LIWE ITALY SRL CIRCULAR INFORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL CON ACCESO INFORMÁTICO.

Mediante este documento se describen las principales medidas de seguridad a adoptar por los usuarios para el cumplimiento de la política de protección de datos personales implantada en LIWE ITALY SRL

Estas normas obligan a cualquier persona que maneje datos personales en las instalaciones de esta entidad, o que se encuentren bajo la responsabilidad de ésta.

Para una aclaración mayor sobre el contenido, la normativa aplicable es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) , y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la citada Ley.

La normativa de protección de datos implantada en LIWE ITALY SRL se encuentra recogida en el MANUAL DE SEGURIDAD, de obligado cumplimiento para todos los usuarios, que se encuentra disponible para su consulta, previa solicitud al Responsable de Seguridad.

A continuación se presenta un esquema de los aspectos más relevantes del Manual de Seguridad:

CONFIDENCIALIDAD

- ✓ Los datos de carácter personal custodiados en LIWE ITALY SRL , ya estén contenidos en el Sistema de Información o custodiados en sus archivos, son propiedad de la organización y todas las tareas derivadas de su tratamiento resultan confidenciales.
- ✓ Los usuarios sólo pueden acceder a los datos necesarios para el desempeño de su actividad dentro de la organización y respetarán la confidencialidad de esos datos.
- ✓ Los usuarios están obligados legalmente a guardar secreto profesional respecto a los datos tratados, y al deber de guardarlos, es decir, evitar el acceso a dichos datos por personal no autorizado.
- ✓ La obligación de mantener la confidencialidad subsistirá aún en el caso de finalizar la relación profesional del usuario con la organización.
- ✓ Se prohíbe expresamente copiar información con datos de carácter personal al ordenador personal o portátil y en cualquier tipo de soporte informático sin autorización expresa del Responsable del Tratamiento.
- ✓ Se prohíbe, así mismo la copia o reproducción de documentos escritos.

CORREO ELECTRÓNICO

- ✓ No abrir ni ejecutar ficheros que se reciban por correo electrónico, especialmente si es de un remitente desconocido, salvo que se tenga la total certeza de su inocuidad, y siempre después de revisarlo con el programa antivirus.

- ✓ El correo electrónico se considera herramienta de trabajo, y como tal podrá ser revisado en caso de incidencia, y desviado en caso de ausencia o baja del trabajador, sin necesidad de previo aviso.
    - Los controles por incidencias técnicas podrán realizarse sin preaviso del trabajador.
    - Los controles preventivos se realizarán con presencia del trabajador si fuera posible. Si se realizan sin presencia del mismo se realizará un preaviso del alcance de dicho control.
    - En casos de ausencia o baja de un trabajador el correo electrónico será desviado al jefe del departamento o a otro empleado del mismo designado por aquel, con la finalidad de no dejar desatendidas las tareas realizadas.
- ✓ El correo electrónico no puede ser empleado para la transmisión de datos protegidos ni para fines diferentes a los establecidos para el correcto desarrollo de sus funciones laborales, sin la autorización del responsable del Tratamiento.
- ✓ La salida de documentos adjuntos a los correos electrónicos que contengan datos de carácter personal deberá estar previamente autorizada.
- ✓ El envío de e-mail a varios destinatarios desde las cuentas de correo electrónicos asignadas por LIWE ITALY SRL se realizarán **siempre** introduciendo los destinatarios en el campo CCO (Copia Oculta o BCC)
- ✓ Únicamente se podrán remitir correos electrónicos a aquellas personas o empresas que hayan prestado su consentimiento para la recepción de información de LIWE ITALY SRL, así como el envío de información a los clientes, relativa a los productos o servicios contratados.
- ✓ Se prohíbe la utilización del correo electrónico corporativo para usos personales o particulares. No se reenviarán mensajes ni documentos corporativos a cuentas privadas del trabajador o de sus familiares o amigos, ya que éstas no gozan del mismo nivel de seguridad. Tampoco se puede configurar la cuenta de correo corporativo para reenviar los mensajes recibidos a una cuenta de correo electrónico privado.

INTERNET

- ✓ El uso de Internet en horario laboral, debe ser exclusivo para fines relacionados con el mismo.
- ✓ En ningún momento se utilizara la conexión a Internet para la descarga de archivos multimedia (música, videos, etc.).
- ✓ No se permite la instalación de programas no autorizados o complementos del navegador de Internet.

PUESTOS DE TRABAJO

- ✓ Los puestos de trabajo están bajo la responsabilidad de algún usuario autorizado que garantice que la información que muestran no pueda ser visible por personas no autorizadas.

- ✓ Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deben estar físicamente ubicados en lugares que garanticen esa confidencialidad.
- ✓ Cuanto el responsable de un puesto de trabajo lo deje sin atención, bien temporalmente o bien al finalizar su turno de trabajo, debe dejarlo en un estado que impida la visualización de los datos protegidos. Esto se puede realizar a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo tiene que implicar la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente. En lo que respecta a la documentación, esta no deberá dejarse expuesta.
- ✓ En el caso de las impresoras debe asegurarse de que no queden documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Tratamiento, los responsables de cada puesto deben retirar los documentos conforme van siendo impresos.
- ✓ Los puestos de trabajo tienen una configuración fija en sus aplicaciones y sistemas operativos, que sólo puede ser cambiada bajo la autorización del responsable de seguridad o por el administrador del sistema.
- ✓ No está permitido a los usuarios la instalación de ningún programa o aplicación. Las aplicaciones necesarias serán instaladas exclusivamente por el personal del Departamento de Informática.
- ✓ Se prohíbe el uso de aplicaciones no relacionadas con la actividad de la organización, por entenderse que pueden comprometer la seguridad de los equipos y permitir de forma no controlada el acceso a datos protegidos.
- ✓ Los ficheros temporales que los usuarios mantengan en sus ordenadores personales deberán ser borrados, una vez haya concluido la finalidad para la que fueron creados (fichero temporal: ficheros de trabajo creados por los usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento)
- ✓ Se prohíbe la creación de nuevos ficheros que supongan el tratamiento de datos personales así como la cesión de los mismos sin previa autorización del Responsable del tratamiento.
- ✓ Se prohíbe utilizar los recursos del sistema de información a los que tenga acceso para uso privado o para cualquier otra finalidad diferente de las estrictamente laborales.
- ✓ Los puestos asignados a cada usuario se consideran herramientas de trabajo, y pueden ser revisados y accedidos desde dirección en el caso de ser necesario. El acceso al puesto de trabajo no requerirá preaviso previo.

CONTRASEÑAS

- ✓ Los usuarios son responsables de la confidencialidad de sus contraseñas. En el caso de que una contraseña sea conocida por una persona no autorizada, se hace constar como incidencia en Registro habilitado para tal fin.
- ✓ La contraseña de acceso caducará al año, debiendo ser modificada en el momento de realizar el primer acceso al sistema.
- ✓ No se accederá al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.

GESTIÓN DE INCIDENCIAS

- ✓ Incidencia es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, ya estén almacenados de manera automatizada o no (incluye también los datos almacenados en "formato papel").
- ✓ Cualquier usuario, si tiene conocimiento de una incidencia, es responsable de la comunicación de la misma al administrador del sistema, o en su caso del registro de la misma en el sistema de registro de incidencias del Tratamiento.
- ✓ El conocimiento y la no-notificación de una incidencia por parte de un usuario son considerados como una falta contra la seguridad por parte de ese usuario.
- ✓ Para la notificación de incidencias el usuario deberá ponerse en contacto con el responsable de seguridad o persona designada al efecto.

GESTIÓN DE SOPORTES

- ✓ Sólo las personas autorizadas pueden manejar soportes. Dicha autorización podrá ser indefinida o temporal.
- ✓ Cualquier soporte recibido deberá ser comunicado al responsable de seguridad, para su registro y gestión, e inventario si procede.
- ✓ Cuando se deseche cualquier documento o soporte deberán adoptarse las medidas de destrucción o borrado para evitar el acceso posterior a la información. Para ello deberá ponerse en contacto con el Responsable de Seguridad.
- ✓ La salida de soportes y ordenadores portátiles fuera de la entidad requiere autorización. Para solicitarla hay que ponerse en contacto con el Responsable de Seguridad.
- ✓ Los soportes con datos de nivel alto deberán distribuirse cifrando los datos contenidos en ellos.
- ✓ Queda terminantemente prohibido facilitar, a persona alguna ajena a la entidad, ningún soporte conteniendo datos a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.

GESTIÓN DE DOCUMENTACIÓN

- ✓ Los documentos deben almacenarse en áreas donde el acceso esté restringido, protegido con puertas de acceso y llave.
- ✓ Se adoptarán las medidas necesarias para evitar la sustracción, pérdida o acceso indebido durante su transporte (si la documentación es confidencial: traslado en sobres opacos y cerrados)
- ✓ La documentación en proceso de revisión, o tramitación, ya sea previo o posterior al archivo, debe ser custodiada por la persona que se encuentra al cargo de la misma, quien tendrá la responsabilidad de la confidencialidad de la misma, impidiendo el acceso de personas no autorizadas.
- ✓ La salida de documentos deberá estar previamente autorizada (incluidos los documentos anejos a un correo electrónico).
- ✓ Existe un registro de entrada y salida de soportes y documentación.

- ✓ Las copias y reproducciones de documentación, así como cualquier papel que contenga datos personales, deberá ser desechado de forma que se evite el acceso a la información y su recuperación posterior.

ACCESOS:

- ✓ El acceso a las áreas privadas de LIWE ITALY SRL deberá efectuarse siempre acompañado de un usuario autorizado.
- ✓ Cada usuario dispondrá de un perfil que le autoriza para determinados accesos a los datos, ya sea automatizadamente o en formato papel.

RESPONSABILIDADES:

- ✓ El usuario será responsable frente a LIWE ITALY SRL y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a la entidad las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

EJERCICIO DE DERECHOS:

Cualquier usuario de datos personales de LIWE ITALY SRL tiene la obligación legal de poder informar a los interesados sobre el ejercicio de los derechos que les corresponden.

El interesado tiene los siguientes derechos, respecto de los datos personales registrados en la entidad:

- ✓ Derecho de acceso: a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
- ✓ Derecho de rectificación: derecho del afectado a que se rectifiquen los datos que resulten inexactos o incompletos.
- ✓ Derecho de cancelación: el interesado podrá solicitar cancelación de aquellos datos cuyo tratamiento no se ajuste a lo dispuesto en la ley, o sean inexactos o incompletos, así como por la previa revocación del consentimiento.
- ✓ Derecho a oposición: si el interesado se opone al tratamiento de sus datos, en aquellos casos en los que no sea necesario su consentimiento para el tratamiento de estos, y siempre que una ley no disponga lo contrario.

Si cualquiera solicita ante el personal de LIWE ITALY SRL el ejercicio de estos derechos, aunque no sea con estas palabras, e incluso aunque sepamos que la empresa no tiene registrados ni trata datos suyos, se le deberá proporcionar un impreso de ejercicio de derechos, y notificarle que debe entregarlo en mano o enviarlo por carta a la dirección de la empresa, junto con la documentación necesaria.

La persona autorizada para gestionar los ejercicios de derechos es Luís Miguel Aroca, por lo que se le deberán comunicar todas las solicitudes de ejercicios de derecho, independientemente del canal de comunicación a través del que se reciban (En mano, por carta, e-mail, fax, etc.)