos

- Los usuarios/as tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desempeño de sus funciones.

- Siempre que un usuario/a abandone su puesto, incluso siendo por breve espacio de tiempo, deberá cancelar su identificación-autenticación (su sesión), procediendo a bloquear su equipo, de forma que para volver a utilizar el mismo haya que identificarse y autenticarse.

- Cada usuario/a 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 inmediatamente al responsable de seguridad o al responsable del departamento correspondiente o al responsable de sistemas.

Uso de los recursos

- Los ordenadores, Smartphones, tabletas y/u otros recursos únicamente podrán ser utilizados por personal debidamente autorizado para acceder a datos o recursos.

- Se prohíbe terminantemente el uso de cualquier recurso no autorizado, así como la incorporación a los ordenadores de información, datos o programas ajenos a la actividad propia de la organización. Queda, así mismo prohibida, salvo que medie autorización expresa del Responsable de Seguridad, la incorporación y/o ejecución de cualquier dato y/o programa proveniente de Internet o correo electrónico.

- En los equipos de la organización, solo se utilizarán aquellos programas y dispositivos de la organización, y/o los contratados a tal efecto.

- Si el usuario/a tuviera indicios de que su ordenador pudiera estar infectado, deberá:

[1] **Queda terminantemente prohibido comunicar los extremos de esta Norma de Seguridad a personal ajeno a la Organización.**

- Avisar al responsable de sistemas de la organización.
- Asegurarse de que la información contenida en el ordenador no es transferida a ningún soporte físico ni a ningún otro dispositivo conectado a ese ordenador.

- Una vez finalizado su trabajo, el usuario/a procederá a apagar sus equipos y todos sus periféricos, salvo que sea necesario mantenerlos encendidos por razones operativas, en cuyo caso deberá cerrar su sesión.

- Los usuarios/as con acceso autorizado a Internet, utilizarán dicho acceso únicamente para el desarrollo de las tareas y funciones que les correspondan por razón de sus respectivos puestos de trabajo.

- Los usuarios/as autorizados para el uso del correo electrónico, se servirán del mismo únicamente para el desarrollo de las tareas y funciones que se les hayan asignado por razón de sus respectivos puestos de trabajo.

- Al utilizar impresoras u otros recursos para la impresión, el usuario/a deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios/as no autorizados para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

- En los equipos de copia, el usuario/a deberá asegurarse que no quedan hojas con datos personales fuera de su control.

Soportes

- A la hora de utilizar soportes para el almacenamiento o transporte de datos de carácter personal, habrá de remitirse a las instrucciones del Administrador del Sistema o del Responsable de Seguridad que observarán el procedimiento definido en el Documento de Seguridad para la gestión y el etiquetado de soportes.

- No está permitida la extracción de soportes (CDs, DVDs, USBs, diskettes, discos duros, equipos fijos/portátiles y cualesquiera otros dispositivos) de los centros de trabajo sin la autorización del Responsable de Seguridad.

Incidencias

- Cualquier incidencia concerniente a los datos de carácter personal, deberá ser puesta inmediatamente en conocimiento del responsable de seguridad, que será el encargado de la puesta en marcha del procedimiento definido en el Documento de Seguridad para la para la gestión de las mismas.

Envíos de correos electrónicos a varios destinatarios

- Los destinatarios adicionales deben añadirse mediante copia oculta, para no poner en conocimiento de terceros su dirección de correo electrónico.

Reenvíos de correos electrónicos

- Debe eliminarse del cuerpo del mensaje aquellas partes del texto procedentes de anteriores reenvíos si en dicho texto se pueden identificar direcciones de correo electrónico.

Comunicaciones a interesados

- Deben realizarse identificando al destinatario de forma inequívoca (nombre completo) no de forma genérica.

Atención de comunicaciones telefónicas/electrónicas

- Se debe permanecer alerta ante técnicas de ingeniería social. No se debe comunicar dato alguno a un destinatario si no se está seguro de que es quien dice ser y procede esa comunicación.

Recomendaciones para tratamientos de datos personales en papel

Impresión de datos personales

Deben ubicarse las impresoras y faxes en ubicaciones alejadas del acceso del público, imposibilitando que personal ajeno a la Organización pueda apropiarse de documentos con datos personales. Como opción, se recomienda la impresión bloqueada (el documento sólo puede ser recogido por el usuario/a que lo envío a la cola de impresión) en aquellos dispositivos de impresión que tengan esta funcionalidad.

Reciclado y destrucción de papel

Los documentos con datos personales que se destinen al reciclado o destrucción, deben previamente haberse procesado con una destructora de papel de tiras o partículas.

En el caso de datos especialmente protegidos, enumerados en el artículo 7 de la L.O. 15/1999 (salud, vida sexual, ideología, afiliación sindical, origen racial o étnico, creencias religiosas, comisión de infracciones penales y/o administrativas) se recomienda la utilización destructoras de papel con capacidad para generar partículas y no tiras.

Duplicados

Los documentos con datos personales especialmente protegidos no se podrán duplicar por medios tecnológicos cualesquiera sin la autorización expresa del responsable del departamento asociado al tratamiento. En cualquier caso, se aplicarán las mismas medidas de seguridad que a los documentos originales.

Archivos y almacenes

Los armarios, archivadores u otros elementos utilizados para almacenar datos personales en papel deben situarse en ubicaciones alejadas del acceso del público, imposibilitando que personal ajeno a la Organización pueda apropiarse de documentos con datos personales.

Los archivadores o armarios deben ubicarse en áreas protegidas por puertas de acceso con sistema de apertura por llave o equivalente. Dichas áreas deben permanecer cerradas fuera del horario de trabajo, siendo tan sólo accesibles por personal de seguridad y limpieza para el desempeño de sus tareas.

En el caso de los datos especialmente protegidos, los archivadores o armarios protegerse con sistemas de apertura por llave o equivalente. Dichos archivadores deben permanecer cerrados fuera del horario de trabajo y no pueden ser accesibles por el personal de seguridad y limpieza.

Puesto de trabajo

No deben dejarse en el puesto de trabajo (mesa o equivalente) ningún documento con datos personales al alcance de personal no autorizado, debiendo retornarse al finalizar la jornada laboral y ante cualquier ausencia del puesto, los documentos a los almacenes originales o a los cajones cerrados con llave del puesto de trabajo.

Correo interno en cajetines

No se permitirán cajetines de correo interno en lugares comunes cuando en dichos cajetines puedan depositarse documentos con datos personales. En caso de que en el correo interno puedan existir documentos con datos personales, dichos documentos deben entregarse directamente al destinatario o bien almacenarse en un repositorio controlado, al que se acceda por medio de identificación.

Entradas y salidas de documentos

Se registrarán las entradas y salidas de documentación en el caso de datos especialmente protegidos, datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, solvencia patrimonial o crédito y cualesquiera datos que permitan evaluar la personalidad del individuo.

Acceso a datos especialmente protegidos

En el caso de acceso a datos especialmente protegidos por personal de otro departamento distinto del asociado al tratamiento, debe verificarse la autorización de la persona para acceder a dichos datos además de consignarse los datos accedidos, fecha del acceso, destinatario y fecha de devolución.

Transporte de documentos fuera de los centros de trabajo

Se pondrá la máxima atención y diligencia para evitar que los documentos con datos personales transportados puedan ser accedidos por terceros no autorizados. En el caso de tratarse de datos especialmente protegidos, deben transportarse en un maletín o equivalente protegido por un sistema de apertura (llave, combinación numérica, sistemas biométricos) sólo accesible al portador.

Ante cualquier duda a la hora de aplicar estas normas, por favor, diríjanse al Responsable de Seguridad.

Derechos ARCO

La L.O. 15/1999 de Protección de Datos de Carácter Personal (LOPD) recoge una serie de derechos personalísimos, que tienen como fin permitir, en todo momento, el conocimiento y control de los datos personales por parte del titular de los mismos, pudiendo conocer en todo momento cuales de sus datos son tratados y por quien, el motivo de dicho tratamiento, así como la capacidad de rectificarlos, cancelarlos u oponerse a dichos tratamientos.

Derecho de acceso

Derecho a solicitar y obtener información sobre:

- Datos de carácter personal sometidos a tratamiento.
- Origen de dichos datos.
- Comunicaciones realizadas o que se tenga previsto realizar con dichos datos.

Derecho de rectificación

Derecho a que se modifiquen los datos que resulten ser incorrectos o incompletos.

Derecho de cancelación

Derecho al bloqueo o supresión de aquellos datos que resulten inadecuados, excesivos o no pertinentes para la finalidad del tratamiento.

Derecho de oposición

Derecho a que no se lleve a cabo el tratamiento de los datos, o a que se cese en el mismo.

ASPECTOS COMUNES

Los citados derechos podrán ejercerse:

Por el titular de los datos

Acreditando su identidad mediante un medio válido en Derecho (DNI, Pasaporte, Firma Electrónica, …)

Por representante legal

En supuestos de minoría de edad/incapacidad que impidan ejercerlos por su titular. Deberá acreditarse la condición de representante legal, así como la identidad, tanto del representado como del representante.

Representante voluntario

El cual debe estar expresamente designado, debiendo acreditarse tanto la representación como la identidad de representante y representado.

REQUISITOS SOLICITUDES

Deberán contener, obligatoriamente:

- Nombre y apellidos
- Petición
- Dirección a efectos de notificaciones
- Fecha
- Firma

A ellos habrá que añadir:

- Copia de los documentos acreditativos de la identidad.
- Copia de los documentos acreditativos de la representación, en su caso.
- Otros documentos que considere relevantes el peticionario.

CANALES

Cualquier trabajador/a ante quien se presente solicitud o formule petición de ejercicio de alguno de los derechos citados anteriormente, está obligado a:

- Informar al peticionario/a de los requisitos que deben cumplir las solicitudes.
- Recepcionar cualquier solicitud formal[2].
- Trasladar[3] dicha solicitud en un plazo máximo de tres días naturales al Responsable de Seguridad de la organización.

[2] Aunque no cumpla los requisitos.
[3] El trabajador/a no puede contestar directamente a la solicitud a menos que formalmente la organización le haya designado para ello.