TELETREBALL, PROTECCIÓ DE DADES PERSONALS I SEGURETAT

GUIA DE BONES PRÀCTIQUES PER A LES ORGANITZACIONS

Versió 2.3, data 31-3-2020

MÚTUA INTERCOMARCAL

Índex

1.- Introducció

El teletreball s´ha definit com aquell fenomen que porta el treball al treballador, en lloc del treballador al treball.

La finalitat d´aquesta guia és orientar a les organitzacions, sobre els aspectes legals i de seguretat vinculats amb el teletreball, aplicable tant davant de les actuals circumstàncies com per a les futures opcions per a conciliar la vida laboral amb la familiar dels treballadors.

No podem obviar els riscos que suposa el teletreball i per tant, una de les claus perquè sigui segur passa per reforçar la ciberseguretat, protegir les dades personals i minimitzar els riscos, ja que s´ha observat últimament un notable increment de l´activitat dels ciberdelinqüents.

Per tant, la necessitat d´assegurar la continuïtat del negoci, garantir la seguretat i confidencialitat de les dades i de respectar els drets dels treballadors, entre ells el dret a la desconnexió digital, ens ha portat a preparar aquesta guia adreçada a les organitzacions.

Finalment abans de prendre qualsevol decisió, heu de consultar prèviament amb els vostres assessors laborals, jurídics i tecnològics, i amb el delegat de protecció de dades en cas que disposeu d´aquesta figura, ja que la finalitat d´aquesta guia és purament informativa i no constitueix, en cap cas, assessorament legal o tecnològic.

Dídac Merino i Ramon Arnó

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

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

2.- El teletreball

2.1.- On es regula

A l´estatut dels treballadors (ET), el real decret legislatiu 2/2015, de 23-10, fonamentalment als següents articles:

a.- L´article 13 (treball a distància).

b.- La modificació de l´article 34.8 segons el real decret llei 6-2019, on es reconeix el dret a sol·licitar el treball a distància en els termes que s´estableixin en la negociació col·lectiva.

c.- El conveni col·lectiu aplicable.

d.- El Real Decret-llei 8/2020, de 17 de març de mesures urgents extraordinàries per a fer front al impacte econòmic i social del covid-10.

2.2.- Les característiques

Les principals característiques del teletreball són:

1.- Distància física entre el treballador respecte a la ubicació de l´organització, és a dir que el treball es pot realitzar des del domicili del treballador o des d´altres llocs triats per ell.

2.- Us de tecnologies de la informació per a la interacció treballador – organització.

3.- Normalment és voluntari i reversible.

4.- S´ha de formalitzar per escrit en forma d'annex, entregant el treballador la informació que estableix la directiva 91/553 relativa a l´obligació de l´empresari d´informar el treballador sobre les condicions aplicables al contracte de treball.

5.- Els teletreballadors tenen els mateixos drets que els que presten els seus serveis al centre de treball, entre ells el dret a la formació o a respectar la vida privada del treballador.

3.- La protecció de dades personals

3.1.- En general

La normativa actual és la següent:

a.- El reglament 2016/679 de protecció de dades (RGPD).

b.- La llei Orgànica 3/2018, de Protecció de Dades Personals i garantia dels drets digitals. (LOPDGDD).

3.2.- Les obligacions de l´organització

Les obligacions bàsiques de qualsevol organització o responsable son resumidament les següents:

1. Acreditar una responsabilitat activa i no simplement passiva o reactiva.

2. Mantenir el Registre d'Activitats de Tractament (RAT).

3. Evitar tractar, si no és necessari:
    - Categories especials de dades
        i. com l'origen racial o ètnic, dades de salut, opinions polítiques, afiliació sindical, sobre religió o creences filosòfiques, sobre vida i orientació sexual, violència de gènere, etc.
    - Dades biomètriques
        i. obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física, que permeten o confirmen la identificació única de la persona (imatges facials, dades dactiloscòpiques, etc.).
    - Dades genètiques,
        i. relatives a les característiques genètiques heretades o adquirides d'una persona física, que proporcionen una informació única sobre la fisiologia o la salut d'aquesta persona, obtingudes en particular de l'anàlisi d'una mostra biològica d'aquesta persona.

4. Realitzar una anàlisi de riscos i aplicar les mesures de seguretat adequades.

5. Contractar els encarregats de tractament que siguin diligents i proactius i signar els contractes amb les mesures de seguretat a aplicar

6. Adaptar les clàusules de protecció de dades, l'avís legal i la política de cookies.

7. Aplicar les mesures de protecció de dades des del Disseny i per defecte.

8. Realitzar avaluacions d'impacte (EIPD - PIA), quan sigui necessari.

9. Designar el Delegat de Protecció de Dades (DPD - DPO), quan la normativa ho exigeixi.

10. Notificar els incidents de Seguretat de manera immediata i completa al responsable.

11. Formar el personal.

12. Avaluar les mesures jurídiques, tecnològiques i organitzatives de manera continuada.

3.3.- La regulació dels drets digitals dels treballadors

La LOPDGDD regula els drets digitals als articles 79 a 96, entre ells el dret a la desconnexió digital.

3.4.- El dret a la desconnexió digital en l´àmbit laboral

És el dret del treballador a desconnectar digitalment per garantir fora del temps de treball, el dret al descans i a les vacances així com a la intimitat personal i familiar.

El dret a la desconnexió digital fora de l´horari laboral es regula a diverses normes:

a.- Article 88 de la LOPDGDD.

b.- Article 20 de l´estatut dels treballadors (ET), el real decret legislatiu 2/2015, de 23-10.

c.- Article 14.j.bis del Real Decret Legislatiu 5/2015, de 30 d´octubre, llei de l´estatut bàsic de l´empleat públic.

Alguns exemples d´aquest dret son els següents:

a.- la no obligació de respondre cap comunicació -correu electrònic, WhatsApp, telèfon- una vegada finalitzada la jornada laboral i per tant el dret a no respondre un correu fins a l´inici de la jornada laboral.

b.- les reunions i les formacions no s´allargaran més enllà de la finalització de la jornada laboral, llevat circumstàncies excepcionals.

c.- incloure un missatge d´avis al correu electrònic del tipus “absent” durant les vacances, assumptes propis, permisos, incapacitats, etc.

d.- no s´aplicaran els anteriors supòsits si concorren causes de força major o a aquelles persones que perceben un plus de disponibilitat i que hi han d´estar contínuament disponibles.

e.- aplicable a persones que treballen als locals de l´organització i també els que fan teletreball

f.- realitzar formació als treballadors.

g.- l´organització no podrà sancionar als treballadors que exercitin el seu dret a desconnectar d´acord amb la normativa.

h.- és un dret, no una obligació.

Per tant cal redactar una política interna reguladora. A mode d´exemple podeu fer anar, entre altres, el model que han signat recentment Telefònica i les organitzacions sindicals majoritàries al mes de juliol de 2019:

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

4.- La seguretat i el teletreball

De manera genèrica apuntem les obligacions bàsiques per a les organitzacions i per als treballadors:

4.1.- Les obligacions de seguretat per a les organitzacions

Les organitzacions han de tenir en compte un conjunt de consideracions:

a.- Definir una política de seguretat.

b.- Concretar quins recursos i quines aplicacions estan autoritzades i quines prohibides, així com facilitar les mesures de seguretat.

c.- Proporcionar, instal·lar i mantenir els equipaments necessaris per al teletreball, fins i tot quan el treballador utilitzi el seu propi equip (byod o bring your own device).

d.- Definir quina és la informació secreta, la confidencial i al que es pot compartir.

e.- Regular els perfils dels treballadors, ja que no tots hi han d´accedir a tota la informació, perfils que s´han de concretar de manera individual enlloc d´utilitzar d´usuaris genèrics, a través de la segregació de funcions.

f.- Fer formació al personal.

g.- Acomplir amb la normativa de protecció de dades personals.

h.- Respectar el dret a la desconnexió digital i altres drets digitals dels treballadors.

i.- Valorar la subscripció d´una ciberassegurança.

4.2.- Les obligacions de seguretat per als treballadors

Els treballadors han de tenir en compte un conjunt de consideracions:

a.- Aplicar les mesures de seguretat seguint les directrius de les organitzacions.

b.- Guardar confidencialitat sobre la informació tractada.

c.- Utilitzar els recursos amb finalitats laborals i no personals.

d.- Notificar les incidències ràpidament a l´organització.

e.- Crear un compte d´usuari específic diferent del compte personal o familiar.

5.- Les mesures de seguretat

5.1.- L´anàlisi de risc

Aquí teniu un model bàsic d'autoavaluació que us pot ajudar a tenir una anàlisi de la seguretat de la vostra organització:

https://adl.incibe.es/

5.2.- Els recursos

Els recursos vinculats amb el teletreball són bàsicament els següents:

1. Accés a la xarxa corporativa a través d´un canal segur.
2. Ús d´un canal segur de comunicacions.
3. Les contrasenyes.
4. L´espai de treball segur.
5. Les mesures de seguretat dels recursos:
    a. L´equip de treball és propietat de l´organització (cope).
    b. L´equip de treball és propietat del treballador (byod).
6. El programari.
7. El correu electrònic.
    a. El compte corporatiu.

   b. El compte personal.

8. La documentació en paper.
9. La webcam.
10. Les videotrucades i les reunions virtuals.
11. Les còpies de seguretat.
12. La notificació i resposta davant dels incidents.
13. La formació.
14. Altres recursos

5.3.- Accés a la xarxa corporativa a través d´un canal segur

POTENCIAR

1. La gestió segura dels ports i les aplicacions d´entrada.
2. L'autenticació dels treballadors que accedeixen a la xarxa:
   a. Nom d´usuari i contrasenya.
   b. Certificat digital
2. L´assignació dels permisos en funció del perfil del treballador.
3. Utilitzar vdi (Virtual Desktop Infrastructure).
4. Mantenir la traçabilitat de les connexions i dels registres d´auditoria.

EVITAR

1. L'ús de team viewer o anydesk amb llicència personal i per tant només utilitzar la llicència corporativa.
2. Obrir l´accés directe als treballadors sense cap control.

5.4.- Ús d´un canal segur de comunicacions

POTENCIAR

1. Un canal segur de comunicacions entre el treballador i l´organització:
    a. VPN (Virtual Private Network).
2. Navegar de manera segura per les pàgines web que tinguin xifrat htpps.
3. Activar l´opció de navegació privada
4. Escriure la url o adreça al navegador i fer clic a continuació.
5. En finalitzar la feina, tancar sempre la sessió, és a dir anar al programa que s´utilitza, buscar el menú tancar sessió i executar-lo.
6. Especial atenció als mètodes d´enginyeria social
    a. Trucades urgents
    b. Correus on demanen fer clic a un enllaç o be omplir un formulari
    c. Comunicacions on es sol.liciten dades sobre comptes, targetes de crèdit o contrasenyes.

EVITAR

1. L´ús de webs sense revisar que l´url sigui correcta
    a. Gugle en lloc de google.com
    b. Aple en lloc de apple.com
2. Connectar-se des de wifis públiques sense VPN.
    a. Hotels
    b. Aeroports
    c. Bars
    d. Centres comercials
3. L'ús de canals no segurs.
4. Utilitzar xarxes peer to peer (e-mule, u-torrent, etc)
5. Al finalitzar la feina, deixar la sessió oberta.
6. Fer clics als enllaços a webs, correus o altres missatges desconeguts o sospitosos.

5.5.- Les contrasenyes

POTENCIAR

1. Custodiar de manera segura, utilizant software creat especialment per guardar les contrasenyes.
2. No compartir les contrasenyes ni el certificat digital
3. Crear contrasenyes fortes i complexes per evitar suplantacions d´identitat:

   a. longitud mínima recomanada de 8 caràcters.
   b. combinació de
      i. lletres,
      ii. números
      iii. caràcters especials
4. Limitar a 3 el nombre màxim d´intents fallits d'autenticació.
5. Activar el doble factor d'autenticació.
   a. Enviament al mòbil ´d un codi d´accés
   b. Aconsellable per a outlook, gmail, twiter, linkedin, etc
6. Modificar les claus genèriques dels dispositius:
   a. Encaminador (router) de casa.
7. Obligar a canviar les contrasenyes de forma habitual, sobretot i de manera immediata després del primer accés
8. Custodiar les targetes que incorporin certificats digitals

EVITAR

1. Compartir les contrasenyes.
2. Que tinguin menys de 8 caràcters o siguin fàcils d´endevinar.
   a. 1234
   b. qwerty
3. Apuntar-les a un post-it o en altres documents fàcilment accessibles.
4. Enviar-les per correu electrònic, WhatsApp, etc.
5. Guardar les contrasenyes de forma automàtica si no posar-les cada vegada.

5.6.- L´espai de treball segur

POTENCIAR

1. L'ús d´un espai a casa, que guardi certa separació amb la resta de dependències.
2. Crear un espai de treball segur, amb limitació d'accés a altres persones

EVITAR

1. Treballar en llocs públics amb persones al voltant:
   a. shoulder surfing

5.7.- Les mesures de seguretat dels recursos

En aquest cas cal distingir dos tipus de recursos diferents:

a.- L´equip de treball és propietat de l´organització (cope)

Es coneix com a cope (corporate owned personal enable).

Aquí es l´organització la que es propietària del dispositiu (ordinador, tablet, mòbil, etc).

b.- L´equip de treball és propietat de l´usuari (byod)

Es coneix com a byod (bring your own Device) o uyod (use your own device).

Aquí és el treballador qui és el propietari del dispositiu (ordinador, tablet, mòbil, etc)

Tant si l´equip de treball es propietat de l´organització com si es propietat de l´usuari (byod), les mesures són les següents:

POTENCIAR

1. La creació d´una carpeta del tipus "feina" amb contrasenya d´almenys 8 caràcters, diferent i separada de la carpeta "personal", on guardarem tota la informació professional o corporativa.
2. Actualitzar el sistema operatiu i la resta de programes com navegadors i altres eines amb els darrers pegats de seguretat
3. Instal·lar un antivirus per protegir-se de les amenaces que s´activi automàticament a l´introduir un usb, cd, dvd, etc
4. Evitar l'accés dels familiars als recursos:
    a. digitals
    b. en paper
5. Crear mecanismes que possibilitin esborrar o localitzar els dispositius de manera remota:
    a. En cas de pèrdua o robament.
6. Bloquejar la pantalla del dispositiu quan hi hagi un període d´inactivitat que només es pot desbloquejar amb una contrasenya.
7. Encadenar físicament el dispositiu per evitar el seu robament
8. Esborrar al finalitzar el teletreball
    a. les carpetes de descàrrega,
    b. la paperera
    c. les cookies o galetes
    d. l´històric de navegació

EVITAR

1. Descarregar fitxers o documents amb dades personals en ubicacions:
    a. Sense contrasenya o xifrades.
    b. No autoritzades

   i. Dropbox gratuïts
2. Utilitzar memòries usb (pendrive) o discs externs sense xifrar
3. Compartir els recursos amb tercers sense autorització.
4. Modificar o desactivar la configuració de seguretat

5.8.- El programari

POTENCIAR

1. L'ús d´eines autoritzades per l´organització i amb llicència d´ús vigent.

EVITAR

1. Instal·lar eines no autoritzades per l´organització o sense llicència d´us.

5.9.- El correu electrònic

a.- El compte corporatiu

POTENCIAR

1. L'ús del compte corporatiu facilitat per l´organització.
2. Comprovar que l´origen del correu sigui ´d un lloc de confiança
3. En cas de dubte, en lloc de respondre al correu, trucar per telèfon al remitent del mateix
4. Protegir-se davant del malware, com per exemple:
   a. Virus.
   b. Phising.
   c. Adware.
   d. Troians.
   e. Spyware.
   f. Ransomware.
   g. Keylogger.
5. Utilitzar el camp cco per enviar correus electrònics a múltiples destinataris.
6. Enviar els missatges amb categories especials de dades o amb informació confidencial, protegits amb una contrasenya

EVITAR

1. L'ús de comptes personals tipus gmail, yahoo, hotmail, etc per temes corporatius o professionals.
2. Reenviar correus des del compte corporatiu al personal o a l'inrevés.
3. Enviar informació en fitxers adjunts sense xifrar o sense protegir amb contrasenya
4. Compartir informació sensible.
5. Descarregar arxius del tipus .exe, .zip, etc
6. Fer clic a enllaços sospitosos, que demanen descarregar adjunts, que siguin urgents, que incorporin enllaços curts
    a. Bit.ly

b.- El compte personal

POTENCIAR

1. Ús exclusiu del compte personal per enviar i rebre correus estrictament personals.

EVITAR

1. Enviar o rebre informació corporativa amb el compte personal.

5.10.- La documentació en paper

POTENCIAR

1. El registre de la sortida i de la devolució de la documentació que el treballador faci anar amb motiu del teletreball
2. Si cal destruir la documentació, fer-ho de forma segura.
3. Aplicar el principi de taula neta, és a dir en finalitzar la feina, guardar la documentació de manera segura en calaixos tancats.

EVITAR

1. Copiar en post-it o en papers, informació confidencial.
2. Que tercers no autoritzats accedeixin als documents impresos.

5.11.- La webcam

POTENCIAR

1. Tancar-la amb un mecanisme físic (tapa, adhesiu, etc) quan no es faci anar.

EVITAR

1. Tenir-la oberta si no es fa anar.

5.12.- Videotrucades i reunions virtuals

POTENCIAR

1. Habilitar l'ús de contrasenyes per evitar l'ús o la visualització per part de tercers no convidats de les converses o els documents
2. Tenir habilitats canals de comunicació ràpida amb tots els treballadors.
3. Disposar de la llista de les persones convidades a la reunió.
4. Habilitar les normes de control d´hora d´inici i de final de la reunió
5. Explicar prèviament si la reunió s´enregistra o no.
6. Assegurar-se que es tanca el micròfon i la web cam al finalitzar la reunió.

EVITAR

1. Deixar els micròfons o la webcam oberta.

5.13.- Còpies de seguretat

POTENCIAR

1. Fer les còpies de seguretat segons l'anàlisi de risc i seguint, entre altres, el sistema 3-2-1:
    a. 3 còpies de seguretat.
    b. 2 ubicacions diferents.
    c. 1 al núvol o cloud.
2. Recuperar-les de forma habitual per comprovar la seva correcció
3. Protegir-les amb contrasenya.

EVITAR

1. Que els treballadors o tercers no autoritzats puguin fer còpies de seguretat.

5.14.- Notificació i resposta davant dels incidents

POTENCIAR

1. La implicació dels treballadors en la ciberseguretat de l´organització.
2. La creació i posada en marxa d´un canal de notificació directa i escrita entre el treballador i l´organització:
    a. Correu electrònic.
    b. Telèfon.
    c. Intranet.
3. La comunicació immediata i completa de qualsevol incident, sospita, dubte o problema tècnic a l´organització.
    a. Virus
    b. Pèrdua o comportament estrany de dispositius
    c. Altes o baixes d´usuaris
    d. Revelació de contrasenya a un tercer
4. Utilitzar el telèfon 017, que es la línia d´ajuda en ciberseguretat d´incibe.

EVITAR

1. Fer les notificacions només de forma oral.
2. Guardar silenci davant d´un incident o intentar resoldre´l sense ajuda de l´organització.

5.15.- Formació i comunicació

POTENCIAR

1. La formació als treballadors en línia sobre ciberseguretat des de la mateixa organització.
2. Donar publicitat i comunicar les normes de ciberseguretat als treballadors

5.16.- Altres recursos

POTENCIAR

1. Compartir una llista de telèfons i de correus electrònics bàsics, que siguin fàcilment accessible per als treballadors.
2. Activar serveis de suport i de resolució de dubtes per configurar els recursos.

6.- Bibliografia

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

Versió 2.3, data 31-3-2020.

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

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