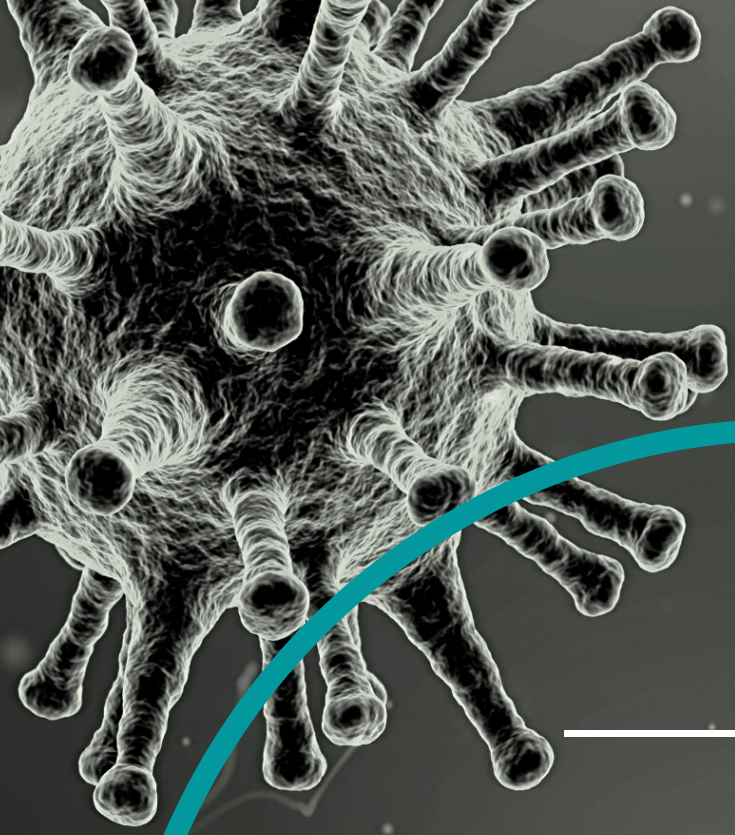

G.E.I.E.S.
GRUPO ESTATAL DE INTERVENCIÓN EN EMERGENCIAS SOCIALES

PAUTAS CORPORATIVAS DE TELETRABAJO

ANTE LA SITUACIÓN DE EMERGENCIA DE SALUD PÚBLICA

18-03-2020

Consejo General del Trabajo Social

DOCUMENTO ELABORADO POR ticdatum

PAUTAS CORPORATIVASDE TELETRABAJO ANTE LA SITUACIÓN DE EMERGENCIA DE SALUD PÚBLICA

Dada la actual situación de emergencia de salud pública ocasionada por el COVID-19, el Consejo Interterritorial del Sistema Nacional de Salud ha recomendado la realización deteletrabajo siempre que sea posible.

Siguiendo esta indicación la organización, en aras a salvaguardar la salud de trabajadores y trabajadoras así como contener la progresión de la enfermedad, ha acordado que la totalidad o parte de la plantilla puedan desarrollar su actividad laboral en su propio domicilio de forma temporal y excepcional mientras perdure la situación de emergencia sanitaria provocada por el COVID-19 y para aquellos trabajos que sea posible realizar a través de medios tecnológicos.

A tal efecto se emiten las siguientes pautas de actuación respecto del desarrollo de la relación laboral en estas circunstancias y en tanto en cuanto perdure la situación de emergencia sanitaria provocada por el COVID-19.

1. Confidencialidad y seguridad de la información.

1.1. Confidencialidad

Con la finalidad de proteger la confidencialidad de la información de la organización deberá guardarse el máximo celo en relación con la información manejada para evitar el conocimiento de la misma por parte de otras personas usuarias que compartan el domicilio de la persona trabajadora.

A tal efecto, deberá preservarse el uso de claves de acceso a la información, particularmente si ésta se encuentra ubicada en un dispositivo personal de la persona trabajadora o se va a acceder en remoto a aquélla.

Así, en el caso de utilizarse un dispositivo personal para el desarrollo del teletrabajo se accederá en remoto, a través de una red segura o VPN, que permite el acceso remoto a la información y no se alojará información corporativa empresarial en el dispositivo personal, ni siquiera para su conservación o para el desarrollo del trabajo en local. En todo caso, es necesario que se establezcan perfiles de acceso para evitar que todo el personal acceda a toda la información o activos de la empresa de manera remota salvo que se haya valorado esta posibilidad por razones del servicio o configuración de éste.

1.2. Seguridad de la información

En teletrabajo se deberán realizar las mismas actuaciones fijadas para la seguridad de la información corporativa en el entorno laboral, como pueden ser las relativas a la periodicidad de las copias de seguridad, actualizaciones automáticas de software, ejecución y actualización periódica del antivirus, tiempos de bloqueo de equipos por inactividad, control de acceso de usuarios, o similares, los cuales no siempre están correctamente configurados o tenidos en cuenta en una instalación personal o doméstica.

Si no es posible instalar en un mismo equipo un arranque dual, esto es, dos sistemas operativos, iguales o diferentes, de los cuales cada uno se utilizará para un entorno (teletrabajo o personal) se instalarán diferentes cuentas de usuario en el mismo equipo; una para entornos confiables (teletrabajo) y otra para asuntos personales.

Si bien la protección que ofrece esta configuración puede ser vulnerable por virus y código malicioso, puede ser una primera línea de defensa poco intrusiva que permite establecer medidas de seguridad diferentes a diferentes perfiles de usuario, facilitando establecer diferentes requisitos para el bloqueo automático del equipo, hacer independiente los historiales de navegación y contraseñas guardadas en el equipo o clasificar mejor los documentos personales de los profesionales permitiendo incluso cifrar la carpeta de cada usuario.

En todo caso, cualquier equipo que vaya a conectase a los entornos corporativos, ya sea propiedad de la organización, proveedor o del empleado, debe cumplir con unos mínimos de seguridad como puede ser tener el sistema operativo actualizado o contar con un antivirus robusto.

Conforme a lo anterior, a continuación se indican algunas medidas de seguridad básicas recomendadas para su aplicación: Estas medidas deberán ser adaptadas por cada organización a su situación particular:

- Instalación del sistema operativo desde una fuente fiable.
- Sistema operativo y aplicaciones actualizadas.
- Software antivirus.
- Cuentas de usuario sin permisos para instalar software.
- Control de acceso robusto.
- Configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc).
- Bloqueo automático por inactividad.
- Software antirootkits.
- Control de software original.
- Cifrado del disco.
- Comprobación periódica de la adecuación de las salvaguardas.
- Guardar en lugar seguro el dispositivo mientras no se utiliza en aras a evitar accidentes domésticos.
- Uso de las conexiones previstas por la organización, si se trata de conexión cifrada (VPN o similar) no acceder de ninguna otra manera.
- Uso responsable de redes de comunicación para evitar sobrecargas.
- Si se utiliza la wifi doméstica, adecuar la clave del wifi a requerimientos de seguridad (uso de claves, no menos de ocho caracteres, etc.).
- No descargar archivos o información corporativa en equipos personales.

2. Métodos de trabajo.

El menor contacto directo con la empresa puede hacer necesario que se establezcan determinados procedimientos de trabajo: a quién reportar el resultado, de qué forma, cada cuánto tiempo, tipos de comunicación (teléfono, correo electrónico, plataformas u otros), periodicidad de reuniones, contenidos y tareas urgentes u ordinarias.

De conformidad con el artículo 88 de la Ley Orgánica 3/2018, de protección de datos y garantía de los derechos digitales, la persona teletrabajadora tiene derecho a la desconexión digital fuera del tiempo de trabajo establecido, a fin de garantizar el respeto de los periodos de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

3. Medios materiales

3.1. En el caso de que la organización haya puesto a disposición de la persona trabajadora medios materiales para que pueda prestar adecuadamente su actividad laboral se describirán los siguientes aspectos:

a. [Describir equipo], con número de serie [número];

b. [Otros elementos entregados (teclados, ratones, pantallas, teléfono móvil, cargadores...)];

c.[...]

3.2. En relación a los medios materiales entregados, la PERSONA TRABAJADORA asume las siguientes obligaciones:

- A prestarles la atención y cuidado necesarios;
- A no utilizarlos para fines privados o personales;
- A utilizarlos únicamente dentro de los horarios previstos en el contrato de trabajo;
- A mantenerlos en todo momento en el interior de su domicilio, salvo para entregarlos a la organización al finalizar la vigencia del período temporal y excepcional.
- A no instalar aplicaciones ni programas informáticos en los dispositivos digitales sin la autorización de la organización;
- A no eliminar o desinstalar ninguna de las aplicaciones o programas instalados por la organización en los dispositivos digitales;
- A mantener en secreto los identificadores de usuario y las claves de acceso (contraseñas) que le facilite la organización. En caso de que la persona trabajadora detecte, o simplemente sospeche, que alguna persona ha podido acceder a dicha información, lo pondrá inmediatamente en conocimiento de la organización, a fin de que esta pueda adoptar las medidas que considere oportunas;
- A no utilizar los medios materiales entregados para acceder a redes públicas de comunicaciones electrónicas, como Internet, para fines no relacionados directamente con la prestación de su actividad laboral;
- A comunicar a la organización, en el menor plazo posible y sin dilaciones indebidas, todas aquellas incidencias que se produzcan en el uso de los medios materiales entregados, y en particular, de cualquier anomalía que afecte o pudiera afectar a la seguridad de la información o de los datos personales a los que tenga acceso o dar lugar al incumplimiento de las obligaciones detalladas en este documento.

3.3. La organización podrá controlar y supervisar la actividad de la persona trabajadora con fines de seguridad, mediante medios telemáticos, informáticos y electrónicos, si bien respetando en todo momento los derechos a la inviolabilidad del domicilio y a la intimidad personal y familiar.

3.4. En el caso de que la persona trabajadora utilice medios propios para la realización de teletrabajo se adoptarán las medidas establecidas en el apartado 1 relativo a la confidencialidad y seguridad de la información.

4. Comunicaciones durante el período de trabajo a distancia

A efectos de la prestación de la actividad laboral y durante los horarios previstos en el regulador de la relación laboral, la organización y la persona trabajadora podrán comunicarse por medios electrónicos o telemáticos, preferentemente mediante plataformas colaborativas y sin realizar descargas directas de documento salvo que sea imprescindible, para evitar sobrecarga de los sistemas, sin perjuicio de poder comunicarse mediante llamada telefónica particularmente en caso de urgencia o de fallos en el funcionamiento de dichos medios materiales o de las redes públicas de comunicaciones electrónicas.

En todo caso, la organización garantizará el derecho a la desconexión digital en el ámbito laboral, y respetará el tiempo de descanso, permisos y vacaciones de la persona trabajadora así como su intimidad personal y familiar.

5. Protección de datos de carácter personal

Los datos de carácter personal relativos a la salud de la persona trabajadora serán tratados, en su caso, por ser necesario para la protección del interés vital de las personas, el cumplimiento legal de lo establecido en la normativa vigente en materia de prevención de riesgos laborales y el interés público esencial en el ámbito de la salud publica frente a amenazas graves para la salud.

Tales datos podrán ser comunicados, en su caso, a los servicios médicos y de prevención para actuar de conformidad con los protocolos establecidos por las autoridades sanitarias, siendo esta la única finalidad del tratamiento de estos datos y siendo tratados únicamente en la medida en que resulte necesario para dar respuesta a tales finalidades; y conservados durante los plazos legalmente establecidos, transcurridos los cuales serán suprimidos.

La persona trabajadora en cualquier momento podrá ejercitar sus derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento de sus datos, 1ºdirigiéndose a la dirección electrónica y/o postal [DEFINIR].

6. Ciberseguridad

A continuación, se indica un conjunto de recomendaciones para teletrabajar de forma segura siguiendo los consejos del Centro Criptológico Nacional (CNN)

- No descargar aplicaciones no oficiales para informarse sobre el Covid 19.
- Prestar especial atención a los mails que se reciben.
- Evitar abrir documentos y archivos adjuntos sobre el Covid 19.
- Asegurar la actualización de los antivirus.
- Tener instaladas las últimas actualizaciones del sistema operativo.
- Tener habilitados canales de comunicación.
- No difundir información que no provenga de medios no oficiales.
- No contribuir a la difusión de contenido no contrastado ni compartir mensajes que puedan generar alarma.
- Prestar atención con imágenes públicas que no enlazan con link a una fuente oficial ya que pueden ser falsas.
- Atender a la redacción, faltas ortográficas o de sintaxis son indicadores habituales de la falsedad de la comunicación.
- Desconfiar de los perfiles que no sigue habitualmente o de reciente creación.

Dª Ana I. Martín Ramos, Exmagistrada, Abogada especializada en protección de datos
D. Iñaki Pariente de Prada, ExDirector de la Agencia Vasca de Protección de Datos, abogado especializado en protección de datos