TELETRABAJO, PROTECCIÓN DE DATOS PERSONALES Y SEGURIDAD

GUÍA DE BUENAS PRÁCTICAS PARA LAS ORGANIZACIONES

Versión 2.3, fecha 31-3-2020

MUTUA INTERCOMARCAL

1.- Introducción

El teletrabajo se ha definido como aquel fenómeno que lleva el trabajo al trabajador, en lugar del trabajador al trabajo.

La finalidad de esta guía es orientar a las organizaciones, sobre los aspectos legales y de seguridad vinculados con el teletrabajo, aplicable tanto ante las actuales circunstancias como para las futuras opciones para conciliar la vida laboral con la familiar de los trabajadores.

No podemos obviar los riesgos que supone el teletrabajo y por tanto, una de las claves para que sea seguro pasa por reforzar la ciberseguridad, proteger los datos personales y minimizar los riesgos, ya que se ha observado últimamente un notable incremento de la actividad de los ciberdelincuentes.

Por lo tanto, la necesidad de asegurar la continuidad del negocio, garantizar la seguridad y confidencialidad de los datos y de respetar los derechos de los trabajadores, entre ellos el derecho a la desconexión digital, nos ha llevado a preparar esta guía dirigida a las organizaciones.

Finalmente antes de tomar cualquier decisión, consultar previamente con sus asesores laborales, jurídicos y tecnológicos, y con el delegado de protección de datos en caso de que disponga de esta figura, ya que la finalidad de esta guía es puramente informativa y no constituye, en ningún caso, asesoramiento legal o tecnológico.

Dídac Merino y Ramon Arnó

- https://www.masqueit.es
- didac.merino@masqueit.es

- http://www.sagaris.cat/
- ramon@sagaris.cat

2.- El teletrabajo

2.1.- Dónde se regula

A estatuto de los trabajadores (ET), el Real Decreto Legislativo 2/2015, de 23-10, fundamentalmente los siguientes artículos:

a.- El artículo 13 (trabajo a distancia).

b.- La modificación del artículo 34.8 según el real decreto ley 6-2.019, donde se reconoce el derecho a solicitar el trabajo a distancia en los términos que se establezcan en la negociación colectiva.

c.- El convenio colectivo aplicable.

d.- El Real Decreto-ley 8/2020, de 17 de marzo de medidas urgentes extraordinarias para hacer frente al impacto económico y social del Covidien-10.

2.2.- Las características

Las principales características del teletrabajo son:

1.- Distancia física entre el trabajador respecto a la ubicación de la organización, es decir que el trabajo se puede realizar desde el domicilio del trabajador o desde otros lugares elegidos por él.

2.- Uso de tecnologías de la información para la interacción trabajador - organización.

3.- Normalmente es voluntario y reversible.

4.- Se formalizará por escrito en forma de anexo, entregando el trabajador la información que establece la directiva 91/553 relativa a la obligación del empresario de informar al trabajador sobre las condiciones aplicables al contrato de trabajo.

5.- Los teletrabajadores tienen los mismos derechos que los que prestan sus servicios en el centro de trabajo, entre ellos el derecho a la formación o a respetar la vida privada del trabajador.

3.- La protección de datos personales

3.1.- En general

La normativa actual es la siguiente:

a.- El reglamento 2016/679 de protección de datos (RGPD).

b.- La ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD).

3.2.- Las obligaciones de la organización

Las obligaciones básicas de cualquier organización o responsable son resumidamente las siguientes:

1. Acreditar una responsabilidad activa y no simplemente pasiva o reactiva.

2. Mantener el Registro de Actividades de Tratamiento (RAT).

3. Evitar tratar, si no es necesario:
    - Categorías especiales de datos
        i. como el origen racial o étnico, datos de salud, opiniones políticas, afiliación sindical, sobre religión o creencias filosóficas, sobre vida y orientación sexual, violencia de género, etc.
    - Datos biométricos
        i. obtenidas a partir de un tratamiento técnico específico, relativas a las características físicas, fisiológicas o conductuales de una persona física, que permiten o confirman la identificación única de la persona (imágenes faciales, datos dactiloscópicos, etc.).
    - Datos genéticos,
        i. relativas a las características genéticas heredadas o adquiridas de una persona física, que proporcionan una información única sobre la fisiología o la salud de esta persona, obtenidas en particular del análisis de una muestra biológica de esta persona.

4. Realizar un análisis de riesgos y aplicar las medidas de seguridad adecuadas.

5. Contratar los encargados de tratamiento que sean diligentes y proactivos y firmar los contratos con las medidas de seguridad a aplicar.

6. Adaptar las cláusulas de protección de datos, el aviso legal y la política de cookies.

7. Aplicar las medidas de protección de datos desde el Diseño y predeterminado.

8. Realizar evaluaciones de impacto (EIPD - PIA), cuando sea necesario.

9. Designar el Delegado de Protección de Datos (DPD - DPO), cuando la normativa lo exija.

10. Notificar los incidentes de Seguridad de manera inmediata y completa al responsable.

11. Formar el personal.

12. Evaluar las medidas jurídicas, tecnológicas y organizativas de manera continuada.

3.3.- La regulación de los derechos digitales de los trabajadores

La LOPDGDD regula los derechos digitales a los artículos 79 a 96, entre ellos el derecho a la desconexión digital.

3.4.- El derecho a la desconexión digital en el ámbito laboral

Es el derecho del trabajador a desconectar digitalmente para garantizar fuera del tiempo de trabajo, el derecho al descanso y las vacaciones así como a la intimidad personal y familiar.

El derecho a la desconexión digital fuera del horario laboral se regula a varias normas:

a.- Artículo 88 de la LOPDGDD.

b.- Artículo 20 del estatuto de los trabajadores (ET), el Real Decreto Legislativo 2/2015, de 23-10.

c.- Artículo 14.j.bis del Real Decreto Legislativo 5/2015, de 30 de octubre, ley del estatuto básico del empleado público.

Algunos ejemplos de este derecho son los siguientes:

a.- La no obligación de responder ninguna comunicación -correo electrónico, WhatsApp, teléfono- una vez finalizada la jornada laboral y por tanto el derecho a no responder un correo hasta el inicio de la jornada laboral.

b.- Las reuniones y las formaciones no se alargarán más allá de la finalización de la jornada laboral, salvo circunstancias excepcionales.

c.- Incluir un mensaje de ancianos en el correo electrónico del tipo "ausente" durante las vacaciones, asuntos propios, permisos, incapacidades, etc.

d.- No se aplicarán los anteriores supuestos si concurren causas de fuerza mayor o aquellas personas que perciben un plus de disponibilidad y que han de estar continuamente disponibles.

e.- Aplicable a personas que trabajan en los locales de la organización y también los que hacen teletrabajo

f.- Realizar formación a los trabajadores.

g.- La organización no podrá sancionar a los trabajadores que ejerciten su derecho a desconectar de acuerdo con la normativa.

h.- Es un derecho, no una obligación.

Por lo tanto hay que redactar una política interna reguladora. A modo de ejemplo puede usar, entre otros, el modelo que han firmado recientemente Telefónica y las organizaciones sindicales mayoritarias en el mes de julio de 2019:

https://fsc.ccoo.es/7d90be81275acecc31ed92448f6ae2c0000050.pdf

4.- La seguridad y el teletrabajo

De manera genérica apuntemos las obligaciones básicas per a las organizaciones y por los trabajadores:

4.1.- Las obligaciones de seguridad para las organizaciones

Las organizaciones deben tener en cuenta un conjunto de consideraciones:

a.- Definir una política de seguridad.

b.- Concretar qué recursos y qué aplicaciones están autorizadas y cuáles prohibidas, así como facilitar las medidas de seguridad.

c.- Proporcionar, instalar y mantener los equipamientos necesarios para el teletrabajo, incluso cuando el trabajador utilice su propio equipo (BYOD o bring your own device).

d.- Definir cuál es la información secreta, la confidencial y al que se puede compartir.

e.- Regular los perfiles de los trabajadores, ya que no todos han de acceder a toda la información, perfiles que deben concretarse de manera individual en lugar de utilizar usuarios genéricos, a través de la segregación de funciones.

f.- Hacer formación al personal.

g.- Cumplir con la normativa de protección de datos personales.

h.-Respetar el derecho a la desconexión digital y otros derechos digitales de los trabajadores.

i.- Valorar la suscripción de una ciberseguiridad.

4.2.- Las obligaciones de seguridad para los trabajadores

Los trabajadores deben tener en cuenta un conjunto de consideraciones:

a.- Aplicar las medidas de seguridad siguiendo las directrices de las organizaciones.

b.- Guardar confidencialidad sobre la información tratada.

c.- Utilizar los recursos con fines laborales y no personales.

d.- Notificar las incidencias rápidamente a la organización.

e.- Crear una cuenta de usuario específico diferente de la cuenta personal o familiar.

5.- Las medidas de seguridad

5.1.- El análisis de riesgo

He aquí un modelo básico de autoevaluación que te puede ayudar a tener un análisis de la seguridad de su organización:

https://adl.incibe.es/

5.2.- Los recursos

Los recursos vinculados con el teletrabajo son básicamente los siguientes:

1. Acceso a la red corporativa a través de un canal seguro.
2. Uso de un canal seguro de comunicaciones.
3. Las contraseñas.
4. El espacio de trabajo seguro.
5. Las medidas de seguridad de los recursos:
    a. El equipo de trabajo es propiedad de la organización (cope).
    b. El equipo de trabajo es propiedad del trabajador (BYOD).

6. El software.

7. El correo electrónico.

    a. La cuenta corporativa.
    b. La cuenta personal.

8. La documentación en papel.

9. La webcam.

10. Las videollamadas y las reuniones virtuales.

11. Las copias de seguridad.

12. La notificación y respuesta delante de los accidentes

13. La formación.

14. Otros recursos.

5.3.- Accede a la red corporativa a través de un canal seguro

POTENCIAR

1. La gestión segura de los puertos y las aplicaciones de entrada.
2. La autenticación de los trabajadores que acceden en la red:
    a. Nombre de usuario y contraseña.
    b. Certificado digital
3. La asignación de los permisos en función del perfil del trabajador.
4. Utilizar vdi (Virtual Desktop Infraestructura).
5. Mantener la trazabilidad de las conexiones y de los registres de auditoría.

EVITAR

1. El uso de team viewer o anydesk con licencia personal y por tanto solo utilizar la licencia corporativa.
2. Abrir el acceso directo a los trabajadores sin ningún control.

5.4.- Uso de un canal hacha de comunicaciones

POTENCIAR

1. Un canal hacha de comunicaciones entre el trabajador y l´organización:a. VPN (Virtual Private Network).
2. Navegar de manera segura por las páginas web que tengan cifrado htpps.
3. Activar la opción de navegación privada
4. Escribir la URL o dirección al navegador y hacer clic a continuación.
5. Al finalizar el trabajo, cerrar siempre la sesión, es decir ir al programa que se utiliza, buscar el menú cerrar sesión y ejecutarlo.
6. Especial atención a los métodos de ingeniería social.
    a) Llamadas urgentes.
    b) Correos donde piden hacer clic en un enlace o be llenar un formulario.
    c) Comunicaciones donde es soliciten datos sobre cuentas, tarjetas de crédito o contraseñas.

EVITAR

1. El uso de webs sin revisar que l'URL sea correcta
    a. Gugle en lugar de google.com
    b. Aple en lugar de apple.com
2. Conectarse desde wifis públicas sin VPN.
    a. Hoteles
    b. Aeropuertos
    c. Bares
    d. Centros comerciales
3. El uso de canales no seguros.
4. Utilizar redes peer tono peer (e-mule, uno-torrente, etc.)
5. Al finalizar el trabajo, dejar la sesión abierta.
6. Hacer clics en los enlaces a webs, correos u otros mensajes desconocidos o sospechosos.

5.5.- Les contraseñas

POTENCIAR

1. Custodiar de manera segura, utilizando software creado especialmente para guardar las contraseñas.
2. No compartir las contraseñas ni el certificado digital
3. Crear contraseñas fuertes y complejas para evitar suplantaciones de identidad:
    a. longitud mínima recomendada de 8 caracteres.
    b. combinación de y.

1. letras,
2. ii. números
3. iii. caracteres especiales
4. Limitar a 3 el número máximo de intentos fallados de autenticación.
5. Activar el doble factor de autenticación.
    a. Envío al móvil ´d un código de acceso
    b. Aconsejable para Outlook, Gmail, Twitter, LinkedIn, etc.
6. Modificar las claves genéricas de los dispositivos:
    a. Router (router) de casa.
7. Obligar a cambiar las contraseñas de forma habitual, sobre todo y de manera inmediata después del primer acceso
8. Custodiar las tarjetas que incorporen certificados digitales

EVITAR

1. Compartir las contraseñas.
2. Que tengan menos de 8 caracteres o sean fáciles de adivinar.
3. 1234
4. qwerty
5. Apuntarlas a un post-it o en otros documentos fácilmente accesibles.
6. Enviarlas por correo electrónico, WhatsApp, etc.
7. Guardar las contraseñas de forma automática si no posarlas cada vez.

5.6.- El espacio de trabajo seguro

POTENCIAR

1. El uso de un espacio a casa, que guarde cierta separación con el resto de las dependencias.
2. Crear un espacio de trabajo seguro, con limitación de acceso a otras personas

EVITAR

1. Trabajar en lugar públicos con personas alrededor:
    a. shoulder surfing

5.7.- Las medidas de seguridad de los recursos

En este caso hay que distinguir dos tipos de recursos diferentes:

a.- El equipo de trabajo es propiedad de la organización (cope)

Se conoce como copo (corporate owned personal enable).

Aquí es la organización la que se propietaria del dispositivo (ordenador, tablet, móvil, etc.).

b.- El equipo de trabajo es propiedad del usuario (byod)

Se conoce como byod (bring your own Device) o uyod (uso your own device).

Aquí es el trabajador quién es el propietario del dispositivo (ordenador, tablet, móvil, etc.)

Tanto si lo equipo de trabajo se propiedad de la organización como si se propiedad de lo usuario (byod), las medidas sueño las siguientes:

POTENCIAR

1. La creación de una carpeta del tipo "trabajo" con contraseña de al menos 8 caracteres, diferente y separada de la carpeta "personal", donde guardaremos toda la información profesional o corporativa.
2. Actualizar el sistema operativo y el resto de los programas como navegadores y otras herramientas con los últimos parches de seguridad
3. Instalar un antivirus para protegerse de las amenazas que s´active automáticamente al introducir uno usb, cd, dvd, etc
4. Evitar el acceso de los familiares a los recursos:
    a. digitales
    b. en papel
5. Crear mecanismos que posibiliten borrar o localizar los dispositivos de manera remota:
        i. En caso de pérdida o robo.
6. Bloquear la pantalla del dispositivo cuando haya un periodo de inactividad que solo se puede desbloquear con una contraseña.
7. Encadenar físicamente el dispositivo para evitar su robo.
8. Borrar al finalizar el teletrabajo
        i. las carpetas de descarga,
        ii. la papelera
        iii. las cookies o galletas
        iv. el historial de navegación:

EVITAR

1. Descargar ficheros o documentos con datos personales en ubicaciones:
    a. Sin contraseña o cifradas.
    b. No autorizadas y Dropbox gratuitos
2. Utilizar memorias usb (pendrive) o discos externos sin cifrar
3. Compartir los recursos con terceros sin autorización.
4. Modificar o desactivar la configuración de seguridad

5.8.- El programa

POTENCIAR

1. El uso de herramientas autorizadas por la organización y con licencia de uso vigente.

EVITAR

2. Instalar herramientas no autorizadas por la organización o sin licencia de os.

5.9.- El correo electrónico

a.- La cuenta corporativa

POTENCIAR

1. El uso de la cuenta corporativa facilitada por la organización
2. Comprobar que el origen del correo sea de un sitio de confianza
3. En caso de duda, en lugar de responder al correo, llamar por teléfono al remitente del mismo.
4. Protegerse ante los malware, como por ejemplo:
    a. Virus.
    b. Phising.
    c. Adware.
    d. Troyanos
    e. Spyware.
    f. Ransomware.
    g. Keylogger.
5. Utiliza el campo CCO para enviar correos electrónicos a múltiples destinatarios.
6. Enviar los mensajes con categorías especiales de datos o con información confidencial protegidos con contraseña.

EVITAR

1. El uso de cuentas personales tipos Gmail, Yahoo!, Hotmail, etc. por temas corporativos o profesionales.
2. Reenviar correos desde la cuenta corporativa al personal o al revés.
3. Enviar información en ficheros adjuntos sin cifrar o sin proteger con contraseña
4. Compartir información sensible.
5. Descargar archivos del tipo .exe, .zip, etc
6. Hacer clic en enlaces sospechosos, que piden descargar adjuntos, que sean urgentes, que incorporen enlaces cortos
    a. Bit.ly

b.- La cuenta personal

POTENCIAR

1. Uso exclusivo de la cuenta personal para enviar y recibir correos estrictamente personales.

EVITAR

1. Enviar o recibir información corporativa con la cuenta personal

5.10.- La documentación en papel

POTENCIAR

1. El registro de la salida y de la devolución de la documentación que el trabajador haga ir con motivo del teletrabajo.
2. El registro de la salida y de la devolución de la documentación que el trabajador haga ir con motivo del teletrabajo.
3. Aplicar el principio de mesa limpia, es decir al finalizar el trabajo, guardar la documentación de manera segura en cajones cerrados.

EVITAR

1. Copiar en un post-it o en papeles información confidencial.
2. Que terceros no autorizados accedan a los documentos.

5.11.- La webcam

POTENCIAR

1. Cerrarla con un mecanismo físico (tapa, adhesivo, etc.) cuando no se utilice.

EVITAR

2. Tenerla abierta si no se utilizar

5.12.- Videollamadas y reuniones virtuales

POTENCIAR

1. Habilitar el uso de contraseñas para evitar el uso o la visualización por parte de terceros no invitados de las conversaciones o los documentos
2. Tener habilitados canales de comunicación rápida con todos los trabajadores.
3. Disponer de la lista de las personas invitadas a la reunión.
4. Habilitar las normas de control a la hora de inicio y de final de la reunión
5. Explicar previamente si la reunión se graba o no. Asegurarse de que se cierra el micrófono y la webcam al finalizar la reunión

EVITAR

1. Dejar los micrófonos o la webcam encendida

5.13.- Copias de seguridad

POTENCIAR

1. Hacer las copias de seguridad según el análisis de riesgo y siguiendo, entre otros, el sistema 3-2-1:
    a. 3 copias de seguridad.
    b. 2 ubicaciones diferentes.
    c. 1 a la nube o cloud.

2. Recuperarlas de forma habitual para comprobar su corrección
3. Protegerlas con contraseña.

EVITAR

1. Que los trabajadores o terceros no autorizados puedan hacer copias de seguridad.

5.14.- Notificación y respuesta ante los incidentes

POTENCIAR

1. La implicación de los trabajadores en la ciberseguridad de la organización.
2. La creación y puesta en marcha de un canal de notificación directa y escrita entre el trabajador y la organización:
   a) Correo electrónico.
   b) Teléfono.
   c) Intranet.
3. La comunicación inmediata y completa de cualquier incidente, sospecha, duda o problema técnico a la organización.
   a) Virus
   b) Pérdida o comportamiento extraño de dispositivos
   c) Altas o bajas de usuarios
   d) Revelación de contraseña a un tercero
4. Utilizar el teléfono 017, que se la línea de ayuda en ciberseguridad de incibe.

EVITAR

1. Hacer las notificaciones solo de forma oral.
2. Guardar silencio ante un incidente o intentar resolverlo sin ayuda de la organización.

5.15.- Formación y comunicación

POTENCIAR

1. La formación a los trabajadores en linea sobre ciberseguridad desde la misma organización.

2. Dar publicidad y comunicar las normas de ciberseguridad a los trabajadores

5.16.- Otros recursos

POTENCIAR

1. Compartir una lista de teléfonos y de correos electrónicos básicos, que sean fácilmente accesible para los trabajadores.
2. Activar servicios de apoyo y de resolución de dudas para configurar los recursos.

6.- Bibliografía

1. Normes de ciberseguretat per a la prestació de serveis en la modalitat de teletreball
   https://ciberseguretat.gencat.cat/ca/detalls/noticia/Normes-de-ciberseguretat-per-a-la-prestacio-de-serveis-en-la-modalitat-de-teletreball

2. Instrucció 3/2018, sobre l'ús de les tecnologies de la informació i la comunicació a l'Administració de la Generalitat de Catalunya
   http://politiquesdigitals.gencat.cat/web/.content/funcio_publica/documents/normativa/circulars_i_instruccions/Instruccio-3-2018_TIC.pdf

3. Coronavirus, ¿cómo podemos ayudarte a trabajar desde casa de manera segura?
   https://www.osi.es/es/cibercovid19

4. Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilància
   https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4691-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia-1/file.html

5. Cómo implantar una política de Acceso Remoto Seguro
   https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/191-abstract-politica-de-acceso-remoto-seguro/file

6. ¿Acceso remoto a la oficina? es posible con VPN
   https://www.incibe.es/protege-tu-empresa/blog/acceso-remoto-oficina-posible-vpn

7. ¿Sabías que utilizar tus dispositivos personales para trabajar puede ser peligroso?
   https://www.osi.es/es/actualidad/blog/2019/05/15/sabias-que-utilizar-tus-dispositivos-personales-para-trabajar-puede-ser