

TELETREBALL. Decàleg de consideracions a tenir en compte

Arran de la situació actual relacionat amb l'emergència sanitària derivada del COVID-19, el teletreball pot ser una opció professional en un entorn diferent de l'habitual i mitjançant dispositius que no són els que habitualment utilitzem.

Tot això no implica que es relaxin les normes i criteris que estableix el Reglament General de Protecció de Dades, més enllà d'a i els dubtes que genera la LOPD en tot això, enviem un escrit de les mesures de seguretat que hauríem d'aplicar tots els que desenvolupin les taques de teletreball.

Decàleg de consideracions a tenir en compte
1- Treballar a través de la VPN que connecta de forma segura amb els servidors de la nostra entitat. Els professionals es descarreguen l'Ekon des de la Intranet i mitjançant la VPN l'equip de l'usuari estarà en la nostra xarxa i tota la informació passarà a través del nostre Firewall.
2- No desar el usuari i la contrasenya de la VPN guardada al ordinador, és a dir, "memoritzada" perquè no la tinguem que escriure cada cop que accedim.
3- No emprar xarxes públiques, connectar el dispositiu a la Wifi privada
4- Mantenir la privacitat de les dades que es poden mostrar des del monitor. Evitar que terceres persones puguin visualitzar les dades personals que tractem en virtut de les nostres tasques.
5- Que tots els dispositius disposin de contrasenya d'accés al dispositiu.
6- Bloquejar sempre la sessió de treball en cas d'absència, encara que sigui puntual. Evitar l'accés no autoritzar a la informació o recursos per part de familiars o amics.
7- No utilitzar les memòries USB, són una possible porta a les infeccions de malware.
8- NO INSTALAR APLICACIONS O UTILITZAR EL NAVEGADOR PER PÀGINES NO SEGURES EN EL DISPOSITIU QUE UTILITZIS PEL TELETREBALL
9- Tancar la sessió de la VPN quan finalitzis el teletreball
10- Emprar els mecanismes habilitats institucionalment per a l'intercanvi de la informació (ekon, e-mail corporatiu i intranet)
11- Eliminar cada dia que es realitzi teletreball <ul style="list-style-type: none">• La informació temporal en carpetes de descarrega• La informació esborrada a la carpeta de reciclatge• Esborra l'historial de navegació• NO GUARDAR CONTRASENYES RECORDADES I SI S'HAN GUARDAT ESBORRAR.
12- Si equip es personal, crea un perfil professional de Microsoft
13- Comunicar qualsevol incidència INMEDIATAMENT en matèria de protecció de dades a la Delegada de Protecció de dades i/o la Responsable de Direcció de l'ASM Horta Guinardó.

La protecció de dades no s'ha d'utilitzar per obstaculitzar o limitar l'efectivitat de les mesures que adoptin les autoritats, especialment les sanitàries, en la lluita contra la pandèmica. Això no vol dir que no haguem de prendre mesures de seguretat en matèria de protecció de dades.

Per qualsevol dubte contacteu amb l'informàtic o la delegada de protecció de dades a través dels correus electrònics alopezosa@asmhg.com, agarciavalls@asmhg.com