PÍNDOLA 29.- MOBILITAT I TELETREBALL

L'Agència Espanyola de Protecció de Dades (AEPD) ha publicat unes recomanacions per protegir les dades personals en situacions de mobilitat i teletreball.

La píndola anterior ja va recollir un seguit de recomanacions en matèria de teletreball. Tanmateix, es considera important fer-se ressò d'aquest document de l'AEPD, per tal que en una situació com l'actual es pugui disposar de la màxima informació possible.

L'AEPD inclou recomanacions tant per al responsable del tractament, com per al personal que participa en les operacions de tractament.

En relació amb les **recomanacions per als responsables del tractament** s'inclou:

1. Definir una política de protecció de la informació per situacions de mobilitat.

Cal definir una política específica per situacions de mobilitat, que formi part i es fonamenti en la política de protecció de dades i seguretat de la informació de l'entitat.

Aquesta política ha de recollir les necessitats concretes i els riscos particulars generats per l'accés als recursos corporatius des d'espais que no es troben sota control de l'organització, de definir les responsabilitats i obligacions que assumeixen els i les treballadores, i ha de determinar quines formes d'accés remot es permeten, quin tipus de dispositius són vàlids per a cada forma d'accés i el nivell d'accés permès en funció dels perfils de mobilitat definits.

Derivades de les polítiques establertes, s'ha de dotar al personal de guies funcionals que els donin directrius de protecció de dades i de seguretat de la informació, els informin de les principals amenaces per les que es poden veure afectats quan treballin des de fora de l'organització, i identifiquin un punt de contacte per comunicar qualsevol incident que afecta a dades personals, així com els canals i formats adequats per fer aquesta comunicació.

Així mateix, el personal ha de signar un acord de teletreball que inclogui els compromisos adquirits en el desenvolupament de les tasques en situacions de mobilitat.

2. Escollir solucions i prestadors de servei confiables i amb garanties.

Cal evitar l'ús d'aplicacions i solucions de teletreball que no ofereixin garanties i que puguin donar lloc a l'exposició de dades del personal, interessats i serveis corporatius de l'organització, particularment, mitjançant els serveis de correu i missatgeria.

També cal recórrer a proveïdors i encarregats que ofereixin solucions provades i garanties suficients que evitin l'exposició de les dades personals del personal, interessats i serveis corporatius de l'organització.

Així mateix, cal tenir en compte que si els prestadors de serveis tenen accés a dades personals, tindran la consideració d'encarregats del tractament havent de formalitzar el corresponent acord que ha d'encabir els continguts i termes de l'article 28.3 RGPD.

3. Restringir l'accés a la informació.

Els perfils o nivells d'accés als recursos i a la informació s'han de configurar en funció dels rols del personal, de manera més restrictiva que els concedits en els accessos des de la xarxa interna, i s'han d'aplicar restriccions d'accés addicionals en funció del tipus de dispositiu des del qual s'accedeixi a la informació i depenent també de la ubicació des de la que s'accedeix.

4. Configurar periòdicament els equips i dispositius emprats en les situacions de mobilitat.

Els servidors d'accés remot han de ser revisats i cal assegurar que estan correctament actualitzats i configurats per garantir el compliment de la política de protecció de la informació per situacions de mobilitat establerta per l'organització, així com el control dels perfils d'accés definits.

Els equips corporatius emprats han:

- d'estar actualitzats;
- tenir deshabilitats els serveis que no siguin necessaris;
- tenir una configuració fixada pels serveis TIC que no pugui ser desactivada ni modificada pel treballador;
- instal·lar únicament les aplicacions autoritzades per l'organització;
- comptar amb software antivirus actualitzat;
- disposar d'un tallafocs local activat;
- tenir activades només les comunicacions (wifi, bluetooth, NFC, etc) i ports necessaris per dur a terme les tasques assignades; i
- incorporar mecanismes de xifrat de la informació.

Si es permet l'ús de dispositius del personal, com suposen un risc més gran per no incorporar els mateixos controls dels equips corporatius, a més a més d'exigir uns requisits mínims per poder emprar-los en l'establiment de connexió remotes, cal valorar la possibilitat de restringir la connexió a una xarxa segregada que només proporcioni un accés limitat a aquells recursos que s'hagin identificat com menys crítics i sotmesos a menor nivell de risc.

5. Monitoritzar els accessos realitzats a la xarxa corporativa des de l'exterior.

S'han d'establir sistemes de monitorització encaminats a identificar patrons anormals de comportament amb l'objectiu d'evitar la propagació de malware per la xarxa corporativa i l'accés i ús no autoritzat de recursos. La seva configuració ha de ser revisada i actualitzada de manera periòdica.

Així mateix, els mecanismes de monitorització implementats han de respectar els drets digitals establerts en la LOPDGDD, en particular, al dret a la intimitat i ús de dispositius digitals i el dret a la desconnexió digital en l'àmbit laboral, i s'ha d'informar al personal sobre l'existència i l'abast d'aquestes activitats de control i supervisió.

6. Gestionar racionalment la protecció de dades i la seguretat.

Les mesures i garanties que s'implementin han d'establir-se a partir d'un anàlisi de riscos en què s'avaluï la proporcionalitat entre els beneficis a obtenir d'un accés a distancia i l'impacte potencial de veure compromès l'accés a la informació de caràcter personal.

Cal planificar i avaluar les aplicacions i solucions d'accés remot tenint en compte els principis de privacitat des del disseny i per defecte al llarg de totes les etapes de desplegament de la solució: des de la definició dels requisits i necessitats fins a la retirada de la solució o d'algun dels seus components.

En relació amb les **recomanacions per al personal que participa en les operacions de tractament:**

1) **Respectar la política de protecció de la informació en situacions de mobilitat definida pel responsable**, així com la resta de les normes i procediments que la desenvolupin, incloent el deure de confidencialitat del personal.

   Les recomanacions al personal han d'estar recollides en la política de teletreball del responsable, referenciades en l'acord de teletreball i ajustades a la situació concreta de les tasques a realitzar.

2) **Protegir el dispositiu emprat en mobilitat, així com el seu accés**

   El treballador ha de tenir en compte i adoptar mesures de protecció del dispositiu com: definir i emprar contrasenyes d'accés robustes i diferents a les emprades per accedir als àmbits personals; no s'ha de descarregar ni instal·lar aplicacions o software que no hagi estat prèviament autoritzats per l'organització; evitar la connexió dels dispositius a la xarxa corporativa des de llocs públics a xarxes wifi obertes no segures; mantenir protegits els mecanismes d'autenticació definits per validar-se en els sistemes de control d'accés remot de l'organització, tenir operatiu i actualitzat el sistema antivirus instal·lat en l'equip, verificar la legitimitat dels correus electrònics rebuts comprovant que el domini electrònic del que provenen és vàlid i conegut, i desconfiant de la descàrrega de fitxers adjunts amb extensions inusuals o connexions estranyes.

   Si es disposa d'un equip corporatiu, no s'ha d'utilitzar amb finalitats particulars, i si l'equip emprat és personal cal evitar simultaniejar l'activitat personal amb la professional i definir perfils independents per desenvolupar cada tipus de tasca.

   Convé desactivar les connexions wifi, bluetooth i similars que no estiguin essent utilitzades, en el cas que puguin ser gestionades per la persona treballadora, i desconnectar la sessió de l'accés remot i apagar o bloquejar l'accés al dispositiu, al finalitzar la tasca.

3) Garantir la protecció de la informació que s'està tractant

Cal adoptar les mesures de precaució necessàries per garantir la confidencialitat de la informació que s'està gestionant, tant si es treballa en llocs públics com en un entorn domèstic. En aquest sentit, és important: no deixar a la vista informació personal en llocs on es dugui a terme el teletreball bloquejant les sessions dels dispositius quan estiguin desatesos; evitar exposar la pantalla a la mirada de tercers; i si es treballa habitualment en llocs públics, es recomanable utilitzar un filtre de privacitat per a la pantalla; evitar que es puguin escoltar converses per part de tercers aliens; i extremar les precaucions en la gestió del suport paper per tal d'evitar accessos no autoritzats.

4) Guardar la informació en els espais xarxa habilitats

És convenient evitar emmagatzemar de manera local en el dispositiu emprat la informació generada. És preferible emprar recursos d'emmagatzematge compartits o en el núvol proporcionats per l'organització i, si s'utilitzen equips personals, no emprar aplicacions per compartir informació no autoritzades per l'entitat. Tampoc s'ha de bloquejar o deshabilitar la política de còpia de seguretat corporativa definida per a cada dispositiu.

Es recomanable revisar i eliminar periòdicament la informació residual que pot quedar emmagatzemada en el dispositiu, com arxius temporals del navegador o descàrregues de documents.

5) Si hi ha sospita de què la informació s'ha pogut veure compromesa, comunicar immediatament la violació de seguretat

Qualsevol anomalia que pugui afectar a la seguretat de la informació i a les dades personals tractades ha de notificar-se al responsable, a la major brevetat possible, a través dels canals establerts a aquest efecte. També pot consultar amb el delegat del protecció de dades i amb el responsable de seguretat de la informació, o els perfils de responsables designats a aquest efecte, traslladant-los tota la informació d'interès de la que tingui constància.

Per a més informació:

- Recomendaciones para proteger los datos personales en situacions de movilidad y teletrabajo AEPD

  https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo.pdf

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*