Política de Seguridad en la Información

El cumplimiento del Reglamento General de Protección de Datos 2016/679, implica que todo el personal con acceso a datos personales conozca las normas de seguridad que afecten al desarrollo de sus funciones.

En este documento, se recogen las principales funciones y obligaciones en materia de seguridad sobre los datos personales que debe acatar cualquier usuario que acceda a los mismos.

Obligaciones comunes que afectan al personal

1. Confidencialidad	Todo el personal está obligado al **secreto profesional**, inclusive finalizada la relación laboral. La **confidencialidad** es extensible a los datos personales, documentación, procedimientos técnicos, especificaciones, parámetros, procesos, programas, datos o información técnica, comercial o financiera que tenga este carácter.
2. Acceso a datos personales	Solamente se podrá **acceder a los datos de carácter personal** a los que se esté autorizado y, exclusivamente para el **desarrollo de sus funciones laborales**, quedando expresamente prohibido su uso para **fines privados.**
3. Medidas de seguridad	Todo usuario está obligado a **adoptar las medidas de seguridad** que la empresa le indique.
4. Cesión de datos	**Está absolutamente prohibida la comunicación de datos personales a terceros no autorizados**, externos o internos a la entidad, excepto en los casos legalmente previstos, y en aquellos supuestos que sea necesario para el desarrollo de la actividad laboral.
5. Uso de periféricos	En el uso de **impresoras, fotocopiadoras, escáner y fax**, se deberá tener la precaución de que en la **bandeja de salida no quede ningún documento** que contenga datos personales. La documentación de las bandejas de salida que no le pertenezca, es **confidencial**.
6. Puestos de trabajo	Los **usuarios son responsables de su puesto de trabajo** y, deberán garantizar, en la medida de lo posible, que ninguna otra persona no autorizada pueda ver la información sobre datos personales que muestran sus equipos informáticos o documentación en soporte papel.
7. Derechos de los ciudadanos	Todo el personal está obligado a **atender los derechos solicitados por terceros (acceso, rectificación, cancelación, oposición, limitación y portabilidad)** y, a ponerlo en conocimiento de su responsable inmediatamente.
8. Incidencias de seguridad	Cualquier **incidencia** que afecte a la **seguridad de los datos** deberá ser **comunicada a su responsable**. Su conocimiento y no comunicación puede ser considerada como una falta contra la seguridad de los datos personales por parte del usuario.
9. Dudas seguridad	**Cualquier duda** con relación a la confidencialidad y seguridad en el tratamiento de datos personales se debe poner en **conocimiento de sus responsables**.

Funciones y Obligaciones del personal con acceso informático

10.Contraseñas	Todos los usuarios de los sistemas informáticos deberán **cumplir con la política de identificación (nombres de usuario y contraseñas)**, indicada por su organización. En caso de elección libre de la contraseña por parte del usuario, queda absolutamente **prohibida la utilización de contraseñas fácilmente identificables**.
11.Confidencialidad contraseñas	Cada **usuario es responsable de la confidencialidad** y salvaguarda de su propia **contraseña**, que no podrá ser comunicada a terceros ajenos o no a la entidad, salvo autorización expresa de la empresa.
12.Uso sistemas informáticos	Está prohibido el **uso de los sistemas informáticos para fines privados**, salvo autorización de sus responsables.
13.Sistemas informáticos	Los terminales y sistemas informáticos solo podrán ser modificados o manipulados por el personal expresamente autorizado. Está prohibido instalar programas informáticos sin la autorización previa de la empresa.
14.Almacenamiento de información	Los usuarios deberán guardar la información y documentos generados en el servidor de la empresa y, salvo autorización expresa o que no se disponga de servidores, **no se podrán utilizar los discos duros locales de los ordenadores** para el tratamiento de datos personales.
15.Puesto de trabajo	Cuando se **abandone el puesto de trabajo**, ya sea temporalmente o por terminar su jornada laboral, **deberá apagar o bloquear su ordenador.**
16.Uso de soportes informáticos	Salvo autorización expresa, está prohibido **la realización de copias de datos personales**, en cualquier tipo de soporte informático (DVD, cintas, Pen Drives, discos duros externos, u otros).
17.Uso de dispositivos portátiles	El **uso externo de ordenadores portátiles, Smartphones**, **tabletas** o similares que contengan datos personales titularidad de su empresa, **requerirá la autorización de sus responsables**.
18.Accesos remotos o teletrabajo	Todas las **medidas** descritas serán **igualmente aplicables** cuando el acceso se produzca en la modalidad de **acceso remoto**, fuera del centro de trabajo
19.Almacenamiento en la nube (Cloud)	Está **prohibido la utilización** se sistemas de almacenamiento en la **nube** (Dropbox, Google Drive…), **plataformas de envíos de correos electrónicos (Mailchimp…)**, cuentas de correo electrónico **no corporativas** (Gmail, Hotmail...) o el uso de cualquier **software** que **no** se aloje en el s**ervidor u ordenador de la empresa**, sin disponer previamente de la autorización expresa y por escrito de la empresa.

Funciones y Obligaciones del personal por medio de soporte papel

20.Custodia y archivo	La **documentación debe ser custodiada y archivada** de manera que no sea accesible por personas no autorizadas, tanto externas como de la propia organización, y procurando no dejar documentación encima de las mesas, sobre todo cuando el trabajador se encuentre ausente de su lugar de trabajo.
21.Destrucción de documentación	**No está permitido tirar documentos y papeles** que contengan datos personales sin adoptar las medidas necesarias que **impidan su posterior visualización**, inclusive en las cajas de reciclaje que pueda habilitar la empresa.
22.Reutilización de documentación	**No se podrá reutilizar la documentación** que contenga datos personales.
23.Salida de documentación	Queda totalmente **prohibido extraer documentación** que contenga datos personales de las instalaciones de la entidad **sin la debida autorización**.

Obligaciones que afectan al uso de los sistemas informáticos, correo electrónico e Internet

24. Uso de Sistemas informáticos	Los **sistemas informáticos** son puestos a disposición del usuario para el **desarrollo de sus obligaciones laborales exclusivamente**, y deben ser utilizados de **forma adecuada.**
25. Uso del correo electrónico	El **uso del correo electrónico es estrictamente profesional**, no permitiéndose ningún uso personal de los recursos técnicos e informáticos facilitados por la entidad, excepto en aquellos casos en los que se cuente con el consentimiento expreso del responsable encargado de la seguridad de la información.
26. Normas de uso del correo electrónico	El **uso del correo electrónico** se debe realizar tomando las **debidas precauciones** que impidan el envío a destinatarios erróneos, no abriendo enlaces de cuyo origen no estemos seguros y utilizando los sistemas de copia oculta (CCO) cuando se envíe el correo a varios destinatarios no relacionados entre sí. Está **prohibido** almacenar o **guardar correos electrónicos privados** o de contenido personal en los gestores de correo de la entidad.
27. Acceso a Internet	El **acceso a Internet** mediante el uso de los equipos informáticos facilitados se **limitará a** temas estrictamente laborales. En concreto, el acceso a Internet queda prohibido, salvo autorización expresa del responsable de la entidad para acceso a Chats, páginas de intercambio de datos (música, juegos, etc.), redes sociales (Facebook, Twitter, etc.) y descargarse programas sin consentimiento.
28. Controles de la empresa	El **correo electrónico e Internet pueden ser controlados por la empresa**, de manera que se informa que los correos electrónicos podrán ser consultados por el responsable con fines profesionales (vacaciones, bajas, suplencias de los trabajadores, finalización de contrato laboral, …) y al objeto de controlar el buen uso de los recursos proporcionados, la comisión de actos ilícitos, así como el control técnico en el envío de correos electrónicos a través de la red de la entidad de determinado volumen.

El **incumplimiento de cualquiera de las obligaciones** que afectan a los usuarios comportará las **consecuencias jurídicas y laborales** que pudieran derivarse frente a su empresa, así como cualquier tercero afectado como consecuencia del incumplimiento.