Teletreball cibersegur
SENSIBILITZACIÓ PER PERSONAL DE SALUT

CONFIDENCIALITAT DE LES DADES

Has de ser reservat amb les dades confidencials, documents, metodologies, anàlisi, programes i documentació que generis per complir el tractament de dades personals del SISCAT.

DISPOSITIUS CORPORATIUS CUSTODIATS

Utilitza dispositius corporatius (més que no personals), i en la mesura del possible, no barregis fitxers de dades de treball amb els d'ús particular. Custodia'ls sempre en llocs segurs i xifra el contingut (disc dur o targeta de memòria) per protegir la informació en cas de pèrdua.

SERVIDORS I SISTEMES D'EMMAGATZEMATGE

Utilitza únicament els servidors, aplicacions, intranet, xarxa corporativa i altres sistemes d'emmagatzematge indicats pel SISCAT per tenir traçabilitat de fitxers amb dades de caràcter personal o confidencials. Evita guardar i compartir informació en suports locals. Tanca la sessió o desconnecta't en acabar la teva feina.

BLOQUEJA LA SESSIÓ I EVITA ACCÉS DE TERCERS

Bloqueja la pantalla (WINDOWS+L) si treballes en un espai compartit (sempre amb les condicions de distanciament social) i no desis documentació impresa a l'abast de tercers. No permetis l'accés a les dades personals o a informació confidencial a persones no autoritzades.

ACTUALITZACIÓ DE SISTEMA I PROGRAMES

Deixa actualitzar l'antivirus i antimalware a diari. En reiniciar la màquina deixa que el sistema operatiu i aplicacions utilitzades es posin al dia. Intenta mantenir sempre un navegador actualitzat a l'última versió per consultar informació a pàgines web i serveis d'Internet, i usa el navegador i connexió que t'indiqui el SISCAT per accedir a les aplicacions.

SUPORTS EXTERNS O ENVIAMENT DE DOCUMENTS

En cas d'haver de transportar suports o enviar documents que continguin dades de caràcter personal sensibles cal xifrar les dades. Mai facis servir sistemes no autoritzats pel SISCAT.

CONTRASENYES PROTEGIDES

Tens credencials d'accés personals i cal mantenir-les en secret. No comparteixis cap contrasenya personal ni cap codi de seguretat. No permetis que les recordin els navegadors i utilitza'n de diferents per l'àmbit professional i personal. La contrasenya segura és llarga, conté majúscules, números i símbols especials.

CONNEXIÓ SEGURA

Usa una connexió segura, millor el 4G que wifis obertes/gratuïtes. Els wifi de casa normalment xifren, però pot ser un xifrat feble. Per això, sempre que sigui possible:

- Que hi hagi https al navegador en enviar dades personals des d'una web.
- Evita l'intercanvi d'informació sensible (per exemple, per correu electrònic) si no ha estat xifrada prèviament.

ATENCIÓ AMB ELS CORREUS ELECTRÒNICS

Estigues alerta amb els correus electrònics que parlen de COVID19. Estan actives moltes campanyes de *phishing* i *ransomware* que aprofiten la situació per infectar amb malware els dispositius i cal posar sota sospita tots els correus electrònics. No cliquis enllaços ni obris adjunts de correu sospitosos. Contacta amb el Centre de Suport davant de qualsevol comunicació estranya.

COMPTE AMB COMPARTIR EN CANALS PÚBLICS

No comparteixis URLs de les reunions virtuals a missatgeria instantània, xarxes socials o altres canals públics. Sense voler pots donar accés a tercers no autoritzats a reunions privades.

REPORTA ELS INCIDENTS

Notifica qualsevol incidència de seguretat de la qual puguis tenir coneixement al Centre de Suport assignat.

Generalitat de Catalunya
S/Sistema de Salut de Catalunya
Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya