Pla de contingències per fer front al Coronavirus SARS-Cov-2 i Tractament de dades personals a l'ASM Horta Guinardó

Els tractaments de dades personals, tot i estar en situacions d'emergència sanitària i declaració d'Estat d'Alarma, s'han de seguir tractant de conformitat amb la normativa de protecció de dades personals (RGPD i Ley Orgánica 3/2018), i per tant li son d'aplicació els seus principis, i entre ells el de tractar les dades amb licitud, lleialtat i transparència, limitació de la finalitat (en aquest cas, salvaguardar els interessos de les persones en situació de pandèmia), principi d'exactitud i el principi de minimització de dades. Sobre aquest últim, es fa referència expressa a que les dades tractades hauran de ser exclusivament limitades a les necessàries per a la finalitat pretesa, sense que pugui estendre dit tractament a altres dades personals no necessàries per la finalitat.

El Real Decret 463/2020, de 14 de març, te com a conseqüència el confinament de determinats sectors, el que dona pas a situacions de mobilitat i teletreball.

L'ASM Horta Guinardó, com a responsable del tractament, pren la decisió de que determinades activitats de l'entitat s'executin en situació de mobilitat i teletreball seguint les recomanacions emeses des de l'Agència Espanyola de Protecció de Dades (AEPD) per a protegir les dades personals i que per les circumstàncies d'urgència obliguen la posada en marxa de solucions amb caràcter provisional.

En definitiva, l'ASM Horta Guinardó i els seus empleats que es troben en situació de teletreball han estat informats i han de seguir les actuacions realitzades.

ACTUACIONS REALITZADES

1. Es defineix una política de protecció de la informació per a situacions de mobilitat

Basada en la política de protecció de dades i seguretat de la informació de l'Entitat, es defineix política específica per a situacions de mobilitat que recull les necessitats concretes i riscos particulars introduïts per l'accés als recursos corporatius des d'espais que no es troben sota el control de la organització.

S'ha determinat quines formes d'accés remot es permeten, que tipus de dispositius són vàlids per a cada forma d'accés i el nivell d'accés permès en funció dels perfils definits. També s'han definit les responsabilitats i obligacions que assumeixen les persones treballadores. *(Veure annex al final d'aquest document: Decàleg del teletreball a les persones treballadores)*

S'han proporcionat guies funcionals adaptades a formar a les persones treballadores derivades d'aquesta política així com formació externa en matèria de protecció de dades i teletreball. *(Veure annexes al final d'aquest document: Manual per trucar amb número oculto; Manual per la instal·lació de la VPN)*

Les persones treballadores han estat informades de les principals amenaces per les que es poden veure afectades al treballar des de fora de l'organització i les possibles conseqüències que poden materialitzar-se si no es segueixen les recomanacions indicades. *(Veure annexes al final d'aquest document: Informació de ciberseguretat i Informació dels possibles atacs i virus)*

Es posa a disposició el contacte del Responsable d'Informàtica i Delegada de Protecció de Dades per comunicar qualsevol incidència que afecti a dades de caràcter personal o situacions que puguin representar un risc per a la protecció de la informació i recursos corporatius, així com els canals i formats adequats per a realitzar la comunicació.

El personal ha signat un acord de teletreball que inclou els compromisos adquirits al desenvolupar les seves tasques en situació de mobilitat, mesures de seguretat i confidencialitat que s'han d'adoptar en el lloc de teletreball, com es protocol·litzaren les comunicacions amb la persona treballadora, quines mesures de prevenció de riscos laborals s'han d'adoptar, quin us farà l'empresa de les dades de la persona treballadora, la duració del mateix i el sistema de control de la jornada. *(Veure annexes al final d'aquest document: Instruccions prevenció teletreball i Autoavaluació teletreball)*

2. Es tria solució i prestador de servei confiable amb garanties.

Mitjançant una xarxa privada virtual - VPN (*Virtual Private Network*) es connecten els equips de les persones treballadores en situació de mobilitat al servidor de domini d'usuaris CSMA Horta. El servidor es inaccessible des de fora de la xarxa per a qualsevol equip o persona que no té configurada la VPN.

Les persones treballadores en situació de mobilitat i que necessiten aquest servei tenen instal·lada la configuració de la VPN en el seus equips de treball. Aquesta VPN fa una connexió encriptada i directa punt a punt entre equip i servidor.

Tots els servidors estan darrere d'un tallafocs (Firewall) físic el qual protegeix la xarxa interna.

S'evita així utilitzar aplicacions i solucions de teletreball que no ofereixen garanties i que poden donar lloca a l'exposició de les dades personals de les persones treballadores, interessats i serveis corporatius de la organització, en particular, mitjançant el serveis de correu i missatgeria.

3. Es restringeix l'accés a la informació.

Els perfils o nivells d'accés als recursos i a la informació s'han configurat en funció dels rols de cada persona treballadora, d'una forma inclús més restrictiva respecte dels atorgats en els accessos des de la xarxa interna. Es mantenen els rols i permisos de Windows establerts en situació d'activitat normal.

Una vegada finalitzada la jornada laboral en situació de mobilitat cal desconnectar la sessió d'accés remot i apagar o bloquejar l'accés al dispositiu.

4. Es configuren i actualitzen periòdicament els equips i dispositius utilitzats en les situacions de mobilitat.

Els serveis d'accés remot han estat revisats i correctament actualitzats i configurats per a garantir el compliment de la política de protecció de la informació per a situacions de mobilitat establerta per l'organització, així com el control dels perfils d'accés definits.

Els equips corporatius utilitzats com clients es troben actualitzats a nivell d'aplicació i sistema operatiu, i/o tenen des habilitats els serveis que no són necessaris. No s'han de descarregar ni instal·lar aplicacions o software que no hagi estat prèviament autoritzats per l'entitat.

S'ha permès l'ús de dispositius personals de les persones treballadores donada la situació d'emergència, tot i que això suposi un major risc per no incorporar els mateixos controls dels equips corporatius, s'han exigit uns requisits mínims per a poder fer-ne us en el establiment de connexions remotes. En aquells dispositius personals que no compleixen els requisits mínims el Responsable d'Informàtica ha facilitat la instal·lació de programes d'antivirus i/o Firewall actualitzats.

La persona treballadora ha de definir i fer servir contrasenyes d'accés segures i diferents a les que fa servir per accedir a correus personals, xarxes socials i altres tipus d'aplicacions en l'àmbit de la seva vida personal.

La informació es guarda en els espai de xarxa habilitats, convé evitar l'emmagatzematge de la informació generada durant la situació de mobilitat de forma local en el dispositiu que es fa servir, es recomana fer us dels recursos d'emmagatzemat compartits.

La persona treballadora en situació de mobilitat ha de revisar i eliminar periòdicament la informació residual que pugui quedar emmagatzemada en el dispositiu com arxius temporals del navegador o descarregues de documents.

5. Es monitoritzen els accessos realitzats a la xarxa corporativa des de l'exterior al programa de gestió informàtic de pacients (HC)

En el programa de gestió informàtic de pacients existeix un sistema de monitorització encaminat a identificar patrons anormals de comportament en el tràfic de xarxa cursat dintre de la solució d'accés remot i mobilitat amb l'objectiu d'evitar la propagació de *malware* per la xarxa corporativa i l'accés i ús no autoritzat de recursos.

6. Es gestiona racionalment la protecció de dades i la seguretat.

Les mesures i garanties establertes en les polítiques definides s'han establert a partir d'un anàlisis de riscos en el que s'ha pogut avaluar la proporcionalitat entre els beneficis a obtenir d'un accés a distància i l'impacte potencial de veure compromès l'accés a la informació de caràcter personal. *(Extret Document Alba: "Si que hem realitzat valoracions prèvies amb els professionals disponibles i relacionats amb la matèria: Delegada de Protecció de Dades de l'entitat, Tècnic informàtic i Responsable de l'Entitat amb el suport de Codi Tipus de la Unió Catalana d'Hospitals – UCH")*

En la política s'han contemplat els procediments interns ja establerts per aprovisionar i auditar els dispositius clients d'accés remot, els procediments d'administració i monitorització de la infraestructura, els serveis proporcionats per encarregats (de tractament) i la forma en que la política es revisada i actualitzada als riscos existents.

Els recursos (programari) que poden ser accedits s'han limitat en funció de la valoració de risc que representi una pèrdua del dispositiu client i l'exposició o accés no autoritzat de la informació manegada.

Es garanteix la protecció de la informació amb la que s'ha de treballar, les persones treballadores han d'adoptar les precaucions necessàries per a garantir la confidencialitat de la informació que s'està gestionant.

Si habitualment es genera i treballa amb paper, durant situacions de mobilitat es important minimitzar o evitar l'entrada i sortida de documentació en aquest suport i extremar les precaucions per evitar accessos no autoritzats per part de tercers. La informació en paper no es pot "desechar" sense garantir que es adequadament destruïda (ex: no llençar fulls sencers o en trossos a les escombraries domèstiques).

Convé extremar les precaucions per evitar l'accés no autoritzats a la informació personal, pròpia i de tercers, no deixant a la vista cap suport d'informació en el lloc on es desenvolupi el teletreball bloquejant els dispositius quan estiguin desatesos. En la mesura que sigui possible es aconsellable prevenir que es puguin escoltar converses per part de terceres persones alienes.

7. Es realitza seguiment i avaluació del teletreball i, si s'escau, modificació de les mesures de seguretat.

Validat per Responsable de Tractament: Alicia Roig **Data:** 18/3/2020	**Validat per Encarregada de Tractament:** Maribel Gonzalez **Data:** 18/3/2020