Bones pràctiques digitals per al treball amb menors

Material elaborat amb el suport de:

Introducció

Les eines digitals s'han convertit en una part intrínseca del desenvolupament de qualsevol treball. L'adopció massificada d'aquestes des de principis de segle, no només ha obert la porta a una gran quantitat de possibilitats, tant en l'automatització com en la facilitació de certes tasques diàries, sinó que també ha generat nous reptes, i l'exposició dels usuaris no tècnics a un gran banc de nous coneixement i eines. Aquestes eines, a més, tenen la particularitat i dificultat afegida d'estar en una evolució contínua, tant en el terreny purament tecnològic, com en l'àmbit legal que l'envolta i que la majoria de vegades es troba un pas enrere.

En els últims anys, el Reglament General de Protecció de Dades (RGPD o *GDPR*), s'ha alçat com a norma reguladora principal dels drets i la normativa digital a la Unió Europea; tot i això, molts dels aspectes que s'hi cobreixen són desconeguts per la majoria d'usuaris. A més, el treball amb infància requereix una consideració especial en ser el col·lectiu un vulnerable, i, per tant, requereix una protecció especial.

La finalitat d'aquest manual, doncs, és la de dotar a usuaris, associacions i professionals que treballen amb menors, de diferents pautes i recomanacions que els permeten utilitzar les eines tecnològiques de manera coherent amb l'acció educativa que s'estiga duent a terme, així com en la protecció i defensa dels drets de la infància. Aquests criteris, tot i tenir en especial consideració les persones menors d'edat, no són d'estricta aplicació en l'àmbit de la infància, sinó que poden ser extensives a totes aquelles entitats i organitzacions que vulguen fer servir les eines digitals d'una manera ètica i segura per a totes les persones que en formen part.

Glossari de tecnicismes:

- **Cookie**: Una *cookie* o galeta és un fitxer creat per una pàgina web per emmagatzemar informació a l'ordinador de l'usuari. Aquesta informació pot contenir dades identificatives, claus d'accés, o les preferències d'ús d'una pàgina concreta.

- **Programari lliure**: El Programari Lliure és un tipus de programari que respecta la llibertat dels usuaris. En aquesta tipologia de programes, els usuaris tenen la llibertat d'executar, copiar, distribuir, estudiar, canviar i millorar el programari. Davant la facilitat d'associar aquests programes amb la seua gratuïtat la majoria de vegades, cal remarcar que el concepte *free software* o programari lliure és una qüestió de llibertat, no de preu.

- **Open source**: El concepte fa referència a programari que té el seu codi obert i accessible per a tothom que el vulga llegir i manipular. La majoria de programes *open source* són també de programari lliure, tot i que això no es compleix en la totalitat dels casos.

- **Extensió (de navegador)**: Complement que s'instal·la en el navegador o explorador web, i que n'amplia la seua funcionalitat.

- **Sistema operatiu**: sistema base de programari que controla el funcionament d'un ordinador, i que, entre altres coses, permet interactuar als usuaris, fa possible la connexió a Internet, gestiona l'execució dels programes, etc.

- **Navegador web**: programa que s'instal·la en un ordinador i permet als usuaris navegar i interactuar per la xarxa mitjançant la connexió, descàrrega i interpretació del contingut de tipus hipertext.

- **Malware**: terme que inclou, però no es limita, als virus informàtics. És un programa malintencionat que accedeix al dispositiu de l'usuari i en pot causar un perjudici mitjançant la destrucció del mateix, el robatori de dades, siga informació o claus d'accés a altres serveis, o el seu bloqueig i control per part d'un individu extern.

- **Pop-up**: finestra o requadre emergent que es genera sobre el contingut o programa desitjat, i que sovint pot contenir informació important, avisos, confirmació d'accions dels usuaris, anuncis o promocions.

- **Software**: tot allò relatiu al programari informàtic, part lògica que permet funcionar a l'ordinador.

- **Hardware**: tot allò relatiu a les parts físiques d'un ordinador, inclou les parts principals indispensables com la CPU, disc dur, placa base,... Així com els perifèrics: pantalla, teclat, ratolí,...

- **Phishing**: forma d'atac informàtic que es val de diferents mitjans i recursos per a fer-se passar per un servei de confiança, suplantant-ne la identitat, i robar a la víctima claus d'accés, informació privada o diners.

- **Spam**: correus o missatges brossa, i no desitjats, que s'envien als usuaris mitjançant els serveis de correu electrònic, o sistemes de missatgeria de les xarxes socials, i que pot contenir des de propaganda fins a *malware* o estafes.

- **Fake News**: notícies potencialment errònies, creades a propòsit o per omissió, i que poden contenir des de dades esbiaixades o no contrastades, fins a informació directament falsa.

- **Dark Patterns**: traduït com a patrons obscurs, és la utilització del disseny d'interfícies, programes, i aplicacions per tal de confondre i guiar a l'usuari perquè aquest faça accions en contra dels seus propis interessos.

- **URL**: combinació de caràcters alfanumèrics que apunten a la localització en Internet d'un recurs, document o arxiu, i permet sol·licitar-lo.

- **Petjada digital**: o empremta digital. Rastre de dades personals que deixa un usuari quan navega i utilitzar els serveis d'Internet. Pot arribar a permetre la identificació d'una persona física reunint i encreuant la suficient quantitat de dades. Comprén la informació que els mateixos navegadors proporcionen a les pàgines en connectar-se, les *cookies*, i altres dades d'ús recollides pels diferents serveis d'internet.

IMPULS!

Decàleg

1. Utilitzem els mòbils o els prohibim

A l'hora de definir límits en l'ús d'Internet per als menors, un dels primers conflictes que es troben és si permetre l'ús lliure dels mòbils o prohibir-los, especialment en xiquets d'una edat primerenca en un context educatiu. El primer instint pot ser prohibir-los en aquest entorn atés que és molt difícil assegurar-se de l'ús que se li està donant, ja que són moltes variables i és difícil mantenir l'atenció d'un gran nombre de xiquets i xiquetes si cadascun porta un mòbil a la mà. No obstant això, els mòbils són una gran eina per a la socialització i l'aprenentatge. En la societat actual gran part de les amistats i de la construcció de la visió del món succeeix a través d'Internet. Prohibir el seu accés impedeix realitzar una educació de l'ús apropiat i conscient d'aquest, podent arribar a donar lloc a conductes perilloses, ja que el menor, en aquest cas, tendirà a utilitzar internet a l'esquena dels adults.

a- Excés d'exposició a la tecnologia en els menors

L'excés d'exposició indiscriminada a les pantalles presenta un triple vessant de conflicte. D'una banda, els infants dediquen menys temps a activitats com la lectura, les manualitats o els jocs a l'aire lliure, necessàries per a un desenvolupament adequat. El consum recreatiu fora de l'escola i els deures ascendeix a una mitjana de quasi tres hores diàries entre els xiquets de fins a dos anys; quasi cinc hores entre els xiquets menors de huit; i més de set hores diàries entre els adolescents (Michel Desmurguet, 2019). Fins i tot des d'un punt de vista purament quantitatiu, això no deixa temps per a qualsevol altra mena d'entreteniment.

D'altra banda, les investigacions realitzades en aquest camp amb xiquets i adolescents demostren que el consum digital interfereix en l'adquisició d'habilitats lingüístiques, en la capacitat de concentració i en la memòria. L'adquisició d'aquestes capacitats requereix el desenvolupament d'una certa tolerància a l'avorriment i la frustració, que es pot aconseguir amb activitats guiades que animen als menors a interactuar amb el món que els envolta.

Finalment, cal no oblidar que el risc de desenvolupar una addició es multiplica quan hi ha una exposició prolongada sense cap supervisió ni control. La gratificació instantània que proporciona l'ús de les tecnologies és un oponent difícil contra el qual batallar, però és necessari crear en els menors un equilibri entre l'ús d'aquesta tecnologia i l'oci fora d'ella.

b- Ús, però amb responsabilitat

Utilitzar els mòbils com a eina en l'entorn educatiu per a fer algunes activitats reforça la comprensió de la tecnologia, alhora que permet al monitor mantenir el

control sobre el seu ús. No té sentit fer segons quines activitats sense accés a la tecnologia que les faria més senzilles. Cal reconéixer que la major part de la cerca d'informació hui dia es realitza a través d'Internet. Per aquest motiu, si s'inclou aqueix tipus d'ús en les activitats diàries del taller, acompanyades d'instruccions de com fer-lo amb seguretat i coherència, s'equipa als menors amb eines per a la vida real, perquè una vegada fora de l'entorn segur tinguen recursos eficients per a enfrontar-se a la xarxa. De la mateixa manera, és important alternar l'ús d'internet amb altres activitats que no la utilitzen.

c- Coherència dels adults

En el cas de l'ús del mòbil, és essencial que el comportament dels monitors vaja d'acord amb el que es tracta de transmetre als joves. Cal prevenir i evitar el cas d'un monitor que prohibeix el mòbil a l'aula, però que està constantment consultant-lo. De la mateixa manera, si es pretén que els alumnes no abusen del seu ús, s'ha d'evitar proposar constantment activitats la realització de les quals depenga d'això. És important propiciar la varietat en les activitats proposades que estimule la cerca d'eines alternatives i solució de problemes. Aquest control del seu ús es pot coordinar amb la no demonització d'aquest; els mòbils i la tecnologia poden ser una gran eina i és crucial reconéixer-los com a tal, i no com l'origen de tots els mals. Els adults actuen com a exemple a seguir; com més models de conducta tinguen els xiquets en la seua vida de persones que, a més d'usar un mòbil o un portàtil, facen exercici, passen temps a l'aire lliure i tinguen una vida fora de les pantalles, més inclinats se sentiran a perseguir aquests entreteniments per a si mateixos.

Els adults que s'encarreguen de guiar activitats d'oci educatiu han d'estar formats per a atendre aquests aspectes com a part integrant de l'activitat.

Fonts

Buenas Prácticas en Redes Sociales. Informe de buenas prácticas. (2021, julio). Centro Criptológico Nacional. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3009-ccn-cert-bp-08-redes-sociales/file.html

Niños en un mundo digital. (2017, diciembre). UNICEF. https://www.unicef.org/media/48611/file

2. Drets d'imatge i infància, XXSS

El dret a l'honor, la intimitat i la imatge dels menors està especialment protegit en l'àmbit de les noves tecnologies i, en concret, en el de les xarxes socials. De fet, l'ordenament jurídic posa l'accent principalment en això a través de la Llei de Protecció jurídica de menors (Llei orgànica 1/1996, de 15 de gener, de protecció jurídica del menor, de modificació del Codi Civil i de la Llei d'Enjudiciament Civil).

En aquesta llei s'estableixen aquests drets, es regula la difusió d'imatges de menors i s'estableix que aquest tipus de conducta pot ser constitutiva de delicte. Així doncs no és qüestió que puga ser presa a la lleugera la distribució en internet d'imatges de xiquets o xiquetes sense el seu consentiment o el dels seus tutors legals. Això ha de ser tingut en compte en les activitats en les quals se solen veure embolicats els menors d'edat, com són l'oci educatiu, el treball en esplais o en centres de joventut.

a- Consentiment legal del menor o dels seus tutors

Sovint existeix la idea que únicament són els tutors legals dels menors els que poden i deuen donar el seu consentiment per a la distribució d'imatges d'aquells. No obstant això, cal tindre en compte que la Llei 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals estableix que els menors a partir de 14 anys poden donar el seu consentiment per a la distribució de les seues imatges. En el cas dels menors de 14 anys, seran els tutors legals els que hagen de donar el consentiment.

b- Treballem la discreció i la intimitat

Tots som conscients que hui dia l'accés a les xarxes socials i la possibilitat de distribuir imatges o vídeos està absolutament generalitzada, i són els mateixos menors els que tenen aqueixa capacitat. Per molt que l'accés a determinats tipus de webs o la possibilitat d'interactuar amb determinats usuaris s'haja intentat controlar mitjançant l'ús de programari que el limita o ho impedeix, s'ha vist que això és quasi com tractar de posar portes a la mar. Així doncs, els educadors s'estan adonant que el millor programari de control que se li pot posar a un menor no se li ha d'instal·lar en el mòbil o en l'ordinador sinó al seu cap. Cal treballar amb ells perquè s'adonen que hi ha dades i imatges que encara que puguen semblar innòcues poden resultar problemàtiques.

Quan parlem d'intimitat en el primer que es pensa és en continguts d'alguna forma compromesos (imatges o vídeos de contingut eròtic o sexual) i, per descomptat, cal fer veure que compartir aquest tipus d'informació pot tenir conseqüències nefastes per als menors. És d'això del que parlem quan diem que cal treballar la discreció. Però hi ha un altre tipus d'informació que en principi pot semblar innòcua, però, precisament per això, la seua difusió pot resultar menys vergonyosa però no menys nociva. Per exemple, cal fer veure que una foto de l'habitació on es passa la vida o, fins i tot, la foto del carrer en la qual es viu també és informació privada i sensible. Una foto de molts amics distribuïda sense el permís de cadascun d'ells pot resultar comprometedora per a algun d'ells. Així mateix, una invitació d'aniversari o qualsevol document en el qual conste la direcció del menor pot ser una pista per a un possible assetjador; el mateix que una foto en la qual se li veja amb l'uniforme o localització del col·legi.

Fonts

¿Pueden los colegios tomar imágenes de los alumnos durante su actividad escolar? ¿Y subirlas a internet? (2018, 14 diciembre). AEPD. https://www.aepd.es/es/prensa-y-comunicacion/blog/pueden-los-colegios-tomar-imagenes-de-los-alumnos-durante-su-actividad

Grooming, acoso a menores en la Red. (2018, 25 mayo). PantallasAmigas. https://www.pantallasamigas.net/grooming-acoso-a-menores-en-la-red/

3. Utilització de serveis amb registre

És impressionant la quantitat d'aplicacions i serveis en línia que s'ofereixen de manera gratuïta: per a creació de presentacions, disseny gràfic, tota mena d'aplicacions educatives, llocs per a l'emmagatzematge de dades, jocs, etc. El problema és que en la majoria dels casos per a poder utilitzar aquests serveis se'ns exigeix que ens registrem. El normal és que considerem que, ja que se'ns ofereix un servei gratuït, que a vegades pot ser de gran qualitat, ens compensa donar les nostres dades. No obstant això, cal no oblidar una frase molt repetida: "Si un servei és gratuït, és perquè el producte eres tu". És a dir, el fet que ens registrem implicarà que les nostres dades seran emmagatzemats i pot ser, inclús, venudes amb o sense el nostre consentiment. Tenint això en compte, val la pena seguir amb el procediment de registre?

a- És el registre obligatori?

Quan un monitor o educador es veu en la necessitat d'utilitzar un determinat servei en línia el primer que ha de fer és comprovar si existeixen alternatives que no requerisquen registre. Una ràpida cerca en la xarxa especificant el terme "sense registre" pot resultar útil, encara que hem d'admetre que pot resultar frustrant la falta de resultats. Per descomptat, si trobem un servei útil que no requerisca donar dades és molt convenient que l'usem com a alternativa al que sí que les requereix, fins i tot si és una mica pitjor en prestacions. Són qüestions que sempre cal sospesar i actuar sabent el que es fa. D'altra banda, l'educador que desitge fer servir un servei en línia per a un grup d'estudiants i que es veja en la tessitura d'haver de registrar-los a tots no ho tindrà fàcil. Primer ha de veure quin tipus d'informació se'ls demana i quin s'exigeix de manera obligatòria. Ens la podem inventar? Una vegada sabut això ha de considerar si els alumnes utilitzaran aqueix servei una sola vegada o si hauran de tornar a utilitzar-ho en diverses ocasions.

b- Possibles riscs

El principal perill en haver de registrar-se, fins i tot si la pàgina només necessita el correu electrònic, és la possibilitat que acabe en una base de dades de *phishing*. Segons el Centre Criptològic Nacional, "el *phishing* és un tipus d'atac en el qual s'utilitza l'enginyeria social per a obtenir dels usuaris informació

personal, principalment d'accés a serveis financers. Per aconseguir el nombre més gran possible de víctimes i incrementar les possibilitats d'èxit, fan ús del correu brossa o *spam* per a distribuir-se. Una vegada que el correu arriba al destinatari, faciliten enllaços a llocs web modificats de bancs o botigues, perquè introduïsquen dades personals com els nombres de compte bancari, contrasenyes, etc.".

Aquests correus *spam* estan escrits perquè la persona senta que ha d'entrar a l'enllaç facilitat i emplenar els formularis amb les seues dades, per exemple dient que l'usuari ha guanyat un premi i ha de cobrar-lo, o fent creure que s'ha efectuat un pagament indegut i que per a bloquejar-lo cal accedir al compte bancari. Els menors són més susceptibles de caure en aquesta mena d'estafes, ja que poden mancar d'experiència per a adonar-se'n, però els adults que tracten amb informació important cal que estiguen també alerta. Per a la seua protecció, cada persona s'hauria de fer un correu dedicat a ser utilitzat en eines en línia i pàgines poc fiables, que no tinga cap connexió amb les seues xarxes socials o altres serveis crítics, que no incloga informació personal en el nom, i a la qual tinguen accés els tutors per a interceptar intents de *phishing* que pogueren arribar.

4. El monstre de les *cookies*, cal evitar-les?

Quan es navega per internet és molt comú trobar una notificació que sol·licita permetre les *cookies* o galetes cada vegada que s'entra a una nova pàgina web. Pot resultar impossible continuar navegant sense acceptar-les, així que moltes vegades s'accepten totes sense pensar. Hem de tindre present que en acceptar s'han descarregat arxius en l'ordinador dels quals no tenim informació. Per a realitzar un bon ús d'internet és important conéixer què són i què suposen.

a- Què són les cookies

Segons la definició de Google, "les *cookies* són xicotets fragments de text que els llocs web que visites envien al navegador". Gràcies a elles, els llocs web poden recordar informació sobre les visites que realitza un usuari, la qual cosa facilita el procés a l'hora de tornar a visitar-los. Algunes *cookies* guarden informació com el nom d'usuari i la contrasenya per a una web que necessita tindre un compte. Altres galetes guarden les preferències, com l'idioma seleccionat o els continguts d'un carretó de la compra en una botiga en línia. Són una eina molt útil per al bon funcionament de la navegació per internet i milloren la qualitat de l'experiència de l'usuari. Contra el que popularment es creu, no és cap mena de *malware*, sinó un petit arxiu de text que s'emmagatzema localment en l'ordinador de l'usuari i facilita diferents tasques.

b- Cookies ètiques vs. no ètiques

L'acció de permetre les *cookies* és, per normativa europea, una acció activa realitzada per l'usuari. Això vol dir que sense tindre permís exprés, una web no hauria de descarregar galetes en un ordinador res més entrar a ella. A l'usuari se li donarà l'opció de permetre-les o bloquejar-les, i en algunes ocasions, podrà triar quines vol acceptar. N'existeixen de tres tipus: tècniques, d'anàlisis i publicitàries. En general, les *cookies* tècniques són essencials per al bon funcionament de la pàgina. Les d'anàlisis milloren l'experiència de l'usuari en guardar dades sobre les seues preferències de navegació, i finalment les publicitàries recullen els hàbits de navegació per a ser utilitzats en anuncis personalitzats.

Encara que siga obligatori demanar permís per a començar a utilitzar-les en una web, el missatge que se li ofereix a l'usuari és en moltes ocasions enganyós, fent ús dels *dark patterns*, i està dissenyat perquè pense que no té una altra opció que acceptar-les totes. La diferència entre les galetes usades de manera ètica i les que no, és quanta informació i opcions queden a la disposició de l'usuari. La manera ètica inclou oferir l'opció de decidir quines *cookies* acceptar i quins bloquejar en cada web que visitem. Per contra, hi ha multitud de pàgines que només ofereixen un botó per a acceptar-les totes en un pop-up que impedeix l'ús apropiat del navegador. En bloquejar totes les galetes és possible que algunes pàgines no funcionen com toca. Aquest sistema intenta portar la llei al límit, en esgotar a l'usuari perquè preferisca acceptar-les totes sense complicar-se.

Com ja es va dir abans, les *cookies* no són perilloses per si mateixes, però això no implica que no es puga fer un ús no ètic d'elles. El principal és la distribució en massa de galetes publicitàries a tercers sense consentiment, que possibiliten rastrejar els usuaris al llarg de diferents pàgines sense relació aparent.

c- Com les bloquegem

Les *cookies* es poden eliminar una vegada ja acceptades, però també es poden bloquejar perquè no es descarreguen des d'un principi. Això es fa des de la configuració de qualsevol navegador que s'estiga usant. Com s'ha dit abans, les *cookies* no són dolentes en si mateixes, sinó que són una eina més que serveix per al bon funcionament de les webs, però no totes les pàgines en fan un ús legítim. Una ràpida busca a internet t'informarà sobre com bloquejar-les per defecte o esborrar-les en el teu navegador.

L'ideal és, sempre que es done l'opció, acceptar només les galetes necessàries per al bon funcionament de la pàgina i rebutjar totes les altres. Res et garanteix que una web no vaja a comerciar amb les teues dades, i per desgràcia hi ha molt poques eines a la disposició de l'usuari per a comprovar-ho.

Fonts

Guía sobre el uso de las cookies. (2022, junio). AEPD. https://www.aepd.es/es/documento/guia-cookies.pdf

Borrar cookies | Ayuda de Firefox. (s. f.). https://support.mozilla.org/es/kb/Borrar%20cookies

5. Informació VS desinformació

a- Exposició a les xarxes socials

Segons L'Agència Espanyola de Protecció de Dades, el 94,8% dels adolescents disposa de mòbil amb conexió a Internet, dispositiu al qual la mitjana accedeix abans dels 11 anys. El 92,2% dels estudiants de 1r i 2n d'ESO tenen telèfon intel·ligent propi. El valor de les relacions socials i el plaer que genera la interacció amb els altres és molt important en la vida d'un adolescent. Els dispositius electrònics s'han convertit en el mitjà més triat per xics i xiques per a socialitzar. Entre 2020 i 2021 es va produir un increment del 45% d'usuaris en Instagram i d'un 76% en TiKTok.

Diverses aplicacions que actuen com a xarxa social no dissenyades per a ús en menors (i, per tant, amb escasses limitacions quant a continguts) són usades per xiquets i joves on s'exposen a les *fake news* i altra informació dubtosa. Un dels aspectes més preocupants de l'ús de les tecnologies d'accés a continguts en Internet és que els i les menors tenen com a única font d'informació les xarxes socials. Sol ocórrer que el que envia el contingut desconeix el tema sobre el qual informa o li falten dades. La seua intenció pot ser bona, però difon mitges veritats o falsedats. També pot ser que conega el tema, però té un biaix ideològic, emocional o intel·lectual que li porta a presentar només una part de les dades, o fer-ho de manera que valide un posicionament previ. El pitjor cas és el d'aquells emissors que tenen interés a manipular o enganyar per a obtenir un benefici propi o danyar a uns altres a través de la desinformació.

Des de l'oci educatiu es pot conscienciar a xiquets i adolescents de què hi ha continguts que no són de fiar i entendre que cal estar alerta. No obstant això, si els troben, cal crear un espai de confiança suficient perquè se senten segurs preguntant a adults de confiança. Si descobrim que els consumeixen, hem de ser capaços de parlar amb ells, donar-los respostes i aclarir la possible confusió que senten, sempre en funció de la seua edat i maduresa. S'ha d'actuar amb serietat però evitant actituds dramàtiques.

b- Com diferenciem entre informació real i informació falsa?

Una de les oportunitats de proporcionar estratègies per a detectar i combatre la informació enganyosa està en les activitats guiades de temps lliure que permeten l'accés a continguts digitals. És possible ajudar als xiquets i joves a

què comprenguen la informació que troben i a distingir entre els fets, les opinions, els rumors i les mentides.

Els cinc consells que dóna la Fundació Gabo per a detectar notícies falses són:

1- Verificar la història: què està tractant de dir? Es pot trobar aquesta notícia en un altre lloc i s'explica de la mateixa manera?

2- Analitzar les emocions: com els fa sentir la història? Les notícies falses intenten manipular els sentiments de les persones perquè facen clic, al contrari que la informació autèntica, que no demanda una resposta immediata del lector.

3- Prestar especial atenció a les imatges: una cerca d'imatge inversa per a trobar d'on prové originalment permet detectar les manipulacions.

4- Comprovar que l'adreça URL corresponga amb l'oficial del mitjà corresponent. Verifique la barra d'adreces en la part superior. Si no, podria ser fals. També es pot comprovar la identitat de l'autor, veure si es tracta d'un expert o d'un simple comentarista.

5- Qüestionar la procedència: fins i tot si ho comparteix un amic, un familiar o una persona famosa, no significa que siga correcte.

Fonts

Un móvil es más que un móvil. (2022, 10 noviembre). AEPD. https://www.aepd.es/es/mas-que-un-movil

Los niños están siendo víctimas de la desinformación: ¿cómo prepararlos para no creer en mentiras? (2019, 22 mayo). Fundación Gabo. https://fundaciongabo.org/es/etica-periodistica/recursos/los-ninos-estan-siendo-victimas-de-la-desinformacion-como-prepararlos

Educando en el derecho a la información: contenidos falsos, nocivos e ilícitos | UNICEF. (2022, 10 marzo). UNICEF España. https://www.unicef.es/educa/blog/educando-derecho-informacion-contenidos-falsos-nocivos-ilicitos

Redes sociales y adolescentes: lo que tenés que saber. (s. f.). UNICEF. https://www.unicef.org/uruguay/redes-sociales-y-adolescentes-lo-que-tenes-que-saber

6. Reunions telemàtiques

a- Revolució pandèmica i consolidació

A partir de l'any 2020, el món va patir moltíssims canvis arran de la pandèmia. Abans d'això, les videoconferències en l'àmbit professional només es realitzaven en casos de necessitat, com quan els participants en la reunió es trobaven en països diferents. No obstant això, la necessitat del seu ús durant els mesos de quarantena va mostrar el potencial d'aquesta tecnologia. Hui dia, s'ha consolidat com a eina indispensable per al treball associatiu i d'equips, que permet que moltes persones participen en el mateix projecte sense necessàriament trobar-se en la mateixa ubicació física.

b- Dificultats i barreres tecnològiques

Sempre que apareix una nova metodologia de treball és inevitable que sorgisquen problemes relacionats. La barrera tecnològica n'és un dels principals. Pel bon funcionament de dinàmiques i reunions realitzades telemàticament cal garantir l'accés a aquesta tecnologia. No tothom té accés a un ordinador portàtil, i encara que el tinguera, no tothom es maneja amb ell com per a instal·lar i utilitzar amb fluïdesa un programari nou. Per a garantir que la transició de les reunions presencials a les telemàtiques siga tan lleugera com siga possible, seria important proporcionar els recursos des de l'organització a tots aquells que vagen a formar part de la dinàmica. Realitzar formacions sobre la instal·lació i utilització del programari, així com assegurar-se individualment que es té el maquinari apropiat a la disposició de tots, són solucions que es poden donar a aquests problemes.

c- Alternatives lliures i gratuïtes

Existeix una altra problemàtica unida a les reunions telemàtiques. La major part del programari disponible per a realitzar-les té una versió gratuïta, però que no permet suportar una reunió amb múltiples participants durant un temps prolongat. Moltes vegades, l'opció més senzilla per a les associacions i empreses és pagar el que costa la versió de pagament d'aquestes aplicacions, però el cas ideal és trobar alternatives gratuïtes i de programari lliure. D'aquesta manera, una associació sense ànim de lucre no depén per a la seua activitat diària d'un servei que puga fer negoci amb les dades dels usuaris, o cares alternatives d'igualment dubtosa protecció de dades.

BigBlueButton és una alternativa *Open Source* a aplicacions com a Zoom, que permet fer classes en línia, realitzar reunions en equip i moltes possibilitats més. Jitsi és també una molt bona alternativa, ja que és lliure, gratuït i també *Open Source*. Jitsi Meet és un servei privat que utilitza jitsi de manera ètica amb algunes limitacions, tot i que menors que a altres serveis.

d- Animem-la i fem-la àgil

Coordinar una reunió de manera efectiva no és una ciència exacta, ni de bon tros, però hi ha una sèrie de punts que poden ajudar a garantir una dinàmica fluida durant aquesta.

1. Puntualitat. Accedir a la reunió a l'hora acordada i no allargar excessivament l'inici d'aquesta.

2. El moderador ha de tindre un esquema clar dels punts a tractar i cenyir-se a ells.

3. Les intervencions han de ser rellevants per al que s'està discutint.

4. Restar silenciat, amb el micròfon apagat durant les intervencions d'uns altres.

5. Utilitzar el xat per a realitzar comentaris que no puguen esperar a una intervenció, o que no siguen prou extensos per a una.

6. Unir-se a la reunió des d'un entorn silenciós i ben il·luminat.

7. Demostrar atenció al que s'està discutint, aportant informació o preguntant quan faça falta.

8. No realitzar altres activitats durant la reunió.

9. Valdre's d'altres eines interactives com Kahoot, Trello o Excalidraw (alternativa Open Source a Jamboard)

Fonts:

Privacidad en reuniones online. (2021, 18 febrero). AEPD. https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-reuniones-online

VALENCIATECH. (2020, 12 noviembre). Servidor videoconferencia - Big Blue Button ». https://www.valenciatech.com/servicios/servidor-videoconferencia-big-blue-button/

7. Treballem el ciberassetjament

El ciberassetjament és l'assetjament o intimidació per mitjà de les tecnologies digitals. Pot ocórrer en les xarxes socials, les plataformes de missatgeria, les plataformes de jocs o qualsevol fòrum d'internet. És un comportament que busca atemorir, enfadar o humiliar a altres persones enviant missatges, imatges o vídeos feridors, abusius o amenaçadors. També és ciberassetjament difondre

mentides o publicar fotografies o vídeos vergonyosos d'algú, així com suplantar a una persona per a assetjar a una tercera. L'informe de Save the Children publicat en el 2019 destacava que l'assetjament en les xarxes socials als menors supera ja al tradicional, el que es desenvolupa cara a cara en el centre escolar i que s'estén posteriorment al carrer. L'assetjament cara a cara i el ciberassetjament ocorren junts sovint i el segon pot ser fins i tot més traumàtic perquè es pateix en soledat, en qualsevol entorn i sense testimonis.

a- Busquem entorns digitals segurs

Existeixen una sèrie de mesures que es poden prendre per a prevenir el ciberassetjament i construir entorns digitals segurs. A continuació es llisten algunes d'elles.

- Configuració del perfil o perfils de les xarxes socials en manera privada. És la forma més eficaç de controlar a qui s'està mostrant la informació. És crucial no acceptar sol·licituds de desconeguts i tindre un control adequat d'amics virtuals i seguidors.
- Utilitzar contrasenyes amb un alt nivell de seguretat amb diversos caràcters especials. Tindre la mateixa contrasenya a tot arreu no és bona idea.
- Informar-se sobre les polítiques d'ús que publica cada plataforma digital. Si hi ha un comportament irrespectuós i que no complisca aqueixes normes es podrà informar els responsables, moderadors, administradors o proveïdors del servei.
- Aprofitar la funció de bloqueig. Habitualment està disponible en les diferents xarxes socials i permet prohibir l'accés a aquells usuaris que envien missatges inapropiats o inesitjats abans que la situació empitjore o derive en un cas més de ciberassetjament.
- Assegurar-se de tindre un bon antivirus i tallafocs actualitzats que protegeixen enfront de l'exposició de les dades personals que s'introdueixen en l'ordinador quan s'activa la cambra del dispositiu o enfront d'intents de connexió des de dispositius no autoritzats.
- Utilitzar un model de cambra amb llum pilot. Aquesta xicoteta aplicació indicarà quan el dispositiu està o no gravant. Així serà possible evitar la intrusió de tercers que puguen realitzar enregistraments no autoritzats.
- Tindre precaució en compartir informació personal en Internet. Mai compartir l'adreça, el telèfon, el nom o els cognoms. Aquest consell pot estendre's per a la informació gràfica com a fotografies i vídeos.
- No respondre a provocacions d'un possible assetjador. L'única excepció és que siga per a informar-lo que el que està fent té es considera delicte. Abans de res, és recomanable no entrar en el joc, ni replicar les seues mateixes actuacions a manera de resposta.

- Acudir a l'educador. És important explicar i buscar ajuda si es considera que una situació podria arribar a desencadenar un mal o un cas d'assetjament. Atallar una situació a temps és evitar un problema.
- Guardar tot el que es considere una possible prova de ciberassetjament, ja siga un email, una conversa per xat o fins i tot una publicació en línia. Podrien resultar d'ajuda si es decidira denunciar els fets més endavant.

b- Estem atents, detectem i donem avís

Com a monitors i educadors, hem de mantenir-nos alerta per a identificar els indicadors del ciberassetjament a temps de protegir la víctima i que les pitjors conseqüències no arriben a manifestar-se. Hi ha dos tipus d'indicadors que poden indicar ciberassetjament, els que tenen relació amb l'ús de les tecnologies i els emocionals.

1) Indicadors en relació amb l'ús d'eines tecnològiques
    - Està pendent constantment que el mòbil o l'ordinador estiguen encesos i disponibles, inclús quan dorm.
    - Es mostra enfadat, depressiu o frustrat després d'utilitzar l'ordinador.
    - Deixa d'utilitzar l'ordinador de forma sobtada.
    - Mostra canvis sobtats de comportament després d'una trucada, missatge, accés a una xarxa...
    - Dona la contrasenya de correu o d'alguna xarxa amb facilitat.
    - Comparteix dades personals en diferents xarxes socials
    - Intercanvia fotos o vídeos i informació personal per xarxes socials
    - Accepta com a amics persones desconegudes.

2) Indicadors emocionals:
    - Expressa canvis sobtats d'humor, d'estats d'ànim o de comportament.
    - Expressa inseguretat i /o ansietat.
    - Li costa controlar-se.
    - Mostra poques habilitats socials (especialment assertivitat).
    - Mostra un aspecte contrariat, trist, deprimit i/o temorenc sense motiu aparent.
    - Plora amb facilitat i/o sovint s'angoixa emocionalment.
    - Es tanca en si mateix, evitant relacionar-se amb els amics o amb la família.
    - Es preocupa excessivament per la seua seguretat personal: dedica molt de temps i esforç a pensar i preocupar-se per trobar trajectes i espais segurs.
    - S'obsessiona per la seua alçada, pes, o altres trets físics.

Malgrat la gravetat del ciberassetjament i del mal que provoca, hi ha més recursos per a combatre'l, ja que deixa una empremta digital que pot servir de prova per a ajudar a parar l'abús. El INCIBE (Institut Espanyol de Ciberseguretat en el seu portal Is4K) ens insta a acudir a les autoritats (Policia Nacional, Guàrdia Civil, policies autonòmiques, etc.) o a la Fiscalia de Menors.

Fonts

Ciberacoso: Qué es y cómo detenerlo. (s. f.). UNICEF. https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Ciberacoso escolar. (2020, 7 septiembre). Internet Segura for Kids. https://www.is4k.es/necesitas-saber/ciberacoso-escolar

Indicadors de coneixement o sospita d'una situació d'assetjament o ciberassetjament. (2019, 27 julio). Gencat. https://xtec.gencat.cat/web/.content/centres/projeducatiu/convivencia/protocols/assetjament-ciberassetjament-entre-iguals/documents/12-indicadors-assetjament-ciberassetjament.pdf

8. Programari Open Source d'ús quotidià

Hi ha multitud de tipus de programes que s'han d'usar diàriament, des de sistemes operatius per a l'ordinador, passant per programes d'oficina i els ja esmentats programes per a realitzar reunions telemàtiques, i arribant finalment a programes més específics d'oci i educació. Tindre familiaritat amb aquestes eines de programari no corporatiu dona independència a les associacions.

a- Sistemes operatius

Tot i que sistemes com IOs o Microsoft són l'opció més coneguda quan es parla de sistemes operatius, no són ni molt menys l'única opció. Linux està disponible per a particulars, entitats i organitzacions, és gratuït i transparent quant a les seues funcionalitats i l'ús que fan de les dades dels usuaris. Qualsevol usuari amb coneixements de programació el pot, fins i tot, modificar per a adaptar-lo a les seues necessitats. Alguns exemples notables, estesos i provats, en son l'Ubuntu i qualssevol de les seues variants en la versió d'escriptori.

b- Eines d'oficina

Les eines de Google o Microsoft tenen una alta presència en l'educació degut a anys de familiarització per a la majoria d'usuaris. Permeten preparar documents

de text, presentacions o fulls de càlcul, fer videocridades, guardar dades en el núvol i fer classes en línia de manera col·laborativa. Així i tot, l'ús de dades que fa l'empresa és preocupant per al món associatiu, sobretot quan es treballa amb menors. En lloc d'utilitzar aquestes eines, Lliure Office està disponible a tot el món de manera universal i gratuïta i de codi obert. Aquesta eina, es pot combinar amb l'ús de diferents programes lliures com el Jitsi, entre altres, per complementar algunes funcionalitats.

c- Eines de creació i edició de contingut

En aquest àmbit, la Suite d'Adobe és el líder indiscutible quan es parla d'aquest tipus de programari. No obstant això, Adobe és una empresa privada que cobra quantitats elevades de diners pels seus serveis. No hi ha una única suite que servisca d'alternativa completa a tots els serveis d'aquesta empresa, però individualment podem trobar opcions suficients. En lloc de Photoshop, el Gimp ofereix un similar ventall de funcionalitats per a la majoria de casos, i és completament gratuït. Per a edició de vídeo, el Kdenlive o OpenShot son programes lliures i ofereixen una gran quantitat d'eines. Per al tractament d'àudio, Audacity és també molt conegut per la seua versatilitat i facilitat d'ús, que es pot combinar amb l'Ardour per a tasques més complexes. Existeixen alternatives per a totes les parts de la Suite d'Adobe disponibles en codi lliure, en el següent enllaç es poden consultar totes:

Font

The GNU Operating System and the Free Software Movement. (s. f.). https://www.gnu.org/

Front Page — Free Software Foundation — working together for free software. (s. f.). https://www.fsf.org/

9. La tecnologia com a eina d'accessibilitat

La tecnologia de la informació en els tallers i activitats socioeducatives contribueix a generar empatia i interacció entre els participants i els educadors, la qual cosa afavoreix la inclusió de les i els menors, especialment aquells que tenen necessitats especials. S'estima que el 80% de les persones amb discapacitat poden accedir i manejar les TIC, i de fet aquest col·lectiu s'ha convertit en usuari habitual i avançat en molts casos d'aquestes. Per això cal fer un esforç i evitar les barreres digitals, que sovint són més difícils de percebre que les barreres físiques.

a- Tecnologia inclusiva

La irrupció de tecnologies inclusives i productes de suport tecnològics faciliten les tasques i rutines de les persones amb discapacitat. Per exemple, equips i programes per a augmentar la mobilitat, l'audició, la visió o les capacitats de comunicació. La digitalització té un gran potencial per a acabar amb les barreres de discriminació basades en variables com la força física, inèrcies o rols que tradicionalment han perjudicat les persones amb discapacitat. Hi ha moltes eines digitals que es poden implementar per a aquest fi.

Plena inclusió és un moviment associatiu que lluita a Espanya pels drets de les persones amb discapacitat intel·lectual o del desenvolupament i els seus familiars. En la guia que edita Plena inclusió Espanya hi ha nombrosos recursos explicats usant el llenguatge de Lectura Fàcil.

Algunes d'aquestes eines poden usar-se també amb persones no discapacitades de manera lúdica, ajudant a la integració de tots. Molts materials didàctics digitals dissenyats per a persones amb discapacitat han resultat interessants i útils també per a persones sense discapacitat. Es poden aprofitar també per a crear consciència de les dificultats d'accessibilitat que activitats quotidianes relacionades amb les TIC presenten per a les persones amb discapacitat.

b- Eines digitals per a ajudar a la inclusió

- **Jocomunico**: tracta sobre la Comunicació Augmentativa i Alternativa (CAA), és a dir, desenvolupada per a persones amb trastorns de la parla, que per a poder comunicar-se recorren als pictogrames. És una aplicació de fàcil ús i flexible per a la creació d'activitats sobre vocabulari, pictogrames, oracions entre altres. A més, és compatible amb Android i iOS; també amb Windows i Mac. És gratuïta i de *software lliure*.
- **Dia a dia**: aquesta aplicació és ideal per a persones amb autisme o problemes de comunicació. Permet dur a terme tasques del dia a dia de manera intuïtiva i senzilla. També té un calendari per a organitzar i guardar tasques, activitats que s'han realitzat. És una aplicació per a persones amb Trastorn de l'Espectre Autista (TEA) que fomenta la comunicació a través de la planificació i organització d'activitats.
- **Google Talkback**: és un lector de pantalla de Google integrat en dispositius amb sistema operatiu Android. És una eina d'accessibilitat que simplifica l'ús del mòbil. En ella pots engrandir els elements de la pantalla i connectar-ne una de braille per a persones invidents. Disponible en Android.
- **BrailleBack:** aplicació és per a persones no vidents. Bàsicament, els ajuda a utilitzar el dispositiu amb un servei combinat de veu i sistema Braille, és a dir, forma un enllaç entre una pantalla braille i dispositiu connectat per Bluetooth. Una altra de les coses a destacar de l'aplicació és que permet

introduir text en diferents aplicacions mitjançant el teclat Braille. És compatible amb Android, gratuïta i de *software lliure*.

- **EmoPlay**: és una aplicació per a treballar el control de les emocions: tristesa, alegria, enuig, ira, de manera senzilla. Només hem de triar l'emoció que volem treballar i ens apareixerà una imatge amb l'expressió facial la qual cosa hem de triar l'escenari per a aplicar-la. A continuació, l'usuari ha de realitzar els gestos que veu en pantalla, per a determinar quina emoció és la que veu o sent.
- **Sígueme:** Està pensada per a potenciar l'atenció visual i entrenar l'adquisició del significat en persones amb TEA (Autisme). L'aplicació està separada per sis fases principals: Atenció, Dibuix, Pictogrames, Vídeos, Imatges i Jocs, que parteixen de l'estimulació basal a l'adquisició de significat a partir d'elements visuals.
- **DictaPicto**. Permet passar la informació de veu a imatges de manera immediata, a través d'una frase parlada per l'usuari que després es transformarà en text o pictogrames. És ideal per a persones amb TEA o les que utilitzen l'aprenentatge a través del sistema pictogràfic per a millorar i fomentar la comunicació, accés a la informació i facilitar la comprensió de l'entorn.

Fonts

Gil, I. (2022, 31 mayo). Las Nuevas Tecnologías al servicio de la discapacidad. Diversidad e inclusión. https://fundacionadecco.org/azimut/las-nuevas-tecnologias-al-servicio-de-la-discapacidad/

Tecnología para personas con discapacidad intelectual. (2020, marzo). Plena inclusión. https://www.plenainclusion.org/sites/default/files/tecnologia_para_personas_con_discapacidad_intelectual.pdf

Soluciones tecnológicas autismo. (2019, 24 abril). Fundación Orange. https://fundacionorange.es/junto-al-autismo/soluciones-tecnologicas/