PÍNDOLA 28.- TELETREBALL & COVID-19

La situació d'emergència causada pel COVID-19 ha provocat una situació d'excepcionalitat que ha incidit en les relacions laborals, generalitzant de forma excepcional les situacions en que es porten a terme relacions de teletreball.

Més enllà de les obligacions que la normativa laboral estableix hem de tenir en consideració l'establert a la Llei Orgànica 3/2018, de Protecció de Dades Personals i Garantia del Drets Digitals (LOPDGDD), en especial l'establert als articles 87,88, 89 i 90.

En aquests sentit des de l'Oficina del DPD volem fer algunes consideracions des de l'òptica de la protecció de dades:

- Per fer teletreball l'empresa ha de proporcionar tots els medis necessaris a fi que el treballador pugui realitzar la seva tasca de forma segura, així com les directrius de seguretat que ha de seguir, i que han de coincidir amb les indicades de forma presencial però de forma adaptada al teletreball.
- S'ha de garantir el dret a la desconnexió digital, motiu pel que s'haurà d'establir un marc horari flexible dins el qual el treballador haurà de realitzar la seva prestació.
- En cas d'utilitzar sistemes de geolocalització, sempre en el marc de les funcions de control establertes a l'article 20.3 de l'Estatut del treballadors, aquests hauran de ser informats d'aquest tractament de dades, conforme l'establert a l'article 13 del RGPD.
- El treballador realitzarà les seves funcions utilitzant les eines que li ha proporcionat l'empresa a aquest efecte, abstenint-se de tractar informació a través d'equips o dispositius mòbils de propietat personal, excepte en el cas d'estar autoritzat per fer ús de mitjans tecnològics propis.
- Cal utilitzar serveis d'emmagatzemament al núvol i eines col·laboratives que estiguin autoritzades per l'empresa.
- El treballador s'abstindrà d'utilitzar xarxes WiFi públiques pel risc que això suposa.
- El treballador tindrà especial cura de les seves claus d'accés, vigilant de no deixar-les accessibles a tercers.
- El treballador verificarà que ha tancat la sessió quan hagi de deixar momentàniament el seu lloc de treball.
- El treballador quan treballi en espais públics (per exemple cafeteria o zona de coworking) utilitzarà filtres que dificulten la visió de la pantalla per tercers.
- El treballador quan estigui en espais públics serà especialment curós de les seves eines de treball, i de tota aquella documentació que tingui, sent responsable de destruir-la adequadament quan ja no la necessiti.
- L'enviament de mails es realitzarà sempre a través del compte de correu institucional.

De forma complementària a aquestes consideracions, des de la perspectiva de seguretat de les dades es recomana:

1. Doble factor d'autenticació per a accessos remot.
2. Disposar d'un equip de salt bastionat i aïllat des del qual es pugui treballar. L'únic accessible des de la VPN, evitant que els usuaris connectin directament als serveis finals.
3. Estudiar i limitar només els accessos a l'equip de salt i des d'aquest, als recursos necessaris (és possible que s'hagi de aïllar en una vlan per evitar moviments laterals).
4. Es recomana l'ús d'equips corporatius al no poder garantir un mínim de seguretat bàsica amb equips personals no gestionats per l'organització. Els equips han d'estar actualitzats (sistema operatiu, antivirus, endpoint, etc.) i disposar de les mateixes mesures de seguretat que dins de l'organització.
5. Evitar l'ús de split-tunnel per equips no segurs.
6. Controlar l'ús de dispositius externs (USB).
7. Conscienciar l'usuari del risc, i que es presti especial atenció en els correus rebuts.
8. Revisió de registres d'activitat, accessos, connexions per evitar possibles compromisos de credencials (en el cas de no existir MFA), com poden ser accessos remots des d'adreces d'altres països.
9. Protocols de comunicació (telèfon) perquè el usuaris puguin comunicar qualsevol activitat potencialment maliciosa.

Per a més informació:

- Medidas de seguridad para acceso remoto
  https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/191-abstract-politica-de-acceso-remoto-seguro/file
- Principios y recomendaciones básicas en Ciberseguridad
  https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html
- 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

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:

dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/oficina-dpd/
Tel.: 93 553 26 42 (9:00 a 14:00 h.) – *TEMPORALMENT INACTIU*