DOCUMENTO PRESTACIÓN DE SERVICIOS TEMPORAL POR EL/LA TRABAJADOR/A EN SU DOMICILIO COMO CONSECUENCIA DEL COVID-19

En Madrid a

REUNIDOS

De una parte: **D. MIGUEL ÁNGEL RODRÍGUEZ ESCRIBANO** con D.N.I. 03809264-G, como Director de Recursos Humanos de la Empresa **SUMINISTROS, IMPORTACIONES Y MANTENIMIENTOS ELECTRICOS, S.A. (SERMICRO)**, con domicilio en la calle Pradillo 48-50, de Madrid.

Y de otra **D./Dña.**_____ con D.N.I. _____, en su calidad de trabajador del GRUPO SERMICRO, en adelante EL/LA TRABAJADOR/A.

Por medio de la presente comparecen y

ACUERDAN

Primero.- Condiciones laborales.

Que, con fecha , EL/LA TRABAJADOR/A ha solicitado al GRUPO SERMICRO la posibilidad de trabajar de forma remota desde su propio domicilio, sin que ello suponga una modificación de las condiciones de trabajo pactadas entre ambas partes que regulan su relación laboral en base a ello establecen las siguientes CONDICIONES:

a) Duración de la modificación: el acuerdo por el que la empresa reconoce al trabajador la posibilidad de trabajar de forma remota desde su domicilio (teletrabajo) tendrá carácter EXCEPCIONAL y TEMPORAL, efectivo a partir del _____.
b) EL/LA TRABAJADOR/A desarrollara, durante este tiempo, sus funciones desde su propio domicilio sito en la calle_____ .

c) La jornada de trabajo continuará siendo la actual y su horario será el mismo que venía realizando hasta el momento.

d) EL/LA TRABAJADOR/A en el horario indicado anteriormente podrá ser localizado por La Empresa mediante teléfono móvil o fijo y a través de las herramientas informáticas suministradas por la empresa.

e) EL/LA TRABAJADOR/A se obliga a asistir a las reuniones objeto de su actividad y objetivos ya sea en el domicilio de La Empresa o de los clientes dentro del referido horario, asumiendo, EL/LA TRABAJADOR/A, los posibles gastos de desplazamiento que pudieran darse.

f) EL/LA TRABAJADOR/A deberá reportar su actividad a La Empresa de acuerdo a los procedimientos establecidos por la compañía o por su superior inmediato.

g) En el supuesto que EL/LA TRABAJADOR/A necesite trasladarse del domicilio indicado, ya sea de forma temporal o permanente, lo deberá poner en conocimiento de La Empresa con una antelación de 15 días.

Segundo.- Prevención de Riesgos laborales.

El Acuerdo Marco Europeo sobre Teletrabajo define esta actividad como "*una forma de organización y/o realización del trabajo, en la cual un trabajo que puede ser realizado igualmente en los locales de la empresa como fuera de estos, de forma regular*".

El trabajo que se desempeña en modalidad de teletrabajo, no exime a la empresa de su obligación de proteger la seguridad y salud de los trabajadores. Tal y como indica la directiva 89/391, el empresario deberá:

- Evitar los riesgos.
- Evaluar los riesgos que no se puedan evitar.
- Combatir los riesgos en su origen.
- Adaptar el trabajo a la persona.
- Tener en cuenta la evolución de la técnica.

- Planificar la prevención.
- Dar las debidas instrucciones a los trabajadores.

Para dar cumplimiento a dicho mandato y, por lo tanto, verificar la correcta aplicación de las normas de seguridad y salud, el empresario tendrá acceso al lugar de desempeño del trabajo, previa notificación y autorización dEL/LA TRABAJADOR/A.

A tal fin, deberá aportar, al servicio de prevención de riesgos laborales del GRUPO SERMICRO, la siguiente información gráfica para comprobar la idoneidad del puesto de trabajo, desde el punto de vista de prevención de riesgos laborales:

- Fotografía de la zona de trabajo (ubicación física donde se trabajará)
- Fotografía de la mesa de trabajo
- Fotografía del equipo de trabajo (ordenador)
- Fotografía de la silla de trabajo
- Fotografía de la luminaria para la iluminación artificial disponible

Esta información deberá remitirse a Belén Casero Pérez (b.casero@sermicro.com) y a Manuel González Polo (m.gonzalezpolo@sermicro.com) en el plazo de 15 días naturales desde la firma del presente acuerdo.

En el caso de que la información facilitada por EL/LA TRABAJADOR/A no fuera suficiente para asegurar dicha idoneidad, se solicitaría por parte del servicio de prevención, permiso para acceder a su domicilio.

Tercero.- Protección de datos.

Como consecuencia de lo que antecede y con el objeto de cumplir las previsiones normativas relativas a la legislación vigente en materia de protección de datos, EL/LA TRABAJADOR/A se compromete a aplicar las instrucciones que se detallan a continuación y estructuramos en la siguiente forma:

1.- Portátiles, smartphones, tabletas digitales:

- No se debe almacenar información corporativa que no sea estrictamente necesaria para el desarrollo del trabajo.
- Se debe cifrar la información confidencial o solicitar a la empresa su cifrado.
- Notificar al personal técnico responsable la sospecha de infección por virus u otro software malicioso del equipo.
- Custodiar el soporte móvil cuando se está fuera de las instalaciones. En caso de robo o pérdida del equipo lo notificas al responsable.
- El usuario aplicará las normas recogidas en la Política de uso del puesto de trabajo que sean relativas al uso de un equipo informático (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, etc.).
- El usuario es el responsable de la información perteneciente o relativa a SERMICRO o cualquiera de las empresas pertenecientes al Grupo ACS, clientes o potenciales clientes de las mismas que esté utilizando para la realización de su trabajo aunque para ello esté empleando un dispositivo que no sea propiedad de la compañía, estando comprometido por ello a garantizar la seguridad de la información que contiene el equipo utilizado.

2.- Archivos temporales o copias de trabajo de documentos:

- Aquellos archivos temporales o copias de documentos creados exclusivamente para la realización de trabajos temporales o auxiliares deben cumplir el nivel de seguridad que les corresponda. Todo archivo temporal o copia de trabajo así creado debe ser borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

- Si en el desarrollo del trabajo se necesita almacenar datos de carácter personal en ordenadores o en cualquier soporte informático, el usuario se responsabiliza de adoptar las medidas de seguridad oportunas mientras dichos datos se mantengan.

3.- Acceso a través de redes de comunicaciones:

- Las medidas de seguridad exigibles a los accesos a datos personales a través de redes de comunicaciones sean o no públicas, deben garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. En caso de desconocer dichos niveles de seguridad abstenerse de su uso y consultar.

4.- Tratamiento de datos en soportes no autorizados.

- Todos los usuarios deberán adoptar las medidas necesarias para asegurar que todos los datos de carácter personal contenidos en tratamientos no automatizados estén debidamente custodiados y protegidos. Serán de aplicación las medidas de seguridad descritas en los apartados anteriores en lo relativo a:
  - ✓ Confidencialidad de la información.
  - ✓ Control de Acceso.
  - ✓ Gestión de soportes y documentos.
  - ✓ Registro de incidencias.
  - ✓ Régimen de trabajo fuera de los locales del responsable o encargado del tratamiento.
  - ✓ Ficheros temporales o copias de trabajo de documentos.

- Medidas de seguridad a tener en cuenta por el usuario:

  - ✓ **Criterios de archivo:** Archivar los soportes o documentos en papel garantizando su correcta conservación, localización y consulta de la información, de modo que posibilite el ejercicio de los derechos por parte del interesado.
  - ✓ **Dispositivos de almacenamiento:** Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal dispondrán de mecanismos que obstaculicen su apertura. Procurar que los mismos sean debidamente utilizados.
  - ✓ ***Para los tratamientos con categorías especiales de datos:*** Los armarios, archivadores u otros elementos en los que se almacene documentación con datos de carácter personal se encontrarán en áreas en las que el acceso esté protegido. Evitar los accesos de personal no autorizado a estas áreas.
  - ✓ **Custodia de los soportes:** La persona que se encuentre al cargo de documentación con datos personales cuando la misma no esté archivada, por estar en proceso de revisión o tramitación, es responsable de custodiar dicha información y de impedir en todo momento que pueda ser accedida por persona no autorizada.
  - ✓ **Entrega de documentación en soporte papel:** Queda estrictamente prohibido la entrega o envío de información en soporte papel relativa a personas físicas en sobres, cajas, o cualquier otro recipiente que no esté herméticamente cerrado, y cuya apertura no suponga la rotura del precinto. La entrega se realizará únicamente al titular de los datos o, en su caso, a la persona que haya autorizado por escrito. Asimismo, queda estrictamente prohibido el envío de información relativa a personas físicas, o confidencial a través de medios que no aseguren el cumplimiento de las normas de seguridad exigidas por la Compañía.
  - ✓ **Destrucción de documentación soporte papel:** Para todos los documentos existentes en soporte papel que contengan datos de carácter personal y/o información confidencial existe un sistema de destrucción física de los mismos. Asimismo, queda prohibido deshacerse de la documentación impresa mediante su depósito en papeleras, contenedores o bolsas de basura.
  - ✓ **Copia o reproducción:** Deben destruirse las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior, siguiendo las instrucciones marcadas en los procedimientos internos

En prueba de conformidad con cuanto antecede, lo firman por duplicado ejemplar en el lugar y fecha indicados.

EL/LA TRABAJADOR/A

D. NOMBRE Y APELLIDOS

AUTORIZACIÓN DE SU RESPONSABLE

D. NOMBRE Y APELLIDOS

Vº Bº RRHH

D. NOMBRE Y APELLIDOS