IV.- Protocolo de uso de equipos y medios informáticos y digitales[1]

PROTOCOLO DE USO DE EQUIPOS Y MEDIOS INFORMÁTICOS Y DIGITALES

La utilización de los equipos y de los medios informáticos y digitales que la empresa pone a disposición de los trabajadores se regirá por las normas que se detallan en el siguiente protocolo:

I.- Uso de los equipos y medios informáticos de la empresa (incluida la dirección de correo electrónico)

1.1.- Los equipos y medios informáticos que la empresa pone a disposición de sustrabajadores son para **uso estrictamente profesional.**

Se autoriza, de forma puntual, el uso personal no reservado de dichos equipos y medios, siempre y cuando no interfiera en el trabajo y sea respetuoso con la legislación vigente y las normas establecidas por la empresa.

1.2.- La empresa podrá verificar en cualquier momento el cumplimiento de dicha obligación, siempre de acuerdo con lo que establezca la normativa vigente en cada momento.

1.3.- No está permitido conectarse o acceder a ordenadores con contraseñas que no sean la propia. Los equipos y medios informáticos que la empresa pone a disposición de sus trabajadores son cedidos a las personas asignadas y se prohíbe sin autorización de la empresa, cederlos a otra persona.

II.- Bajada de archivos y acceso a páginas web

2.1.- Está totalmente prohibida la descarga de cualquier archivo o fichero informático en los equipos de la empresa, excepto cuando se trate de archivos o ficheros procedentes de una fuente conocida y que guarden estricta relación con cuestiones profesionales.

[1] Versión 01 – Abril de 2017

2.2.- En caso de que un usuario necesite descargar un archivo procedente de una fuente desconocida, así como en todos aquellos casos en que un usuario necesite instalar un programa en el sistema o en su ordenador, deberá solicitarlo al responsable de informática de la empresa que, previas las verificaciones que tenga por convenientes, descargará e instalará el programa o bien autorizará al usuario para que lo haga directamente.

2.3.- En particular, quedan expresamente prohibidas las descargas:

a) De programas o archivos sin contar con la preceptiva autorización o licencia de su titular.

b) De material pornográfico de cualquier tipo, así como de pornografía infantil en particular.

2.4.- Está totalmente prohibido el acceso a páginas web que no sean necesarias para el desarrollo de la tarea profesional del trabajador.

Se prohíbe expresamente el acceso a los siguientes tipos de páginas web:

a) Páginas web de pornografía en general, así como de pornografía infantil en particular.

b) Páginas web que inciten al odio, a la violencia o a la discriminación por razón de raza, origen étnico o nacional, edad, religión, afiliación o no afiliación política o sindical, género, estado civil, orientación sexual o cualquier otra característica o circunstancia personal.

III.- Datos

3.1.- Los datos y documentos (de todo tipo, ya sea técnicos, comerciales, económicos, de know-how o de organización) a los que tengan acceso los trabajadores en el transcurso de su trabajo son estrictamente confidenciales y está totalmente prohibida su difusión, manipulación, eliminación, copia o uso para cualquier otro fin que no sea el desarrollo de la actividad profesional encomendada al trabajador.

3.2.- Los datos de referencia no saldrán de la empresa, excepto si es estrictamente necesario para el desarrollo de la actividad. En este caso habrá que comunicarlo previamente al responsable de informática de la empresa y el soporte que se utilice deberá haber sido validado por éste. Los datos se grabarán encriptados para dificultar su apropiación por un tercero en caso de pérdida del soporte.

IV.- Seguridad

4.1.- Cada usuario accederá al sistema previa identificación a través de un nombre de usuario y un password personal. El sistema, de forma periódica obligará al usuario a cambiar la contraseña**.**

4.2.- Cada usuario tendrá acceso, dentro del sistema, únicamente a la información que necesite para el desarrollo de su trabajo. Periódicamente el responsable de informática revisará los permisos de acceso a los efectos de mantenerlo actualizado.

4.3.- Los datos se almacenarán siempre en la red para facilitar el control de accesos y las copias de seguridad. En ningún caso está permitido el almacenamiento en equipos locales. A los servidores, sólo podrá tener acceso el responsable de informática y el Responsable de Cumplimiento Penal cuando así se requiera.

4.4.- La red contará con un sistema de copias de seguridad automático. El responsable de informática velará para que el mismo funcione de forma correcta y los datos puedan ser recuperados.

4.5.- Cuando se dé de baja un equipo informático, el responsable de informática adoptará las medidas oportunas para garantizar que la información que pudiera haber en su disco duro haya quedado totalmente destruida y no sea accesible a terceros.

4.6.- Cualquier usuario que desee conectar un dispositivo móvil personal en la red (móvil, tableta, etc.) deberá validarlo previamente con el responsable de informática.

V.- Grabaciones

5.1.- Está totalmente prohibida la instalación de equipos ocultos de grabación de imágenes y/o de voz.

5.2.- Sin perjuicio de lo anterior, la empresa podrá instalar cámaras de seguridad, que cumplan la normativa en materia de seguridad, siempre que estén debidamente señalizadas. Las cámaras de referencia en ningún caso enfocarán zonas donde se pueda vulnerar la intimidad (como vestuarios o aseos).

5.3.- Las imágenes tomadas por las cámaras de seguridad instaladas conforme al anterior punto 5.2. quedaran registradas temporalmente en un disco duro, al que sólo podrán acceder aquellas personas debidamente autorizadas por la empresa.

VI.- Daños informáticos a sistemas, documentos y programas de terceros

Está totalmente prohibida cualquier conducta que tenga por objeto o consecuencia borrar, dañar o alterar de cualquier forma datos, programas y documentos informáticos de terceros así como cualquier conducta tendente a obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. También está prohibida la utilización de los equipos y recursos de la empresa para acceder sin autorización a sistemas o equipos de terceros o para obtener información confidencial de los mismos.

Está totalmente prohibido también el envío desde los equipos de la empresa de spam así como de cualquier tipo de programa malicioso (malware) con independencia de cuál sea su denominación y funciones.

VII.- Incidencias y denuncias

La empresa velará para el cumplimiento efectivo de las obligaciones recogidas en el presente protocolo.

En caso de que el responsable de informática o algún otro miembro de la empresa detecte una posible incidencia o incumplimiento del presente protocolo, lo comunicará al Responsable de Cumplimiento, a efectos de que éste, previas las verificaciones que considere necesarias, pueda adoptar las medidas que correspondan a fin de corregir la situación, adoptar las medidas disciplinarias que conforme a la legislación laboral corresponda o, incluso, denunciar los hechos a las autoridades competentes.