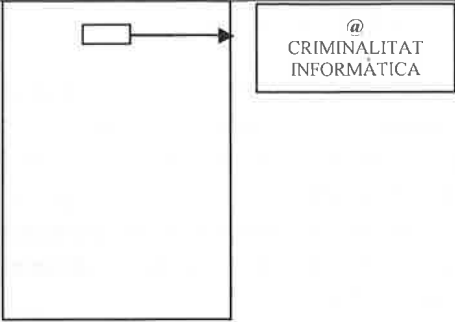


 GOVERN ILLES BALEARS	Conselleria de Presidència, Funció Pública i Igualtat Direcció General d'Emergències i Interior. ISPIB MANUAL DE PROCEDIMENTS	CODI PTN-014-PT
Títol: PROTOCOL D'ACTUACIÓ DE LA POLICIA LOCAL EN INCIDÈNCIES RELACIONADES AMB LES TECNOLOGIES DE LA INFORMACIÓ I COMUNICACIÓ (TIC)		
Responsable del procés de l'ISPIB: Rafel Covas Femenia	Tipus: operatiu	Data d'edició: 15/03/2023 Edició: 1 Nombre de pàgines: 8
OBJECTIU ESPECÍFIC: mitjançant el present protocol d'actuació policial es pretén, en primer lloc, donar a conèixer la tipologia de delictes relacionats amb els fets comesos a través de les tecnologies de la informació i comunicació, i la seva posterior metodologia d'actuació per part dels agents de la Policia Local, especialment dels policies tutors; aquests són els encarregats de treballar la problemàtica que afecta els menors d'edat en tots els àmbits, i també els que duen a terme les accions preventives necessàries mitjançant els centres educatius per prevenir i donar a conèixer els perills derivats de l'ús de les TIC, així com assessorar els equips directius en els casos de necessitat.		
NORMATIVA DE REFERÈNCIA		
Llei orgànica 10/1995, de 23 de novembre, del Codi penal i Llei d'enjudiciament criminal. LO 1/2015, de 30 de març, per la es modifica la LO 10/1995, de 23 de novembre, del Codi Penal.	Instrument de ratificació del conveni sobre ciberdelinqüència, signat a Budapest el 23 de novembre de 2001 i ratificat per Espanya, el qual és efectiu des de l'1 d'octubre de 2010 (BOE núm. 226, de 17/09/10)	
Llei orgànica 5/2000, de 12 de gener, reguladora de la responsabilitat penal dels menors, i Reial decret 1774/2004, de 30 de juliol, pel qual s'aprova el Reglament de la Llei orgànica 5/2000, de 12 de gener, reguladora de la responsabilitat penal dels menors	Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions, i Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic	
Instrucció 2/2011, d'11 d'octubre, sobre el fiscal de sala de criminalitat informàtica i les seccions de criminalitat informàtica de les fiscalies	Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.	
DOCUMENTS RELACIONATS:		
	GENERALITATS	
	En el Codi penal espanyol no hi ha cap títol específic que reculli els delictes que col·loquialment coneixem com a <i>delictes informàtics</i>. La realitat actual té en compte un nou delicte o delictes clàssics comesos a través d'un mitjà nou: les tecnologies de la informació i comunicació. La persecució d'aquests delictes estableix una diferència substancial respecte de la resta. La investigació a través del mitjà tecnològic té unes característiques específiques per la naturalesa de la prova informàtica. La Fiscalia General de l'Estat va dictar la Instrucció 2/2011 per la qual es va crear la figura del fiscal de sala de Criminalitat Informàtica, que coordina l'actuació dels fiscals provincials i potencia la unificació de criteris d'actuació en totes les jurisdiccions territorials del ministeri públic.	
NÚM.	ACTIVITATS	NORMATIVA I RESPONSABLE

1	Actuació de la Policia Local en incidències mitjançant les TIC amb els presumptes autors coneguts, desconeguts o residents a l'estranger En el cas que un agent de l'autoritat tengui coneixement, directament o bé per mitjà d'una denúncia, d'un presumpte fet delictiu comès mitjançant l'ús de les noves tecnologies de la informació i comunicació (Internet, xarxes socials, telèfon mòbil, tauletes tàctils o similars, sempre amb connexió a la xarxa), es durà a terme la metodologia d'actuació present: Presentació de denúncia per part de l'interessat. OPCIONS: a) Presentació de la denúncia en dependències policials de les forces i cossos de seguretat de l'Estat: els afectats per un presumpte fet delictiu tenen la possibilitat de presentar una denúncia per escrit davant el Cos Nacional de Policia o davant la Guàrdia Civil, segons la zona, per donar inici a les diligències policials. b) Presentació de la denúncia davant els òrgans judicials: els mateixos afectats també poden presentar una denúncia davant el jutjat d'instrucció o fiscalia de guàrdia. c) Presentació de la denúncia en dependències de la Policia Local: en el cas que un possible afectat per un fet delictiu comès mitjançant les TIC sol·liciti presentar la denúncia davant un agent de la Policia Local de les Illes Balears, s'ha de procedir de la manera següent: C.1 Recollida de la denúncia: en el cas que la presumpta víctima vulgui presentar la denúncia davant la Policia Local, es recollirà per escrit indicant els fets descrits per la víctima amb tota la informació necessària per a la posterior investigació per part de les unitats especialitzades. En el cas dels menors d'edat, es recollirà la denúncia i, sempre que sigui possible i evitant demores, aquesta es farà en presència de la persona que tengui la pàtria potestat (pare o mare), la tutela o la guarda de fet. Si els pares no poden ser presents en el moment de la denúncia, els fets denunciats es posaran en coneixement seu al més aviat possible. C.2 Annexos adjunts a la diligència de denúncia: es tracta d'aportar la màxima informació sobre referències informàtiques que permetin accedir-hi posteriorment de manera voluntària o judicial. En el cas que el denunciant no aporti els indicis necessaris relatius als fets que han motivat la presentació de la denúncia, es recolliran per investigar-los posteriorment, i seran accessibles des de qualsevol espai públic d'Internet. En el cas d'arxius ubicats en servidors informàtics (correus electrònics, xarxes socials, etc.) es podrà aportar la impressió de la pantalla en què es vegin els arxius esmentats, sempre que el denunciant els vulgui donar de manera voluntària com a referència als fets assenyalats en la seva manifestació. També és important en els correus electrònics assenyalat les dades del remitent (adreça electrònica).	LO 10/1995 DEL CODI PENAL LECr.
---	---	---

	En el cas de telèfons mòbils (missatges de Whatsapp, correu, etc.) es pot fotografiar la pantalla del telèfon mòbil en què es troba el text que motiva la denúncia, i també les dades del remitent (número de telèfon, si és conegut), sempre que les dades siguin aportades voluntàriament per la possible víctima. També es recollirà manifestació als possibles testimonis que puguin aportar indicis d'interès per a l'esclariment dels fets comesos. — Indicis: És important recordar a la presumpta víctima que conservi tots els arxius ubicats en sistemes tecnològics (correu electrònic, telèfon mòbil, etc.), així com que els guardi en suport informàtic perquè les unitats especialitzades en criminalitat informàtica els investiguin posteriorment. — Presumptes autors: Si es té coneixement de la identitat dels presumptes autors dels fets indicats en la denúncia, es podran identificar i fer constar per diligència, la qual s'adjuntarà a l'atestat així com la resta d'indicis per investigar (impressions, fotografies, etc.). C.3 Investigació dels fets: la Instrucció 2/2011, d'11 d'octubre de 2011, de la Fiscalia General de l'Estat sobre el fiscal de sala de Criminalitat Informàtica i les seccions de criminalitat informàtica de les fiscalies, en l'apartat de funcions de les seccions territorials de criminalitat informàtica, fa referència a les unitats especialitzades de les forces i cossos de seguretat de l'Estat o, si escau, de les policies autonòmiques per garantir l'eficàcia exigible en les investigacions sobre fets il·lícits relacionats amb la criminalitat informàtica. Els cossos de la Policia Local han de traspasar els atestats relatius a criminalitat informàtica (denúncies, manifestacions, documents d'interès, identificacions, etc.) a les unitats especialitzades del Cos Nacional de Policia o de la Guàrdia Civil, segons la zona, així com indica la Instrucció de la Fiscalia General de l'Estat per a la seva investigació. — Intervenció de dispositius informàtics o de comunicació: En el cas d'intervenció de dispositius informàtics (ordinadors portàtils, tauletes tàctils, etc.) o de comunicació (telèfons mòbils, telèfons intel·ligents...) com a indicis de presumptes delictes, és important en aquest cas mantenir la cadena de custòdia d'aquests elements, per la qual cosa s'han de lliurar a les unitats policials especialitzades de l'Estat o al jutjat de guàrdia. NO es podrà accedir al contingut d'aquests dispositius si s'infringeix el dret fonamental al secret de les comunicacions (telefonades rebudes, missatges, correus electrònics, etc.).	
2	Actuació IMMEDIATA de la Policia Local en fets delictius, en els quals s'han fet servir tecnologies de la informació i comunicació (TIC) a) Investigació dels fets i actuació en relació amb els presumptes autors en delictes propis o no de la criminalitat informàtica: una vegada comprovats els fets descrits per la víctima i tenint els indicis necessaris, i	

	si es constata que els fets són constitutius d'un presumpte delictes, amb els presumptes autors localitzats, per la mateixa manifestació de la víctima o per la manifestació de testimonis, o bé per altres vies, s'ha de citar el presumpte autor a les dependències policials per prendre-li manifestació sobre els fets succeïts, o es donarà trasllat de les diligències al Cos Nacional de Policia o de la Guàrdia Civil, segons zona, per continuar amb la instrucció de l'atestat policial. S'han de tenir en compte els delictes que són tramitats mitjançant judicis ràpids. Cal tenir en compte el que estableix la Llei de responsabilitat penal del menor com a presumptes autors de fets delictius, i s'ha de recordar que per imputar un delictes s'ha de tenir l'edat penal (14 anys complits). Si el presumpte autor és menor d'edat i major de 14 anys, ha de comparèixer acompanyat de l'advocat particular o d'ofici i dels seus representants legals per prendre-li manifestació. b) Detenció dels presumptes autors per part de la Policia Local: en el cas que no es traspassi l'atestat inicial a les forces i cossos de seguretat de l'Estat, i una vegada verificada la implicació dels presumptes autors, se'ls imputarà el fet delictiu amb la lectura dels seus drets, i en el cas de delictes, es farà de la manera següent: — Lectura dels drets segons l'article 520 i següents de la LECr. — En el cas de menors d'edat, l'advocat es podrà entrevistar amb ell/ella abans de fer l'exploració. — Avís als pares/mares o tutors legals sobre la situació del seu fill/a. — Avís a la Fiscalia de Menors i atenció a les seves indicacions, o al jutjat d'instrucció segons l'edat del presumpte/s autor/s. — Cal recordar que el temps màxim de detenció d'un menor d'edat és de 24 hores, i el d'una persona major d'edat és de 72 hores, i s'ha de tenir en compte que no es podrà mantenir una persona detinguda més temps de l'estrictament necessari per a la realització de les gestions per esclarir els fets presumptament succeïts. Una vegada detingut el presumpte autor dels fets, serà traspassat a les forces i cossos de seguretat de l'Estat o al jutjat de guàrdia o a la Fiscalia de Menors, segons la seva edat, seguint el procediment habitual en cada cas de la Policia Local i segons el fet delictiu.	LO 10/1995 DEL CODI PENAL LO 5/2000 RPM LECr.
3	Tramitació d'atestats per fets delictius a través de les TIC En els delictes comesos mitjançant les noves tecnologies de la informació i comunicació (TIC) s'ha d'indicar a la caràtula de l'atestat el símbol "@" i l'epígraf "CRIMINALITAT INFORMÀTICA" sota el símbol, a la part superior dreta del document inicial, segons mostra la figura les unitats especialitzades en criminalitat informàtica:	

	 — Tramitació atestats: Al jutjat d'instrucció de guàrdia de cada partit judicial i a la Fiscalia de: Manacor } Eivissa } a cada fiscalia del partit judicial. Menorca } Inca } Palma } a la Fiscalia de Criminalitat Informàtica (Edifici de sa Gerreria). En el cas d'haver d'iniciar diligències d'investigació per un fet delictiu relacionat amb les TIC, s'enviarà una còpia de la denúncia del perjudicat o de les primeres diligències a la fiscalia corresponent de cada zona. En el cas de la Policia Local, s'enviarà l'atestat o primeres diligències a: a) Tramitació de diligències a les forces i cossos de seguretat de l'Estat; aquests són els responsables de la tramitació judicial. b) Tramitació directa de diligències al jutjat d'instrucció i a la fiscalia corresponent.	
4	Catàleg inicial de delictes als quals s'estén el marc competencial de l'àrea de criminalitat informàtica, segons la Instrucció 2/2011 de la Fiscalia General de l'Estat a) Delictes en els quals l'objecte de l'activitat delictiva són els mateixos sistemes informàtics o les TIC — Delictes de danys, sabotatge informàtic i atacs de denegació de serveis prevists i penats en l'article 264 i concordants del Codi penal. — Delictes d'accés sense autorització a dades, programes o sistemes informàtics prevists i penats en l'article 197.3 del Codi penal. — Delictes de descobriment i revelació de secrets de l'article 197.1 del Codi penal comesos a través de les TIC o l'objecte dels quals siguin dades que es trobin registrades en fitxers o suports informàtics electrònics o telemàtics. — Delictes de descobriment i revelació de secrets d'empresa prevists i penats en l'article 278 del Codi penal comesos a través de les TIC o l'objecte dels quals siguin dades que es trobin registrades en fitxers o suports informàtics o electrònics. — Delictes contra els serveis de radiodifusió i interactius prevists i penats en l'article 286 del Codi penal. b) Delictes en els quals l'activitat criminal fa servir els avantatges que	LO 10/1995 DEL CODI PENAL

	ofereixen les TIC per executar-los — Delictes d'estafa prevists i penats en l'article 248.2, lletres <i>a</i>, <i>b</i> i <i>c</i>, del Codi penal, sempre que en els supòsits <i>a</i> i <i>c</i> s'utilitzin les TIC per portar a efecte la transferència o operació de qualsevol tipus en perjudici d'un altre. — Delictes de persecució de menors de 16 anys —<i>child grooming</i>— prevists i penats en l'article 183 bis del Codi penal quan es porti a efecte a través de les TIC. — Delictes de corrupció de menors o de persones discapacitades o relatives a pornografia infantil o referida a persones discapacitades prevists i penats en l'article 189 del Codi penal quan per desenvolupar o executar l'activitat delictiva s'utilitzin les TIC. — Delictes contra la propietat intel·lectual dels articles 270 i següents del Codi penal quan es cometin utilitzant les TIC. c) Delictes en els quals l'activitat criminal, a més de fer servir els avantatges que ofereixen les TIC per executar-los, comporta una especial complexitat en la seva investigació que requereix coneixements específics en la matèria — Delictes de falsificació documental dels articles 390 i següents del Codi penal quan per a l'execució del delicte s'hagin emprat les TIC, sempre que la circumstància esmentada sigui determinant en l'activitat delictiva i generi especial complexitat tècnica en la investigació criminal. — Delictes d'injúries i calúmnies contra funcionari públic, autoritat o agent d'aquesta prevists i penats en els articles 211 i següents del Codi penal comesos a través de les TIC, sempre que la circumstància esmentada sigui determinant en l'activitat delictiva i generi especial complexitat en la investigació criminal. — Delictes d'amenaques i coaccions prevists i penats en els articles 169 i següents del Codi penal comesos a través de les TIC, sempre que la circumstància esmentada sigui determinant en l'activitat delictiva i generi especial complexitat en la investigació criminal. — Delictes contra la integritat moral prevists i penats en l'article 173.1 del Codi penal comesos a través de les TIC, sempre que la circumstància esmentada sigui determinant en l'activitat delictiva i generi especial complexitat en la investigació criminal. — Delictes d'apologia o incitació a la discriminació, l'odi i la violència o de negació o justificació dels delictes de genocidi prevists i penats en els articles 510 bis i 511 del Codi penal comesos a través de les TIC, sempre que la circumstància esmentada sigui determinant en l'activitat delictiva i generi especial complexitat en la investigació criminal. — Qualsevol altre tipus delictiu en l'execució del qual hagi estat determinant la utilització de les TIC i en què la circumstància esmentada generi una especial complexitat en la investigació criminal.	
5	Unitats específiques de delictes informàtics de les forces i cossos de	

	seguretat de l'Estat a les Illes Balears — Cos Nacional de Policia C/ Ruiz de Alda, 8 07011 Palma Tel. 971 225 200 a/e: mallorca.delineco@policia.es — Guàrdia Civil Camí de Son Rapinya, 3-5 (direcció provisional) 07013 Palma Tel. 971 288 303 a/e: ib-cmd-palmamallorca-pj@guardiacivil.org	
6	Fiscalia de delictes informàtics a les Illes Balears Travessia d'en Ballester, 20 07002 Palma Tel. 971 219 443 Fax: 971 219 482 a/e: jose.diaz@fiscalia.mju.es	
7	Glossari cibernètic <i>Ciberassetjament escolar</i> —en anglès, <i>cyberbullying</i>—: terme que fa referència a l'acte de turmentar i molestar una altra persona fent servir mitjans electrònics com ara el correu electrònic, el xat, els blogs, els llocs webs, els missatges SMS, entre d'altres. <i>Ciberassetjament a menors</i> —en anglès, <i>grooming</i>—: consisteix en accions deliberades per part d'una persona adulta amb l'objectiu d'establir llaços d'amistat amb un menor mitjançant Internet per obtenir una satisfacció sexual a través d'imatges eròtiques o pornogràfiques seves o, fins i tot, com a preparació d'una trobada amb finalitats sexuals. <i>Falsa alarma</i> —en anglès, <i>hoax</i>—: són missatges de correu electrònic amb contingut fals, però sobretot atractius. Normalment són distribuïts en cadena pels successius receptors, atès el seu contingut impactant que simula sorgir d'una font d'informació fiable i seriosa, o perquè el mateix correu sol·licita ser reenviat. <i>Programa maliciós</i> —en anglès, <i>malware</i>—: qualsevol programa que tenguin per objecte fer malbé ordinadors, sistemes informàtics o xarxes, i també els seus usuaris. <i>Pesca</i> —en anglès, <i>phishing</i>—: fa referència a comunicacions fraudulentament dissenyades per induir els consumidors a divulgar informació de tipus personal, financera, bancària o sobre els seus comptes d'Internet (usuaris, contrasenyes, dades de les targetes bancàries...). <i>Correu brossa</i> —en anglès, <i>spam</i>—: enviament massiu i indiscriminat i no sol·licitat de publicitat mitjançant el correu electrònic. També són utilitzats a través del telèfon mòbil mitjançant missatges SMS.	

<i>Troia</i>: programa informàtic que conté la lògica necessària perquè el seu creador pugui accedir a l'interior del sistema d'un usuari i a la seva informació. <i>Sexting</i>: és un manlleu de l'anglès que uneix "sex" ('sexe') i "texting" ('enviament de missatges de text via SMS des de telèfons mòbils'). Encara que el sentit original es limitava a l'enviament de texts, el desenvolupament dels telèfons mòbils ha fet que actualment aquest terme s'apliqui a l'enviament, especialment mitjançant el telèfon mòbil, de fotografies i vídeos amb contingut de cert nivell sexual, gravades pel seu protagonista.		
Procediment elaborat pel coordinador del Programa Policia Tutor  Rafel Covas Femenia	Procediment revisat pel director de l'ISPIB  Vicenç Martorell Palou	Procediment aprovat pel director general d'Emergències i Interior  Jaime Barceló Huguet

Diligència de validació: el present protocol ha estat revisat i validat pel Fiscal delegat de Criminalitat Informàtica de la Fiscalia General de les Illes Balears, Sr. José Díaz Cappa, que ha participat en la seva redacció (11/01/2013).

