Finestra del Cau

Fitxa d'activitats

Finestra del Cau	Seguretat digital al cau: una responsabilitat i una oportunitat educativa
Nom de l'activitat	Tractem bé les dades sensibles?
Durada	1 hora
Etapa educativa	Caps
Nombre de participants	Variable; amb tot el Consell

Objectius

1. Prendre consciència sobre la gestió que fem de dades personals de les nostres infants i joves.
2. Revisar les eines que utilitzem per gestionar i ordenar les dades personals de l'agrupament

Material necessari

- Fulls
- Bolígrafs
- Un ordinador (opcional)

Desenvolupament

Els agrupaments guardeu moltes dades de les infants i joves membres del cau, com per exemple:

- Nom complet
- DNI
- Gènere
- Data de naixement
- Núm. targeta sanitària
- Informació sanitària
- Adreça completa
- Noms complets tutors legals
- Números de telèfon de tutors legals
- Adreces de correu electrònic de tutors legals
- Informació familiar
- Signatures
- Número IBAN
- Quan i on es fa l'activitat ordinària
- Fotografies

Aquestes dades estan en documents com autoritzacions i el cens, però depèn de com les guardem correm el risc que es filtrin.

Segons l'Agència Catalana de Ciberseguretat, "un dels ciberatacs més freqüents que podem patir com a usuaris d'Internet és el robatori de dades personals, ja sigui perquè els nostres comptes s'han vist compromesos o bé perquè una empresa o institució que custodiava les nostres dades ha patit un ciberatac i els ciberdelinqüents han aconseguit robar-les. En qualsevol cas, les nostres dades personals poden quedar exposades de forma pública i comprometre la nostra seguretat.

Els ciberdelinqüents poden aprofitar les dades robades per cometre fraus o per publicar-les i vendre-les al mercat negre d'Internet. Podem saber si algunes de les nostres dades han estat publicades a la dark web consultant-ho a la web Have I Been Pwned. "

En gran grup, parlem de quins perills creiem que pot tenir la filtració de totes les dades que hem llistat abans.

Tot seguit, o si no en sabem dir cap, podem revisar què diu l'Agència Catalana de la Ciberseguretat respecte com pot afectar una filtració de dades.

Aquestes dades, com hem dit abans, les acostumem a guardar amb certa documentació, així que revisarem quin tipus de documentació guardem i com, pensant quin risc de filtració té cadascuna segons on i com les guardem.

Ompliu la següent taula en petits grups (us podeu repartir uns quants tipus de documentació per grup), omplint només aquella documentació que guardeu.

Tipus de documentació	On es guarda?	Tothom hi té accés? Si no, qui i com es decideix?	Es guarda permanentment?	Risc de filtració (de l'1 al 10)
Autorització anual				
Fitxa d'inscripció				
Autorització d'activitat puntual				
Fotografies infants				
Autorització drets d'imatge				
Marxants de campaments				
Sol·licituds beques (documents adjunts)				
Documentació de gestió econòmica de quotes				
Altres (podeu afegir més categories que creieu necessaries)				

Per puntuar el risc de filtració, us deixem un llindar. Un 1 seria que està en un repositori privat on només té accés el correu electrònic de l'agrupament (Exemple: només algunes persones de l'agrupament hi tenen accés i són les responsables de guardar les dades), i un 10 que està en un espai totalment públic on tothom té accés contínuament. (Exemple: un cap que va marxar fa cinc anys podria accedir a alguna informació)

Sumem totes les puntuacions i fem la mitja del risc:

Si la mitja és menys de 3, molt bé, sou prou segures, tot i que sempre cal anar amb compte!

Si la mitja és menys de 5, no està malament, poc risc, tot i que es pot millorar.

Si la mitja és menys de 8, ep!, que ens apropem al risc alt, cal fer canvis immediats.

Si la mitja és més de 8, segurament les dades sensibles del vostre agrupament ja s'han filtrat, poseu-vos les piles i comenceu a fer canvis!

Com solucionem els problemes que hem trobat?

Propostes d'emmagatzematge de dades amb control d'accés:

Disc dur al cau: és la més segura, però també té el seu costat negatiu, ja que l'accés a les dades està limitat geogràficament.

Drive propi del correu de l'agrupament: només tenen accés les persones que amb accés al correu de l'agrupament, però s'ha d'actualitzar la contrasenya (mínim anualment) i vigilar que tot es pengi des del correu de l'agrupament i no des de correus personals.

Unitat compartida (Google Drive): amb el correu associatiu podeu crear una unitat compartida, funciona de forma similar a una carpeta compartida però amb alguns avantatges de seguretat. Tots els documents que es pengen pertanyen al domini del correu i no al compte que els ha penjat (en aquest cas "agrupaments.escoltes.org"), el compte "propietari" de la unitat té diverses opcions de permisos per als altres usuaris per poder limitar quin és l'accés que té cadascú. Fins i tot limitar l'opció de descarregar, copiar o imprimir arxius.

Consells

- *Cal limitar l'accés a aquesta documentació. Si feu servir el núvol (Google Drive, Dropbox, etc.), cal vigilar a quins correus electrònics s'han compartit certes carpetes o documents.*
- *El núvol és una eina amb molt de potencial per guardar informació i tenir un accés fàcil, però això també implica que s'ha de cuidar bé qui té accés i com. Cal revisar bé la política de privadesa de les dades de l'eina que utilitzem, ja que pot ser que l'empresa propietària usi les dades que guardem en el seu programari per lucrar-se, i això implicaria una filtració de dades sensibles també.*
- *Igual que amb el programari del núvol, cal vigilar quines xarxes socials fem servir i quina informació hi compartim i com, a més de la política de privadesa de dades d'aquestes empreses també.*
- *Recordeu només demanar la documentació mínima necessària, ja que com menys en tingueu, menys risc a què es filtrin més dades.*

Per acabar, com a consell, decidim un pla d'acció per reduir el risc de les dades sensibles de les infants i joves de l'agrupament. Aquest pla d'acció pot incloure la capacitació de les membres de consell amb formacions sobre el tema.