

MANUAL DE BONES PRÀCTIQUES EN MATÈRIA DE PROTECCIÓ I SEGURETAT DE LES DADES PERSONALS

Aplicable a la Fundació Germà Benito Menni, CET El Pla, CET Intecserveis i Empresa Inserció i a les persones treballadores, col·laboradores, en pràctiques o voluntàries.

MESURES INFORMÀTIQUES

1. L'accés als sistemes i aplicacions s'ha de demanar pel circuit establert i s'ha d'ajustar a les funcions de cada persona.
2. L'usuari, la contrasenya i el doble factor són personals. No es poden compartir, ni tan sols amb companys o responsables.
3. Si una contrasenya pot ser coneguda per una altra persona, s'ha de canviar i comunicar-ho immediatament.
4. Només es pot consultar la informació necessària per a la feina assignada. Està prohibit accedir a dades per curiositat o interès personal.
5. Cal evitar que persones no autoritzades vegin la pantalla. En abandonar el lloc, s'ha de bloquejar manualment la sessió.
6. En acabar la jornada, s'han de tancar les aplicacions, guardar la informació al repositori corporatiu i finalitzar la sessió.
7. No es poden instal·lar programes, aplicacions, extensions, macros o serveis al núvol sense autorització.
8. No es poden connectar USB, mòbils o dispositius personals o desconeguts. Els suports autoritzats amb dades sensibles han d'estar protegits.
9. La pèrdua o el robatori d'un ordinador, mòbil, targeta, clau o suport s'ha de comunicar immediatament.

TRACTAMENT DE DADES I FITXERS

10. Les dades s'han de guardar a les aplicacions i carpetes corporatives previstes. No s'han de conservar en comptes personals o al disc local.
11. Els fitxers Word, Excel o similars només es poden crear si són necessaris, amb les dades mínimes i accessos limitats.
12. No es poden crear llistes, formularis, bases de dades o arxius paral·lels sense seguir el procediment intern.

TRACTAMENT DE DADES I FITXERS, CONTINUACIÓ

- 13.** Quan acaba la finalitat d'un fitxer de treball, s'han d'eliminar les còpies temporals i conservar només la versió que correspongui.
- 14.** Formar part de la mateixa Fundació no permet compartir dades lliurement entre CET El Pla, CET Intecserveis o altres entitats. Cal comprovar finalitat, necessitat, destinatari i canal.
- 15.** Les dades personals no es poden utilitzar en formacions, estudis, recerca o publicacions sense el procediment i les garanties corresponents. Sempre que es pugui, s'han d'utilitzar dades anònimes.

CORREU ELECTRÒNIC, INTERNET I COMUNICACIONS

- 16.** El correu corporatiu és per a finalitats professionals. No es poden enviar dades des d'un compte personal ni reenviar-les a una bústia privada.
- 17.** Abans d'enviar, cal revisar el destinatari, les còpies, l'adjunt i les dades incloses. En enviaments múltiples externs, s'ha d'utilitzar CCO quan les adreces no hagin de ser visibles.
- 18.** Quan sigui possible, s'ha de compartir un enllaç corporatiu amb permisos limitats en lloc d'un adjunt. La informació sensible s'ha de protegir.
- 19.** No es poden enviar dades laborals, socials, sanitàries o identificatives per WhatsApp personal, xarxes socials o serveis no autoritzats.
- 20.** No es poden descarregar programes sense llicència, fitxers sospitosos o continguts aliens a la feina que puguin afectar els sistemes.
- 21.** Les eines d'intel·ligència artificial només es poden utilitzar si estan autoritzades. No s'hi poden introduir expedients, dades de salut, discapacitat, informació psicosocial, contrasenyes o informació confidencial.
- 22.** Els resultats de la IA s'han de revisar. No es poden prendre decisions sobre persones basant-se només en una resposta automatitzada.

DOCUMENTS EN PAPER I ESPAIS DE TREBALL

- 23.** Els documents amb dades s'han de guardar en armari, calaixos o espais protegits. No s'han de deixar a la vista en taules, vehicles o zones comunes.
- 24.** Els documents impresos s'han de retirar immediatament de la impressora, fotocopiadora o escàner.
- 25.** El paper inservible o duplicat s'ha de destruir amb destructora o contenidor confidencial. No es poden destruir originals sense autorització.
- 26.** La sortida de documents o suports fora de les instal·lacions ha d'estar justificada, autoritzada i protegida durant el transport.

DADES DE SALUT, DISCAPACITAT I INFORMACIÓ PSICOSOCIAL

- 27.** Les dades de salut, discapacitat i situació psicosocial només poden ser consultades pels professionals que les necessiten per a funcions de prevenció, suport o inclusió laboral.
- 28.** La informació s'ha de registrar de manera objectiva, respectuosa, actualitzada i limitada al necessari. No s'hi poden incloure rumors, etiquetes o opinions personals.
- 29.** La documentació mèdica detallada correspon al servei sanitari. L'entitat ha de rebre, com a regla general, la conclusió d'aptitud i les mesures preventives, no el diagnòstic complet.
- 30.** No s'ha de comunicar el diagnòstic o el motiu mèdic d'una absència a l'equip. S'han d'utilitzar expressions neutres com "absència" o "no disponible".
- 31.** La història social, la documentació de l'USAP o unitat de suport i l'itinerari sociolaboral s'han de conservar separats de l'expedient laboral ordinari i amb accessos restringits.
- 32.** En una coordinació amb serveis sanitaris, socials o administracions, cal comprovar destinatari, finalitat, dades mínimes i canal segur.
- 33.** La informació s'ha de facilitar a la persona treballadora de manera clara i accessible. Si intervé representació legal, cal comprovar-ne l'abast i informar també la persona sempre que sigui possible.

IMATGES, IDENTIFICACIÓ, CONTROL HORARI I VIDEOVIGILÀNCIA

- 34.** Les fotografies i les dades identificatives només es poden utilitzar per a les finalitats autoritzades. No es poden publicar imatges del lloc de treball o de persones en perfils personals.
- 35.** No es poden fer fotografies o gravacions amb dispositius personals. Quan siguin necessàries per a la feina, s'han d'utilitzar els dispositius i els procediments autoritzats.
- 36.** Les targetes identificatives, d'accés o de control horari són personals. No es poden prestar ni utilitzar per registrar l'accés o la jornada d'una altra persona.
- 37.** Només el personal autoritzat pot accedir a les imatges de videovigilància. Està prohibit consultar-les per curiositat, copiar-les o compartir-les, així com tocar, moure, cobrir, desconnectar o manipular les càmeres. Qualsevol petició d'accés o incidència s'ha de comunicar a la persona responsable.

CLAUS, PORTES I ACCÉS FÍSIC

- 38.** Les portes d'espais amb documents o equips s'han de mantenir tancades quan no hi ha personal autoritzat.
- 39.** No es poden fer còpies de claus o targetes pel compte propi. La pèrdua s'ha de comunicar immediatament.

INFORMACIÓ A TERCERES PERSONES

- 41.** No es pot facilitar informació per telèfon, correu o presencialment sense verificar la identitat i l'autorització de la persona sol·licitant.
- 42.** Les sol·licituds d'accés, rectificació, eliminació, oposició o altres drets s'han de derivar al canal de privacitat o al DPD. No s'han d'eliminar dades pel compte propi.
- 43.** Els proveïdors només poden accedir a les dades necessàries per al servei contractat i segons les instruccions de l'entitat. No es poden contractar eines pel compte propi.

INCIDÈNCIES DE SEGURETAT

- 44.** S'ha de comunicar immediatament qualsevol pèrdua, enviament equivocat, accés indegut, document abandonat, contrasenya exposada, virus, publicació accidental o permís excessiu.
- 45.** Davant una incidència, cal aturar o limitar l'acció si és possible, sense destruir correus, registres o altres proves.
- 46.** La comunicació ha d'indicar què ha passat, quan, quines dades hi havia, qui pot estar afectat, qui hi ha pogut accedir i quines mesures inicials s'han pres.
- 47.** No s'ha d'esperar a tenir tota la informació. Comunicar ràpidament és actuar correctament; ocultar o retardar pot augmentar les conseqüències.

FINALITZACIÓ DE LA RELACIÓ I CONFIDENCIALITAT

- 48.** Quan una persona canvia de funció o entitat, s'han de revisar els seus accessos i retornar la documentació que ja no necessita.
- 49.** En finalitzar la relació, s'han de retornar equips, claus, targetes, documents i suports. No es poden conservar còpies, contactes o correus en comptes personals.
- 50.** El deure de confidencialitat es manté després de finalitzar la relació laboral, professional, de pràctiques o voluntariat.

RECORDATORI FINAL

En cas de dubte, no improvisis: atura't i consulta el teu responsable, Sistemes, Recursos Humans o el Delegat/da de Protecció de Dades, segons la situació.

Canal d'incidències: _____ DPD: hospitalbarcelona.dpd@sjd.es

Nom i cognoms: _____

Data i signatura: _____

La signatura acredita la recepció i comprensió del manual. No implica un consentiment general per al tractament de dades personals.