# SICAP-FEPOL acusa Justícia de minimitzar el ciberatac a Puig de les Basses: 26.000 documents i dades personals exposades

*Alt Empordà | 19-08-2026 | 20:21*


**Centre Penitenciari Puig de les Basses i Domingo Estepa / GN**

SICAP-FEPOL acusa el Departament de Justícia d?haver minimitzat la gravetat del ciberatac perpetrat des del Centre Penitenciari Puig de les Basses, a Figueres. Segons el sindicat, les darreres dades facilitades per la Direcció General i els organismes tècnics contradiuen la versió inicial d?un accés puntual i limitat.

Els interns haurien accedit a una dotzena de carpetes de la xarxa departamental i haurien generat una còpia d?uns 40 GB d?informació, formada per aproximadament 26.000 documents, prop de 300 dels quals estarien duplicats.

Els primers indicis de l?activitat es remuntarien al febrer. Al maig, els accessos haurien arribat a la xarxa general del Departament de Justícia i, durant el juliol, s?haurien concentrat el 97% de les visualitzacions. Malgrat això, l?atac no es va detectar formalment fins al 9 d?agost.

Matrícules, DNI i telèfons de comandaments

Entre la informació que hauria quedat exposada hi ha matrícules de vehicles vinculades als números d?identificació professional ?NIP?, DNI associats a adreces de correu electrònic, llistats antics de personal, documentació de gestió interna, telèfons de comandaments de la presó i dades de persones voluntàries que accedeixen al centre.

SICAP-FEPOL adverteix que aquesta informació podria facilitar la identificació, el seguiment, les amenaces o possibles accions dirigides contra els professionals penitenciaris.

El fet que els interns no accedissin directament al Sistema d?Informació Penitenciari Català ?SIPC? ni al portal ATRI no descarta, segons el sindicat, que determinats documents haguessin estat exportats prèviament d?aquestes plataformes i desats en carpetes compartides.

La versió inicial del Departament assenyalava que no s?havia accedit als sistemes d?informació penitenciaris considerats crítics ni s?havia compromès el funcionament dels serveis. Justícia també va anunciar una investigació tècnica de l?Agència de Ciberseguretat de Catalunya i va posar els fets en coneixement del jutjat de guàrdia de Figueres i de l?Autoritat Catalana de Protecció de Dades. Així es va comunicar públicament després de detectar-se l?incident.

Fins a sis mesos d?activitat sense detectar

La informació traslladada als representants sindicals apunta que al febrer ja s?hauria produït una alteració relacionada amb minuts de trucades del centre, presumptament destinats a la venda.

L?activitat hauria fet el salt a la xarxa departamental durant el maig i hauria assolit la màxima intensitat al juliol. SICAP-FEPOL reclama explicacions sobre com una operació d?aquesta magnitud va poder mantenir-se durant mesos sense activar cap mecanisme eficaç de detecció precoç.

Després de descobrir-se l?accés, es van canviar les contrasenyes i es van actualitzar els equips. El sindicat considera que aquestes actuacions eren imprescindibles, però sosté que van arribar quan la vulneració ja s?havia produït i no resolen les possibles mancances prèvies de control, supervisió i monitoratge.

Una credencial guardada en una carpeta accessible

Segons la informació facilitada durant una reunió amb els representants del personal, el servidor del sistema biomètric de control d?accessos compartia infraestructura amb la xarxa general del Departament de Justícia.

A més, una credencial hauria quedat emmagatzemada inadequadament en una carpeta accessible dins la infraestructura gestionada pel proveïdor tecnològic T-Systems. També s?hauria reconegut que el nivell de seguretat existent abans de l?atac era un «nivell estàndard molt pobre».

SICAP-FEPOL considera que, si aquestes dades es confirmen, el cas no es limita a l?actuació dels interns, sinó que evidencia una cadena de possibles deficiències en la segmentació de les xarxes, la custòdia de les credencials, la supervisió del proveïdor i la detecció d?accessos anòmals.

El sindicat exigeix que l?anàlisi anunciada sobre T-Systems tingui conseqüències si s?acrediten incompliments contractuals o legals. També recorda que la responsabilitat última de contractar, supervisar i garantir la seguretat dels sistemes correspon a l?Administració.

No hi ha proves que els arxius sortissin de la presó

Actualment no consta cap prova que els 40 GB d?informació s?hagin difós fora del centre penitenciari. SICAP-FEPOL puntualitza que no afirma com a fet acreditat que s?hagi produït una filtració externa, però alerta que tampoc es pot garantir que no hi hagués una extracció de dades.

La investigació ha posat sota custòdia sis equips informàtics. També s?haurien intervingut dos

reproductors MP3 i un dispositiu USB, suports que podrien haver estat utilitzats per copiar informació sense que la seva circulació fos detectada immediatament.

El sindicat subratlla que, encara que no es demostri una difusió posterior, l?accés no autoritzat a informació personal ja representa una vulneració de seguretat.

Quatre interns sota investigació

Les dades facilitades assenyalen la possible implicació de quatre interns. Un d?ells, considerat el principal responsable, hauria estat sotmès al règim de l?article 93 i traslladat a un altre centre. Un segon estaria subjecte al règim de l?article 94, mentre que un tercer hauria actuat com a col·laborador.

El quart intern hauria proporcionat informació rellevant per ajudar a aclarir els fets. La investigació judicial haurà de determinar les responsabilitats individuals i el paper concret de cadascun dels implicats.

SICAP-FEPOL reclama que Justícia expliqui quins mitjans informàtics tenien a l?abast, quines restriccions s?havien aplicat, com van aconseguir les credencials i per què interns sotmesos a règims de control especial van poder accedir durant mesos a documentació departamental.

El sindicat exigeix el cessament de Domingo Estepa

Davant la gravetat del cas, SICAP-FEPOL reclama el cessament immediat del director general d?Afers Penitenciaris, Domingo Estepa. Si no dimiteix, demana que sigui destituït pel conseller de Justícia.

El sindicat també exigeix una auditoria integral i independent, la comunicació individual a totes les persones afectades, mesures específiques de protecció, la revisió completa de les credencials i la implantació generalitzada de l?autenticació de doble factor.

Entre les peticions també figuren la separació efectiva dels sistemes penitenciaris i departamentals, la retirada temporal dels terminals que no puguin certificar-se com a segurs i la instal·lació de sistemes reals de detecció precoç d?intrusions i descàrregues massives.

«Si diversos interns es van poder moure durant mesos per la xarxa del Departament, el problema no és només qui va prémer les tecles: també és qui va dissenyar, contractar, supervisar i permetre un sistema amb unes vulnerabilitats com aquestes», conclou SICAP-FEPOL.

Autor: Redacció