



Col·legi Oficial de
Psicologia de Catalunya

Comunicació i Guia d'acció davant la Bretxa de Seguretat d'EHOLO





Referent a la notificació a l'AEPD o als pacients sobre l'atac que ha sofert EHOLO, això depèn de quina informació i quin ús li doneu a EHOLO. Si només l'utilitzeu per agenda, reserva i no té dades de salut ni de menors no s'ha de comunicar. Però si la Plataforma té alguna dada de menors (encara que sigui identificativa o de contacte) o de salut, s'hauran de fer les notificacions. Per tant:

- Només teniu dades identificatives i de contacte (sense dades de menors): No heu de fer res.
- Només teniu dades identificatives i de contacte (amb dades de menors): S'ha de comunicar a l'AEPD.
- Teniu dades de salut (amb menors o sense): S'ha de comunicar tant a AEPD com a pacients.

Per poder fer aquesta comunicació, és indispensable que demaneu a EHOLO el següent:

1. Demanar si les vostres dades personals han sigut realment afectades perquè possiblement es farà una notificació, és per això que heu de saber si les vostres dades estan realment afectades, cal assegurar-se que no es tracta només d'un correu enviat automàticament a tots els usuaris d'EHOLO.
2. Si les vostres dades han estat afectades, heu de demanar a EHOLO un informe sobre l'incident que inclogui la següent informació:
 - a. Tipus d'incident (accés no autoritzat / *ransomware* / fugida / exfiltració / error humà).
 - b. Data i hora de la detecció.
 - c. Data i hora en què es va produir (si es coneix).
 - d. Comportament de l'atacant (moviments laterals, filtració, consultes, etc.).
 - e. Si va haver-hi filtració de dades o només accés.

- f. Si es va intentar extorsió i explicació d'aquesta.
- g. Vector d'atac (*phishing*, contrasenya robada, exploit, vulnerabilitat del sistema, error humà, API exposada, mala configuració, etc.).
- h. Condicions que van permetre l'accés.
- i. Fallades de seguretat que van intervenir.
- j. Descripció de la naturalesa de la violació de seguretat
- k. Indicació de les mesures de seguretat prèvies que s'havia adoptat i
- l. Indicació de les mesures que s'han implementat i de reforç arran de la violació (mesures correctives adoptades).

Referent a les notificacions:

- La notificació a AEPD s'ha de fer en el següent enllaç identificant-te amb el certificat digital de l'empresa/activitat:
 - <https://sedeaepd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/nbs/procedimientoBrechaSeguridad.jsf>
- Per comunicar la incidència als pacients, es pot utilitzar el model facilitat pel mateix EHOLO.

Hi ha termini de 72 hores per fer aquestes notificacions des del moment en què EHOLO us ha traslladat aquesta incidència, i per tant si s'han de fer aquestes notificacions s'ha de demanar a EHOLO la informació indicada el més aviat possible per després fer les notificacions.