

POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS

1.- OBJETO Y FINALIDAD.

En fecha 1 de septiembre de 2017 se aprobó el **Código de Conducta de LA FARGA GESTIÓ D'ESQUIPAMENTS MUNICIPALS, S.A.** (en adelante LA FARGA GEM, S.A.) que dispone entre sus valores, normas y principios de actuación, y en concreto en el apartado 3.8.2., el Uso adecuado de las herramientas informáticas.

A fin de facilitar el cumplimiento de dichos principios, se elabora la presente Política que tiene como finalidad, no solo la **protección física y el buen funcionamiento de los equipos electrónicos** que facilita la empresa a sus trabajadores, sino también la **protección de la información** cada vez más abundante y más dispersa, y que resulta accesible desde múltiples dispositivos.

La proliferación de dispositivos electrónicos con acceso a mucha información de la organización, ha incrementado exponencialmente el **riesgo de que terceros puedan tener acceso al sistema**, obteniendo información confidencial que podría causar un grave perjuicio a la organización.

Por ello, resulta fundamental diseñar unas pautas de uso dirigidas a todas las personas trabajadoras de la empresa, que **eleve el estándar de seguridad** y la protección de dicha información, evitando que cualquier persona trabajadora, por acción u omisión, pueda ocasionar un perjuicio al patrimonio de la empresa, o a su reputación, a través de:

- accesos no autorizados a los ordenadores
- infecciones por malware
- robo y fuga de datos en formato digital

- ataques de ingeniería social, es decir, engaños para manipular a los empleados a fin de obtener información de LA FARGA GEM, S.A., o para entrar en los sistemas de dicha entidad, u otras operativas tendentes a estos fines.

Estas recomendaciones e instrucciones están alineadas con el Código de Conducta y Convenio Colectivo de LA FARGA GEM, S.A., se han consensuado con los representantes de los trabajadores y se comunicarán a cada una de las personas trabajadoras.

2.-DEFINICIÓN MEDIOS TECNOLOGICOS y TIC'S.

. **Medios tecnológicos:** Son todos aquellos equipos, programas o aplicaciones utilizadas para realizar determinadas funcionalidades en un ordenador, dispositivo móvil o Tablet, tales como el sistema operativo, programas de ofimática o herramientas de comunicación, entre otros.

. **TIC's -Tecnologías de la Información y la Comunicación-:** Recursos, medios, herramientas, aplicaciones e instrumentos para almacenar, procesar, gestionar y tratar, en cualquier de sus formas, la información, y *enviarla de un lugar a otra*, permitiendo el más rápido acceso a la misma para el desarrollo de la actividad empresarial (Internet, redes sociales, etc..). Su finalidad es comunicar, compartir y difundir la información.

3.- MEDIDAS PARA UNA CORRECTA UTILIZACION DE LOS MEDIOS TECNOLOGICOS yTIC's.

Los empleados de LA FARGA GEM, S.A. utilizarán los equipos y dispositivos electrónicos que la empresa pone a su disposición, en base a las siguientes indicaciones:

3.1. Propiedad de los equipos y dispositivos electrónicos.

Todos los equipos y dispositivos electrónicos facilitados a los empleados para el desempeño de su trabajo son propiedad única y exclusiva de LA FARGA GEM. S.A. Por ello, las personas trabajadoras tienen el *deber de cuidado y diligencia* respecto a dichos medios, y comunicarán a la cualquier incidencia que se produzca en los mismos por causas ajenas a su

voluntad (robos, hurtos, daños...). La comunicación de dichas incidencias se hará con la máxima urgencia en cuanto se tenga conocimiento de las mismas y al **responsable inmediato**, a fin de que puedan adoptarse las medidas oportunas en orden a la protección de la información que se contenga en dichos equipos o dispositivos.

Como propietario de dichos dispositivos, LA FARGA GEM, S.A. **tendrá la facultad de controlar y monitorizar las actividades de las personas trabajadoras** relativas al uso de los mismos, respetando siempre la dignidad e intimidad de las personas, así como el respeto al secreto profesional en caso de periodistas. En este sentido, la empresa podrá establecer los mecanismos para detectar y prevenir conductas contrarias a la normativa legal o interna de la que pueda derivarse un perjuicio para la empresa, o para sus trabajadores, usuarios o terceros.

Asimismo, una vez finalizada la relación laboral, la empresa tiene derecho a recuperar los dispositivos cedidos a la persona trabajadora para el desempeño de sus funciones, así como la información contenida en los mismos, incluidas las comunicaciones electrónicas, que serán propiedad de LA FARGA GEM, S.A.

Los empleados únicamente podrán acceder a los sistemas informáticos debidamente instalados por la empresa. No instalarán, utilizarán o distribuirán ningún tipo de software o aplicación que pudiera, siquiera potencialmente, afectar a la seguridad de los sistemas, ni podrán hacer copias o descargas no autorizadas, ni efectuar acciones que pudieran permitir la entrada de virus informáticos.

3.2. Uso de los dispositivos electrónicos:

El usuario de cualquier dispositivo informático o de comunicación que sea propiedad de la entidad, no podrá, bajo ningún pretexto, divulgar o transmitir información ilegal, sexista, abusiva, difamatoria, obscena, racista, ofensiva, pornográfica, o cualquier tipo de información ofensiva o no autorizada por las Leyes, ya sea a través de fotografías, textos, banners publicitarios o enlaces a páginas externas; tampoco podrá publicar, transmitir, reproducir, distribuir o explotar cualquier otro componente dañino para la integridad de los sistemas informáticos o que pueda

infringir derechos de propiedad intelectual; del mismo modo, tampoco podrán publicar o facilitar material o acceso a recursos sobre hacking, craking, o cualquier otra información que LA FARGA GEM, S.A. considere susceptible, aunque sea potencialmente, de comprometer la seguridad o integridad de los sistemas informáticos.

. **Craking:** modificación del software con la intención de eliminar los métodos de protección que llevan los programas a fin de evitar la realización de copias, el borrado de los números de serie, verificación de fechas, etc..

. **Hacking:** descubrimiento de las debilidades de una red o sistema informático para acceder al mismo y a la información que en los mismos se contiene.

Queda expresamente prohibido:

-La utilización de la red para juegos de azar, sorteos, subastas, descargas de vídeo, audio u otros materiales no relacionados con la actividad profesional. Si en algún caso, y para un fin estrictamente profesional, fuera necesario el acceso a alguna página con acceso no autorizado, únicamente se podrá llevar a cabo el mismo, cuando medie *autorización expresa y escrita* del responsable del departamento.

- El acceso a debates en tiempo real (chat/IRC) porque son especialmente peligrosos ya que facilitan la instalación de utilidades que permiten el acceso no autorizado al sistema, excepto si es con fines formativos y previa autorización del responsable del departamento.

- *La descarga premeditada o instalación de programas o archivos de origen desconocido*, vía Internet o por cualquier otra vía -CD-ROM, USB, o correo electrónico,...-que no hayan sido autorizados expresamente por el Departamento Informático, ni de cualquier otro tipo de trabajo o material que sea propiedad intelectual de terceros, cuando no se disponga de autorización expresa del indicado Departamento Informático o del responsable del departamento.

- Instalar o ejecutar desde cualquier punto de la red, programas o archivos que intenten descubrir información diferente a la del propio usuario en cualquier elemento de la red tales como detectores, escáneres de puertos, programas de administración remota, etc...

- Efectuar acciones negligentes que pudieran permitir la entrada de virus informáticos.

El **Convenio Colectivo** vigente a título *enunciativo* las conductas relacionadas con el uso de los dispositivos tecnológicos, correo electrónico e Internet, en su artículo 33 que por su relevancia se reproducen a continuación:

33.1 Tendrán la consideración de **faltas leves**:

i) La utilización del correo electrónico e Internet por parte de los trabajadores:

i) 1. Realizar envíos de mensajes de forma masiva o en cadena, no autorizados, especialmente aquellos con finalidades comerciales o publicitarias sin el consentimiento del destinatario (correo basura).

i) 2. Realizar cualquier tipo de envío sin relación con la actividad profesional que perturbe el funcionamiento normal de la red.

Se considerarán **faltas graves**:

k) La utilización del correo electrónico, Internet y de las redes sociales corporativas por parte de los trabajadores:

k) 1. La falsificación de mensajes de correo electrónico.

k) 2. La utilización y el tratamiento de datos de carácter personal de terceros sin la autorización necesaria.

k) 3. El envío de mensajes o imágenes con material ofensivo, inadecuado o con contenidos discriminatorios por razones de género, así como aquellos que promuevan el acoso sexual.

k) 4. La utilización de la red para juegos de azar, sorteos, subastas, descargas de vídeo, audio u otros materiales no relacionados con la actividad profesional.

k) 5. El acceso a debates en tiempo real (chat/IRC), porque son especialmente peligrosos ya que facilitan la instalación de utilidades que permiten el acceso no autorizado al sistema.

k) 6. El acceso a páginas web (www) y a otras utilidades como FTP, Telnet, etc. que no estén relacionadas con la actividad de La Farga o con las tareas del puesto de trabajo del usuario, especialmente las de contenido sexual y/o pornográfico, salvo autorización expresa.

k) 7. La descarga premeditada o instalación de programas de origen desconocido o propiedad del usuario en los sistemas de La Farga, excepto si existe autorización previa de la dirección técnica.

Se consideran **faltas muy graves**:

s) La utilización del correo electrónico, Internet y redes sociales corporativas por parte de los trabajadores:

s) 1. Destruir, alterar, inutilizar o dañar de cualquier forma los datos, programas o documentos electrónicos de La Farga o de terceros. Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal.

s) 2. Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la dirección técnica, o cualquier otro tipo de trabajo o material que sea propiedad intelectual de terceros, cuando no se disponga de autorización.

s) 3. Instalar o ejecutar desde cualquier punto de la red programas o archivos vía Internet o vía CD-ROM, discos u otros soportes sin la autorización expresa de la dirección técnica.

s) 4. Instalar o ejecutar desde cualquier punto de la red programas o archivos que intenten descubrir información diferente a la del propio usuario en cualquier elemento de la red, tales como detectores, escáneres de puertos, programas de administración remota, etc.

3.3. Acceso a información de la organización:

Todos los empleados de LA FARGA GEM, S.A. tienen acceso a los dispositivos e información a través de unas claves de acceso -nombre de usuario y contraseña- que son *secretas, personales e intransferibles*. La protección del sistema frente al posible acceso de terceros, reside en la fortaleza y celo con la que sean protegidas por los empleados.

Por ello, las contraseñas deberán incluir varios tipos de caracteres y deberán ser modificadas cada cierto periodo de tiempo que *no será superior a 1 año*.

Con carácter general, siempre que sea posible se trabajará sobre los servidores corporativos. Cuando sea necesario trabajar en modo local, el trabajador será responsable de que la información guardada en local quede también guardada en el servidor para evitar su pérdida.

Se evitará el copiado de información -de cualquier tipo- de la empresa o de datos personales, en dispositivos externos, o su envío por correo electrónico a otras direcciones personales, así como el **envío o copiado de información a carpetas en la nube o servidores remotos que no sean del entorno corporativo** vía Internet (tipo Google Drive, Microsoft One Drive, DropBox, WeTransfer, etc.). Cuando fuere necesario dicho copiado, se solicitará **autorización escrita del responsable del departamento**, y se

llevará a cabo el copiado **cifrado o con contraseña** a fin de evitar la fuga de dicha información en caso de extravío o robo.

Se prohíbe terminantemente:

- Entregar o facilitar las claves de acceso por parte de un trabajador a otro, salvo cuando fuera estrictamente necesario por motivos de vacaciones, baja laboral, u otros motivos justificados, en cuyo caso dichas claves se entregarán con autorización expresa del responsable del departamento.
- Destruir, alterar, inutilizar o dañar de cualquier forma los datos, programas o documentos electrónicos de La Farga o de terceros. Estos actos podrían ser además constitutivos de un delito de daños.

3.4. Uso del correo electrónico corporativo:

Cualquier comunicación por escrito de un empleado efectuada desde su dirección de correo personal corporativa, representa a toda la organización. Por ello, toda comunicación electrónica corporativa puede ser monitorizada y vigilada por la empresa a fin de asegurar el cumplimiento de la normativa legal y del Código de Conducta, con salvaguarda de los derechos de dignidad e intimidad de las personas trabajadoras, así como el respeto al secreto profesional en el caso de los periodistas.

Queda prohibido el uso del *correo electrónico corporativo* para el envío de comunicaciones de carácter privado. Si bien se permite el uso de los equipos y dispositivos para uso personal/privado, siempre de modo limitado y razonable, los mensajes electrónicos de carácter personal y privado deberán realizarse siempre vía web ya través de una cuenta de correo privada, nunca a través de una dirección de correo corporativa.

Queda expresamente prohibido:

- El envío de mensajes de forma masiva o en cadena, no autorizados, especialmente aquellos con finalidades comerciales o publicitarias sin el consentimiento expreso del destinatario (correo basura).
- Realizar envíos sin relación con la actividad profesional y que puedan perturbar el funcionamiento normal de la red.

- El uso de equipos o correos de otros empleados, así como la falsificación de mensajes.
- El envío de mensajes o imágenes con material ofensivo, inadecuado, difamatorio, o con contenidos discriminatorios por razón de género, así como aquellos que promuevan el acoso sexual o por razón de sexo.

Se tendrá máxima cautela con la apertura de mensajes recibidos de remitentes desconocidos, más aún si tienen el asunto en otro idioma o llevan archivos adjuntos. Se eliminarán los mensajes con anexos susceptibles de ejecución y, en caso de duda, se consultará siempre, antes de abrirlos con el Departamento de Informática.

Por motivos de seguridad, se realizarán copias de seguridad de los correos electrónicos y se podrá acceder a su contenido cuando se produzcan problemas técnicos o de seguridad, o cuando existan sospechas de incumplimiento de las normas contenidas en este documento, y siempre con las medidas indicadas en el apartado quinto de este documento relativo a control y vigilancia.

3.5. Gestión de incidencias: Los empleados estarán atentos a cualquier incidencia que pueda surgir en relación con el uso de los equipos o dispositivos o el acceso a los sistemas de información. El uso inapropiado de los recursos puede conllevar serias consecuencias y perjuicios a la empresa.

Los empleados deberán informar sobre cualquier tipo de incidencia en el Uso de los Medios Tecnológicos que pueda comprometer el correcto funcionamiento de los sistemas informáticos o la protección de la información, al responsable TIC asignado al servicio y/o mediante comunicación a incidencias.tic@lafarga.com, indicando en el asunto se trata de INCIDENCIA USO MEDIOS TECNOLOGICOS, para facilitar su registro y resolución.

4.- **PRINCIPIO DE CONFIDENCIALIDAD** de toda la información de la que los trabajadores puedan ser conocedores, tanto respecto a otros empleados, como de proveedores, usuarios, fuentes informativas en la actividad periodística o terceros.

La confidencialidad de la información, de los datos personales y de las comunicaciones, constituye un derecho fundamental reconocido en la Constitución Española, que debe guiar el modo de recibir, tratar, y proporcionar información. Por tanto, todos los trabajadores y directivos deberán mantener el más estricto secreto profesional y guardar confidencialmente toda la información que manejen en el curso de su labor profesional.

5.- DIRECCION Y CONTROL DE LA ACTIVIDAD LABORAL

5.1.- Alcance

El artículo 18.1 de la *Constitución Española* garantiza el derecho al honor, a la **intimidad personal y familiar** y a la propia imagen. Asimismo, el artículo 18.3 del mismo Cuerpo Legal protege el **secreto de las comunicaciones** y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

Asimismo, este derecho a la privacidad de los trabajadores, *“ha de conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia la empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores”* (Grupo de Trabajo Directiva 679/16), así como con lo dispuesto en el artículo 20.3 del *Estatuto de los Trabajadores* que dispone: *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.”*

Por ello, la empresa podrá adoptar las medidas que considere más oportunas para ejercer la oportuna vigilancia y control sobre dichos medios, y velar por el cumplimiento, por parte del trabajador, de sus obligaciones y deberes laborales tal como ha señalado en diversas ocasiones la Sala de lo Social del TS (entre otras STS 119/2018 de 8 de febrero).

Los principios que han de regir dicha actividad de vigilancia y control son:

- a) Juicio de idoneidad: ¿La medida de control es susceptible de conseguir el objetivo propuesto?
- b) Juicio de necesidad: ¿La medida de control es necesaria, en el sentido de que no existe otra medida más moderada para la consecución del objetivo?
- c) Juicio de proporcionalidad: ¿La medida de control es proporcionada al derivarse de su aplicación más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto?
- d) Juicio de justificación: ¿existe causa objetiva que justifique la medida?



Cuando sea necesario un registro sobre la persona del trabajador, en sus taquillas y efectos particulares, se tendrá en cuenta lo dispuesto en el artículo 18 del Estatuto de los Trabajadores: *“Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.”*



5.2.- Control del correo electrónico corporativo:

Cuando fuera necesario el control del correo electrónico, este se llevará a cabo siempre bajo los principios indicados en el apartado anterior y con programas informáticos de búsqueda ciega ***dirigida y no indiscriminada***.



La revisión se hará a presencia de la persona trabajadora a cuyo correo electrónico se vaya a acceder y de un representante legal de los trabajadores (por la particularidad de su actividad, recogida específicamente en el artículo 20 de la Constitución, se extremará el cuidado en el caso de los periodistas teniendo en cuenta que el secreto profesional es una garantía de la libertad de información). Se levantará acta de las acciones realizadas con identificación de los intervinientes, el objeto del acceso y su resultado, debiendo firmar como mínimo dos de las partes intervinientes.

5.3.- Control del acceso a Internet

La política de la empresa respecto a Internet se basará más en la prevención que en la detección. En tal sentido, se dará prioridad a la utilización de herramientas dirigidas a limitar el acceso a determinadas páginas o descargas de contenidos -por ejemplo, mediante el bloqueo a algunas paginas webs o instalando advertencias automáticas-.

Se facilitará información a la persona trabajadora cuando se detecten accesos sospechosos en Internet a fin de comprobar la existencia de riesgo por abuso y/o para evitar posibles riesgos de seguridad en la red. En este caso, se analizarán tanto el tiempo empleado como las webs visitadas y de su resultado se podrá determinar una actuación correcta o incorrecta de la persona trabajadora. Si como consecuencia de estas comprobaciones, se revela una posible utilización abusiva de Internet, se podrá valorar la posibilidad de proceder a otros controles.

6.- COMISION INFORMATICA



Se constituirá una Comisión Informática integrada por dos representantes de la empresa y dos de los trabajadores que valorarán, y en su caso elaborarán, un listado de excepciones a estas normas generales, así como la adaptación, si fuese necesario, de estas normas a las mejoras y avances de Medios Tecnológicos y TIC'S que se vayan incorporando a la Empresa.

7.- APROBACION Y COMUNICACIÓN



Esta política se someterá a la consideración de los representantes de los trabajadores a fin de que puedan hacer sus aportaciones, previa remisión al Consejo de Administración para su aprobación.

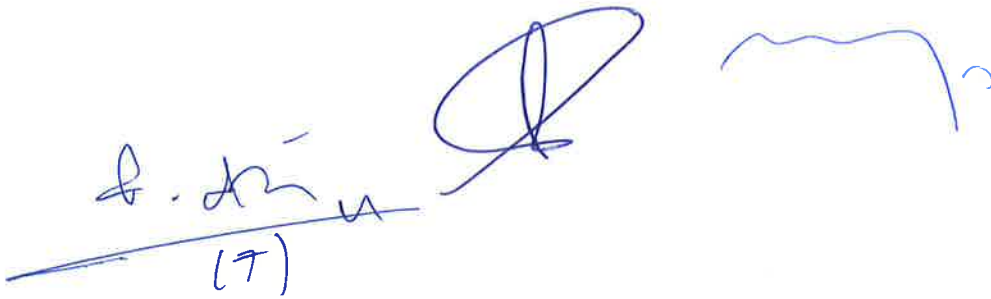


Una vez aprobado por el Consejo de Administración, se entregará una copia del mismo por vía electrónica a cada trabajador solicitándose el acuse de recepción del mismo y se insertará el mismo en la Intranet para consulta de todos los trabajadores, indicándose su ubicación.

Se incluirá también este protocolo en el pack de bienvenida que se facilita a todos los trabajadores, debiéndose dejar constancia de su recepción.

Asimismo, se proporcionará la formación adecuada para su conocimiento y se revisará anualmente esta política.

Barcelona, 11.1.2019



Handwritten signature and initials in blue ink. The signature consists of a stylized 'J' followed by a large loop. To the left, the initials 'J. M.' are written above a horizontal line, with '(7)' written below the line. To the right of the main signature is a wavy line.