UNIVERSITAT DE BARCELONA

Estudi i anàlisi de la cultura de la ciberseguretat dins la Policia de la Generalitat - Mossos d'Esquadra Reptes actuals i futurs

Marc Tortellà i Muns

Tutor: Jordi Vilardell i Molas

Juny de 2018

Treball Final de Màster

Màster en Direcció Estratègica de Seguretat i Policia

Facultat de Dret. Universitat de Barcelona

Agraïments

Al meu tutor del TFM, Jordi Vilardell, per la seva orientació i dedicació per tal d'assessorar-me i guiar-me en la seva redacció. El seus amplis coneixements de lideratge i gestió de persones i equips han estat sens dubte una font d'aprenentatge i de recursos inesgotable.

A l'Institut de Seguretat Pública de Catalunya per facilitar-me al màxim la realització d'aquests estudis enfocats a la direcció estratègica policial amb l'objectiu millorar la meva formació i capacitació professional.

Al Comissari Xavier Porcuna, per confiar amb mi i introduir-me en el món de les tecnologies i telecomunicacions policials. Una oportunitat que ha estat cabdal dins el meu futur professional.

A l'Intendent Ramón Tomàs, per ajudar-me de manera inestimable a realitzar aquest Màster, amb la paciència i serenor només reservada als grans gestors policials.

Als meus pares Bartomeu i Mercè, per inculcar-me els valors del treball i de l'esforç com a essència de millora contínua com a professional i com a persona.

A la meva dona Carolina Valenzuela i als meus fills Marc i Alba, que són la llavor de la meva inspiració i allò pel qual respiro i visc dia rere dia. D'ells aprenc contínuament i m'impregnen constantment del valor més important a la vida, l'amor de família.

Resum

La cultura en ciberseguretat és un concepte relativament nou de no fa més d'una dècada. Arran de l'aparició de normativa en referència a les obligacions de les administracions envers la seguretat digital en les seves infraestructures i l'aplicació de la protecció de dades envers el servei que es dona al ciutadà tant en l'àmbit públic com el privat, així com la creació d'estructures estatals per enfortir l'administració pública enfront els nous reptes digitals, ha fet que les organitzacions d'arreu de l'estat, on s'inclouen el cos dels Mossos d'Esquadra, hagin fet un esforç per situar-se dins uns alts nivells de competència per, d'una banda protegir les seves infraestructures i les dades amb informació sensible que gestionen i d'altra banda enfortir la resiliència de l'organització envers un ciberatac dirigit.

Aquest nou escenari d'operacions on les ciberamenaces i la criminalitat mitjançant el món virtual creixen exponencialment any rere any, ha fet que dins la policia catalana es creï una cultura de ciberseguretat pròpia. Per tal d'estudiar-la, s'ha analitzat el context professional on es fa necessària la creació, la normativa que li aplica des d'una vessant pràctica, com es genera, quin elements la conformen, cap a on està orientada, quina conscienciació crea i quines perspectives estratègiques de futur té per mantenir-la.

Alhora també s'ha analitzat i comparat sota el prisma dels tres nivells de cultura organitzacional que defineix l'autor Edgar Schein i mitjançant un qüestionari s'ha determinat si la cultura en ciberseguretat ha arrelat a la organització i si s'ha adequat a les premisses i nivells que assenyala l'autor.

Paraules clau: ciberseguretat, cultura, conscienciació, organització, dades, ciberamenaces

Abstract

The culture in cybersecurity is a relatively new concept, existing for less than a decade. Following the appearance of regulations, in reference to the obligations of the administrations towards digital security in their infrastructures and the application of the protection of data regarding the service, that is given to citizens both in the public and private fields, the creation of state structures to strengthen the public administration against the new digital challenges have made organizations from all over the state, which include catalan police-Mossos d'Esquadra, make an effort to situate at high levels of competition to, on the one hand, protect their infrastructures and data with sensitive information that they manage and on the other hand strengthen the resilience of the organization towards a targeted cyber attack.

This new stage of operations where cyber threats and criminality through the virtual world grow exponentially year after year has led to the creation of a culture of cybersecurity within the catalan police. In order to study it, the professional context where creations is necessary has been analyzed where we, the regulators who apply it from a practical point of view, how it is generated, what elements become part of, where it is oriented, what kind of awareness is created and what future strategic perspectives have to keep it.

At the same time, it has also been analyzed and compared under the prism of the three levels of organizational culture defined by author Edgar Schein. Through a questionnaire, it has also been determined whether the culture in cybersecurity has rooted in the organization, and whether it has been adapted to premises and levels that the author mentioned.

Keywords: cybersecurity, culture, awareness, organization, data, cyber threats

UNIVERSITAT DE BARCELONA

Sumari

UNIVERSITAT DE BARCELONA

Glosari de figures

Llista d'abreviacions

Abreviació	Desenvolupament
ABP	Àrea bàsica policial
APT	Advanced persistent threat
CERT	Centre d'emergència i resposta temprana
CESICAT	Centre de seguretat de la informació de Catalunya
CGIC	Comissaria general d'investigació criminal
CGINF	Comissaria general d'informació
CGRO	Comissaria general de recursos operatius
CGTSE	Comissaria general de planificació de la seguretat
CTTI	Centre de telecomunicacions i tecnologies de la informació
DGP	Direcció general de la policia
DSIP	Divisió de sistemes d'informació policial
ENS	Esquema nacional de seguretat
ISPC	Institut de seguretat pública de Catalunya
OAC	Oficina d'atenció al ciutadà
PG-ME	Policia de la Generalitat-Mossos d'Esquadra
LPAC	Llei del procediment administratiu comú de les administracions públiques
SGSI	Sistema de gestió de seguretat de la informació
SIP	Sistemes d'informació policial
TIC	Tecnologies de la informació i comunicació
UCIBER	Unitat de ciberseguretat policial
WiFi	Wireless Fidelity

1 Introducció

La ciberseguretat és un concepte relativament nou nascut en ple segle XXI. Aquest terme deriva de la seguretat de la informació i ha anat evolucionant amb el temps, ja que les organitzacions no només protegeixen la informació que generen i que emmagatzemen, sinó que també han protegir la infraestructura tecnològica que la suporta.

Aquesta ràpida evolució ha fet que les organitzacions i empreses s'hagin adaptat progressivament modificant la seva morfologia per ser més eficaços envers la protecció dels seus actius i la continuïtat de negoci. Aquest nou paradigma també ha afectat a les organitzacions policials que han hagut d'adaptar-se ràpidament a aquests nous canvis, passant en poc temps d'un món analògic a un digital en la seva àmplia globalitat i complexitat.

En aquest treball de fi de Màster i com a responsable policial en l'àmbit de la ciberseguretat, pretenc estudiar com s'ha adaptat el cos dels Mossos d'Esquadra a aquestes noves amenaces cibernètiques, com s'ha hagut d'organitzar en la cerca constant de millora i optimització de recursos i quines mesures ha hagut de prendre per tal de crear una nova cultura en ciberseguretat.

L'etapa de generació d'aquesta cultura, juntament amb l'anàlisi del conjunt d'elements que la conformen així com la seva orientació envers a tots els usuaris, són eixos vertebradors d'aquest nou model policial de seguretat de la informació que ha anat impregnant a les policies capdavanteres d'arreu del món. Accions en formació i conscienciació en seguretat, l'establiment de polítiques internes dins l'organització i la supervisió constant dels actius, fan de la tasca diària un repte continu de millora i d'eficiència.

En aquest escenari de continu canvi de les tecnologies de la informació també analitzaré des d'una perspectiva d'anàlisi estratègica, quins àmbits de millora existeixen i com pot evolucionar aquest cos policial des de diferents vessants als nous reptes del futur de la cultura de ciberseguretat, tant sigui des d'un prisma d'augment de capacitats, com de millores en polítiques i configuracions de seguretat com en la de consolidació dels compromisos de l'alta direcció envers els nous reptes cibernètics.

Alhora m'he proposat comprovar fins a quin grau divergeix la visió d'aquells que generen aquesta cultura respecte d'aquells que la reben, ja estiguin destinats en serveis centrals especialitzats com en serveis territorials realitzant tasques de patrullatge ordinari de seguretat ciutadana. Tanmateix, servirà per comprovar si efectivament s'ha consolidat una cultura de ciberseguretat dins el cos policial català o pel contrari encara queda un llarg camí per recórrer dins l'essència de la cultura de les organitzacions i els seus diferents nivells que desgranaré a continuació durant el treball.

Per aquests motius, he desgranat en quatre punts els objectius bàsics que cerca aquest

treball, essent principalment destacables els següents que es relacionen a continuació.

Objectius:

- Analitzar com s'ha creat la cultura de ciberseguretat dins la policia autonòmica catalana
- Identificar els elements que la desenvolupen dins la recentment creada Unitat de Ciberseguretat Policial
- Detallar les estratègies per mantenir-la durant el temps i com pot evolucionar per millorar i adaptar-se als nous reptes de futur
- Verificar si hi ha diferència de visions entre la Unitat que vetlla per la ciberseguretat dins la policia i la resta d'Unitats que la reben com a producte. L'empremta.

2 Evolució de l'analogia a la digitalització dins la policia

2.1 Context professional

2.1.1 Policial

Els inicis de les primeres promocions de la PG-ME, durant els anys 80, foren purament analògics, on els atestats policials es confeccionaven amb màquines d'escriure convencional i calca de carboni per entregar còpies al Ministeri Fiscal, a l'interessat i còpia per l'arxiu. No obstant això, les competències que en disposava el cos eren purament anecdòtiques, reduïdes a tasques de vigilància d'edificis oficials, com ara Palau de la Generalitat i Parlament.

Arran de l'entrada en vigor de la llei 10/94[1] de la policia de la Generalitat - Mossos d'Esquadra, es comença el desplegament, en forma de taca d'oli, arreu del territori català. Dins els calendari, s'establí la comarca d'Osona com a primera seu de la primera Àrea Bàsica Policial (ABP) de la Policia de la Generalitat- Mossos d'Esquadra (PG-ME).

En aquells temps, tota dada de caràcter personal s'emmagatzemava en els llibres oficials de la comissaria -llibres de detinguts, llibres d'identificacions de l'Oficina d'Atenció al Ciutadà (OAC) i arxius de ressenyes de les persones detingudes- els quals restaven en custòdia dels responsables policials de torn durant les 24 hores.

La màxima preocupació en aquell moment, a part de la qualitat de la dada, era el trencament d'alguna plana del llibre, les errades de transcripció i posterior esmenat amb el bolígraf o com a factor crític, la pèrdua o sostracció d'un d'aquests llibres.

És doncs als inicis de la dècada del '90 on s'establí un nou programa revolucionari que per primer cop, arreu de l'estat espanyol, s'implantava a la policia en ple procés d'informatització. El programa conegut con "Arnau[2]", s'establia ja com un primer pas al procés d'informatització, on les diligències amb un nou editor de text ja estaven preestablertes i només calia annexar-les i omplir els camps amb dades personals. L'any 1994, s'obrí la primera comissaria de desplegament de la PG-ME, l'ABP Osona, situada a la localitat de Vic.

Aquest primer pas dins l'Oficina d'Atenció al Ciutadà (OAC), també s'incorporà posteriorment a les Sales de Comandament Policial, on mitjançant un programa informàtic era capaç de emmagatzemar la gestió de les patrulles i els incidents als quals hi assistien.

Però no és fins el 2001, que neix el que és conegut oficialment con Sistemes d'Informació Policial (SIP), que aglutina en un mateix conjunt, una suma d'aplicacions policials que conformen un ampli espectre, tant en l'àmbit purament policial, com en el administratiu i el

[1] LLEI 10/1994, d'11 de juliol, de la policia de la Generalitat - Mossos d'Esquadra en la qual es crea la policia catalana i es refon històricament amb els seus origens del segle XVIII. Disponible a: http://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_resultats_fitxa/?documentId=93461&action=fitxa

[2] Sobrenom amb el que es coneixia el primer editor de diligències policials de la PG-ME

d'investigació. És doncs, l'impuls definitiu cap a una digitalització global de la policia a Catalunya

A data d'avui s'aglutinen un total de 82 aplicacions policials que donen servei a 17000 policies autonòmics i 11000 policies locals connectats als SIP distribuïts en 206 ajuntaments[3].

2.1.2 Organització

Aquest canvi de paradigma produït per un nou escenari, juntament amb l'aparició d'una nova normativa (LOPD 1999) que tractarem més endavant, farà que les rutines i mecàniques dels agents del cos de la PG-ME primerament i després de les policies local canviïn radicalment, donat que:

- Els SIP són centralitzats i consultables des de qualsevol part del territori
- L'accés a la informació, modificació o esborrat queda plenament auditat
- No cal còpia d'arxiu i en cas de necessitar-la, se'n pot imprimir un esborrany
- Les diligències i el cos de l'atestat es configuren en una preforma, per tal d'evitar els errors involuntaris o els oblits d'informació dels agents
- La informació, en cas de pèrdua o esborrada involuntària es pot recuperar mitjançant les còpies d'arxiu
- Les dades de les aplicacions són comunes entre elles, les dades que s'introdueixen en una com a marca, serveixen també per les altres

És doncs un procés, el de la digitalització, certament idíl·lic on tot són avantatges més enllà d'haver de realitzar una forta inversió econòmica i fer un esforç de canvi d'inèrcies de treball.

2.1.3 Estructural

Per tal d'adequar-se a aquest nou escenari, es crea el 2001 la Divisió del Pla Informàtic (DPI), que serà l'embrió de la posterior Divisió de Sistemes d'Informació Policial (DSIP) i en el qual es generen les primeres adequacions a la Llei Orgànica de Protecció de Dades (LOPD[4]) de 1999, la organització de processos en la informatització de l'activitat policial, i la planificació i distribució dels equips informàtics, pantalles i impressores arreu de les comissaries.

Agents que estaven al carrer, passen a formar-se en la gestió i organització d'una nova estructura policial, sense la qual, no es pot endegar aquest nou repte del segle XXI.

---

[3] Actualment un 97,63% dels ajuntaments amb policia local esta connectats als SIP

[4] Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. Disponible a: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

Amb el pas dels anys, la nova DSIP, s'encarregarà del disseny i impuls de nous projectes informàtics, de la gestió, distribució i anàlisi de les dades d'activitat policial, i de la seguretat lògica dels arxius informàtics així com la vetlla del bon ús dels SIP. Aquest canvi estructural es detallarà, primerament amb el Decret 243/2007[5], de 6 de novembre, d'estructura del Departament d'Interior, Relacions Institucionals i Participació, ja derogat, i posteriorment en una el Decret 415/2011, que és l'actualment en vigor i on s'ordena cada funció en Àrees i Unitats policials.

En aquest treball i a mode descriptiu, la Divisió de Sistemes d'Informació Policial (DSIP) s'estructura en 3 Àrees centrals.

- Àrea de Coordinació de Projectes dels Sistemes d'Informació Policial (ACSIP)
- Àrea d'Elaboració de Dades Policials (AEDP)
- Àrea de Seguretat en Tecnologies de la Informació (ASTI).

Alhora, cada àrea policial s'estructura en unitats policials que fins i tot es poden dividir en varis grups, en el cas que ens ocupa l'ASTI es divideix en:

- La Unitat de Gestió d'Usuaris (UGU) que gestiona els accessos dels usuaris a les aplicacions policials i assigna el nivell de privilegi necessari depenent de la funció i tasques assignades a l'usuari.
- La Unitat d'Auditories (UAD) que realitza les auditories dels sistemes policials en relació a la correcta utilització de les aplicacions informàtiques.
- La Unitat de Ciberseguretat Policial (UCIBER) que dissenya i avalua els mecanismes necessaris per a la seguretat dels sistemes d'informació policial.

Al llarg d'aquest treball s'anomenarà principalment la UCIBER com a mostra d'una unitat de nova creació i que respon a unes necessitats molt concretes de l'organització que desenvoluparem més endavant.

2.2 Context legal

Abans de començar a parlar de les normes aplicables a la ciberseguretat, primer cal definir què és la ciberseguretat. Segons el diccionari del centre nord-americà National Initiative for

[5] DECRET 243/2007, de 6 de novembre, d'estructura del Departament d'Interior, Relacions Institucionals i Participació. Disponible a : http://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_resultats_fitxa/?action=fitxa&versionId=1520856&versionState=02&language=ca_ES&documentId=423614&mode=single

Cybersecurity Careers and Studies[6] (NICCS), ens adscrit al Departament de Seguretat Nacional, la ciberseguretat és "l'activitat o procés, capacitat o estat pel qual els sistemes d'informació i comunicacions i la informació continguda en ells estan protegits i/o defensats contra danys, ús no autoritzat, modificació o explotació. "

És a dir, es pot dir que la ciberseguretat són aquelles mesures destinades a protegir els usuaris i empreses que operen a Internet. En realitat, la ciberseguretat s'inscriu dins un concepte més ampli de la seguretat de la informació, l'objectiu el qual és protegir la informació digital de sistemes que es troben interconnectats.

Existeixen també altres conceptes relacionats a la ciberseguretat, com poden ser el cibercrim, les ciberamenaces o el ciberespai, la característica principal i comuna resideix en l'existència dels mateixos a la xarxa. Ho definirem doncs de la següent manera:

Cibercrim: Consisteix en totes aquelles conductes delictives que es practiquen mitjançant l'aprofitament de la xarxa.

Ciberamenaces: Són les possibilitats de comissió de danys a persones o organismes mitjançant l'ús d'Internet.

Ciberespai: És aquella realitat simulada implementada dins dels ordinadors i xarxes digitals existents a nivell mundial, sent un concepte més ampli que el propi Internet.

En definitiva, la ciberseguretat el que pretén és protegir-nos davant d'atacs o actuacions il·legals o il·lícites de tercers a la xarxa.

Per tal d'adaptar-nos als nous reptes, cada estat i de retruc la Unió Europea crea normatives, que segons l'àmbit d'actuació es detallen a continuació.

2.2.1 Normes Autonòmiques

2.2.1.1 CME

És indiscutible la importància capital per a una organització com la Policia de la Generalitat – Mossos d'Esquadra el valor que cal atorgar als sistemes d'informació/tecnologies de la informació (SI/TI), l'article 76.1 del Decret 415/2011[7], de 13 de desembre, d'estructura de la funció policial de la Direcció General de la Policia atribueix a la Divisió de Sistemes d'Informació Policial (DSIP), entre d'altres, les següents funcions:

---

[6] National Initiative for Cybersecurity Carriers and Studies. Department of Homeland Security. Disponible a: https://niccs.us-cert.gov/glossary

[7] DECRET 415/2011, de 13 de desembre, d'estructura de la funció policial de la Direcció General de la Policia, article 76.2b i 78 Disponible a: http://dogc.gencat.cat/ca/pdogc_canals_interns/pdogc_resultats_fitxa/?action=fitxa&mode=single&documentId=594021&language=ca_ES

a) Vetllar, amb la resta d'òrgans competents en matèria de sistemes d'informació, pel control de la seguretat d'aquests sistemes, la integritat de les seves dades i l'eficiència de la seva explotació.

b) Executar la inspecció i la realització d'auditories en relació amb la correcta utilització de les aplicacions informàtiques i l'alimentació de les bases de dades de caràcter policial.

El mateix text legal atribueix en el seu article 78 les següents funcions a l'Àrea de Seguretat en Tecnologies de la Informació (ASTI):

a) Dissenyar, implantar, gestionar i avaluar els mecanismes necessaris per a la seguretat dels sistemes d'informació policial, així com l'assegurament de la utilització de les dades de caràcter personal d'acord amb el que estableix la normativa vigent en aquesta matèria.

b) Gestionar l'assignació d'usuaris i els perfils i nivells d'accés als sistemes d'informació de la Direcció General de la Policia.

c) Exercir qualsevol altra funció de naturalesa anàloga que li encomanin.

S'ha de tenir en compte però, que existia en aquell moment una important asimetria entre les funcions enumerades en el Decret 415/2011 i les actuals funcions operatives de l'ASTI que es veuen limitades als punts b) de l'article 76.1 i punt b) de l'article 78.

2.2.1.2 CESICAT

Un actor de gran rellevància per la PG-ME, és el Centre de Seguretat de la Informació de Catalunya (CESICAT) com a Centre d'Emergència i Resposta Temprana[8] (CERT) de referència per l'administració pública a Catalunya. Mitjançant l'acord GOV/103/2012[9], de 16 d'octubre, pel qual s'encarrega a la Fundació la planificació, la gestió i el control de la seguretat de les TIC de l'Administració de la Generalitat i el seu sector públic, el CESICAT es responsabilitza de l'establiment i el seguiment dels programes d'actuació corresponents del Pla, sota la direcció estratègica del Govern de la Generalitat, col·laborant amb les entitats del sector públic de l'Administració de la Generalitat, els governs locals de Catalunya, del sector privat i de la societat civil per tal d'assolir els següents objectius:

a) Establiment i execució d'una estratègia nacional de seguretat TIC.

b) Suport a la protecció de les infraestructures crítiques TIC nacionals.

[8] Un CERT és un centre de resposta a incidents de seguretat en tecnologies de la informació format per experts responsables del desenvolupament de mesures preventives i reactives davant incidents de seguretat dels sistemes d'informació

[9] ACORD GOV/103/2012, de 16 d'octubre, pel qual s'encarrega a la Fundació Centre de Seguretat de la Informació de Catalunya la planificació, la gestió i el control de la seguretat de les TIC de l'Administració de la Generalitat i el seu sector públic. Disponible a: https://ciberseguretat.gencat.cat/web/.content/PDF/ACORD-GOV1032012.pdf

c) Promoció d'un teixit empresarial català sòlid en seguretat TIC.

d) Increment de la confiança i protecció de la ciutadania catalana en la societat de la informació.

La Fundació CESICAT, en el marc de les funcions que li són pròpies, d'acord amb els seus estatuts aprovats mitjançant un Acord de Govern de 22 de desembre de 2009[10] i l'objectiu primer del Pla de seguretat de la informació de Catalunya, és l'ens idoni per gestionar les tasques necessàries per assolir aquest objectiu de protecció de la informació i la infraestructura TIC de les institucions i ciutadans de Catalunya i, en especial, de la del Govern de la Generalitat.

Per aquet motiu se li assignen les següents funcions:

a) La planificació, gestió i control de la seguretat de les TIC de l'Administració de la Generalitat i el seu sector públic, i encarregar a l'òrgan rector de la Fundació que impulsi les mesures necessàries per dur-la a terme.

b) Que el CESICAT i el Centre de Telecomunicacions i Tecnologies de la Informació[11] (CTTI) es coordinin en la relació amb l'Administració de la Generalitat i el seu sector públic, de manera que el CTTI centralitzi la interlocució administrativa i el CESICAT, la interlocució operativa de la seguretat TIC.

2.2.2 Normes estatals

Com un inici de la repercussió que l'administració electrònica produiria dins la gestió de l'Administració pública, en el seu article 6 de la Llei 11/2007[12], de 22 de juny, d'accés electrònic dels ciutadans als serveis públics i el seu Reial decret de desplegament 3/2010, de 8 de gener, aplicable a totes les Administracions públiques territorials i als organismes i entitats de dret públic que en depenen, reconeixien ja veritables drets dels ciutadans en relació amb la seguretat, on s'emmarcaven principalment:

a) La garantia de la seguretat i confidencialitat de les dades

b) La obtenció dels mitjans d'identificació electrònics necessaris. DNIe

c) La utilització d'altres sistemes de signatura electrònica admesos

[10] Acord de Govern GOV 50/2009 en el qual es fa referència a Acord 103/2012. Disponible a: https://ciberseguretat.gencat.cat/web/.content/PDF/ACORD-GOV1032012.pdf

[11] ACORD GOV/53/2009, de 24 de març, pel qual s'encarrega la prestació de serveis de tecnologies de la informació i comunicacions al Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya. Disponible a: http://portaldogc.gencat.cat/utilsEADOP/AppJava/PdfProviderServlet?versionId=997618&type=01

[12] Ja derogada quan va entrar en vigor la Llei 39/2015, de 1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPAC)

En una continua evolució legislativa, va entrar en vigor la Llei 39/2015, de 1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPAC)[13], derogant l'antiga Llei 11/2007 en la qual tractava especialment els següents punts:

- Comunicacions per via electrònica en les relacions dels interessats amb les Administracions Públiques on les persones físiques podien triar si, per a l'exercici dels seus drets i obligacions amb les administracions públiques, es comunicaven a través de mitjans electrònics o no, si bé el mitjà triat podia ser modificat en qualsevol moment. També, pel que fa a les comunicacions entre els interessats i les administracions públiques, destacava la utilització de la signatura electrònica pels interessats.

- Utilització de mitjans electrònics en la tramitació de procediments administratius on s'establia l'obligació per a les administracions públiques de comptar amb un registre electrònic general o, si s'escau, adherir-se al de l'Administració General de l'Estat. El registre electrònic va permetre la presentació de documents tots els dies de l'any durant les 24 hores, si bé la presentació d'escrits en un dia inhàbil s'entenia realitzada en la primera hora del primer dia hàbil següent.

- Nou règim de notificacions electròniques. D'entre les novetats de la LPAC en matèria d'Administració electrònica, mereixien també una menció singular les novetats introduïdes en matèria de notificacions electròniques.

En aquest sentit, les notificacions s'havien de practicar, amb caràcter preferent, mitjançant la via electrònica, i es realitzaven a la seu electrònica de l'Administració corresponent. Tanmateix, la notificació electrònica es complementava amb la possibilitat que les notificacions es continuessin practicant en paper, si bé en aquest últim cas, hi havia el deure de que fossin posades a disposició de l'interessat a la seu electrònica de l'Administració corresponent.

Més enllà de l'afectació a les administracions públiques per donar servei al ciutadà, la llei d'administració electrònica va crear una dependència de les administracions i entitats en general al món cibernètic, fent que cada vegada més el tràmit en paper quedés desplaçat i amb tendència a l'obsolescència. La immediatesa i la facilitat d'ús han fet que el món lògic superi al físic.

Aquesta dependència va crear de retruc un nou tipus de vulnerabilitat a les administracions, ja que fer-se accessible a la ciutadania suposa fer-se accessible a qualsevol persona i ordinador del món, amb els perills que això comporta.

Per aquest motiu, l'any 2013 des del Consell de Seguretat Nacional, es contemplà la ciberseguretat dins dels seus dotze àmbits d'actuació amb el propòsit de fixar les directrius

[13] Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques. Disponible a: https://www.boe.es/boe_catalan/dias/2015/10/02/pdfs/BOE-A-2015-10565-C.pdf

generals de l'ús segur del ciberespai a través de l'impuls d'una visió integradora que garantís la seguretat i el progrés, assolint a través de l'adequada coordinació i cooperació entre totes les administracions públiques, però també entre aquelles amb el sector privat i amb els ciutadans.

I així durant l'any 2013, l'Estratègia de Seguretat Nacional[14] a través de la qual es va instar a l'administració pública a adoptar les mesures més adequades per protegir les dades personals, a realitzar una avaluació de l'impacte en la protecció de les dades personals i que posteriorment haurà d'esdevenir en un anàlisi de riscos, i gestionar aquests riscos mitjançant l'adopció de mesures necessàries per eliminar-los o mitigar-los. Es varen recollir les amenaces i els desafiaments que s'havien d'abordar a nivell de tot l'estat per tal de preservar la seguretat digital. I és per això, que van fixar un total de sis (6) objectius específics els qual s'enumeren a continuació:

1) per a les administracions públiques, garantir que els Sistemes d'Informació i Telecomunicacions posseeixen el nivell adequat de seguretat i resiliència

2) per a les empreses i les infraestructures crítiques, impulsar la seguretat i la resiliència de les xarxes i els sistemes d'informació usats pel sector empresarial en general i els operadors d'infraestructures crítiques en particular

3) en l'àmbit judicial i policial, potenciar les capacitats de prevenció, detecció, resposta, investigació i coordinació davant de les activitats del terrorisme i la delinqüència en el ciberespai

4) en matèria de sensibilització, conscienciar els ciutadans, professionals, empreses i administracions públiques espanyoles dels riscos derivats del ciberespai

5) en capacitació, aconseguir i mantenir els coneixements, habilitats, experiència i capacitats tecnològiques que necessita Espanya per sustentar tots els objectius de la ciberseguretat

6) pel que fa a la col·laboració internacional, contribuir en la millora de la ciberseguretat, donant suport al desenvolupament d'una política de ciberseguretat coordinada a la Unió Europea i en les organitzacions internacionals, així com col·laborar en la capacitació d'Estats que ho necessitin a través de la política de cooperació al desenvolupament

Així mateix, i mitjançant la ISO 27001[15] de seguretat de la informació a la qual es poden adaptar les empreses, es va determinar la preservació de la seva confidencialitat, integritat i disponibilitat, així com dels sistemes implicats en el seu tractament, dins d'una organització.

[14] Estratègia de Seguretat Nacional de 2013. Disponible a: http://www.dsn.gob.es/es/file/144/download?token=JdtEVkaN

[15] ISO 27001. Estàndard per la Seguretat de la Informació. Sistema de gestió de seguretat de la informació. Disponible: http://www.iso27000.es/download/doc_sgsi_all.pdf

Per garantir que la seguretat de la informació era gestionada correctament, els gestors de la seguretat havien d'identificar inicialment el seu cicle de vida i els aspectes rellevants adoptats per garantir la seva C-I-D, que en sigles es defineix com:

Confidencialitat: la informació no es posa a disposició ni es revela a individus, entitats o processos no autoritzats.

Integritat: manteniment de l'exactitud i completesa de la informació i els seus mètodes de procés.

Disponibilitat: accés i utilització de la informació i els sistemes de tractament de la mateixa per part dels individus, entitats o processos autoritzats quan ho requereixin.

Sobre la base del coneixement del cicle de vida de cada informació rellevant s'havia d'adoptar l'ús d'un procés sistemàtic, documentat i conegut per tota l'organització, des d'un enfocament de risc empresarial. Aquest procés es va desenvolupar sota el Sistema de gestió de seguretat de la informació (SGSI).

Per últim, i per tal d'acabar amb la recopilació de normativa estatal cal destacar que data d'avui, juny de 2018, es contempla com a referència per part de la UCIBER, el Codi de Dret de la Ciberseguretat[16], on es recull en un sol codi electrònic tota la normativa que afecta la ciberseguretat dividit en els següents eixos vertebradors:

. Constitució Espanyola

. Normativa de Seguretat Nacional

. Infraestructures crítiques

. Normativa de seguretat

. Equip de resposta a incidents de seguretat

. Telecomunicacions i usuaris

. Ciberdelinqüència

. Protecció de dades

. Relacions amb l'administració

Tot i la rellevància de la normativa que acabem de detallar, cal destacar que afecten especialment i específicament a l'hora de generar procediments interns dins la PG-ME, les següents normatives:

[16] Código del derecho de la ciberseguridad. Disponible a: https://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=173_Codigo_de_Derecho__de_la_Ciberseguridad.pdf

Normativa de Seguretat Nacional:

. Reial Decret 3/2010, de 8 de gener, pel que es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica

. Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Interoperatibilitat en l'àmbit de l'administració electrònica

Telecomunicacions i usuaris:

. Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic

. Llei 59/2003, de 19 de desembre, de firma electrònica

Protecció de dades:

. Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal

. Reial Decret 1720/2007, de 21 de desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal

Relacions amb l'administració:

. Llei 39/2015, d' 1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.

2.2.3 Normes Europees

El proppassat 25 de maig de 2018 va entrar en vigor el Reglament UE 2016/679[17] del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades.

Tal i com es descriu en les seves consideracions, mitjançant aquesta normativa es cerca de manera clara el garantir un nivell uniforme i elevat de protecció de les persones físiques i eliminar els obstacles a la circulació de dades personals dins de la Unió, el nivell de protecció dels drets i les llibertats de les persones físiques en el tractament d'aquestes dades, que ha de ser equivalent en tots els estats membres. Com a objectiu primari garantirà que l'aplicació de les normes de protecció dels drets i les llibertats fonamentals de les persones físiques en

[17] Reglament (UE) 2016/679 del Parlament europeu i del consell - de 27 d'abril de 2016 - relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46 / CE (Reglament general de protecció de dades). Disponible a: https://www.boe.es/doue/2016/119/L00001-00088.pdf

relació amb el tractament de dades de caràcter personal sigui coherent i homogènia a tota la Unió Europea.

Cal remarcar a més que la protecció que atorga aquest reglament s'aplica a les persones físiques, independentment de la seva nacionalitat o el seu lloc de residencia, en relació amb el tractament de les seves dades personals. El reglament no regula el tractament de les dades personals relatives a persones jurídiques i en particular a empreses constituïdes com a persones jurídiques. D'aquest punt en parlarem més endavant, ja que els usuaris apliquen una concepció genèrica a aquest aspecte, ampliant la normativa també a les persones jurídiques.

També cal tenir en compte que la protecció de les persones físiques en el tractament de dades de caràcter personal per part de les autoritats competents als efectes de la prevenció, la recerca, la detecció o l'enjudiciament d'infraccions penals o l'execució de sancions penals, inclosa la protecció davant de les amenaces contra la seguretat pública i la lliure circulació d'aquestes dades i la seva prevenció, és objecte d'un acte jurídic específic en l'àmbit de la Unió Aquest reglament no s'aplica a les activitats de tractament destinades a aquestes finalitats i les dades personals tractades per les autoritats públiques han de regir-se per un per la Directiva (UE) 2016/680 del Parlament Europeu i del Consell[18].

Com a avantatja per l'usuari i pels investigadors, val a dir que amb l'entrada en vigor del Reglament General de Protecció de Dades (RGPD), els usuaris europeus no seran privats del seu dret fonamental a la protecció de dades pel fet que l'empresa estigui ubicada fora de la Unió Europea, sempre que sigui una delegació que ofereixi béns o serveis -tot i siguin gratuïts-, o es dediqui al control del comportament de ciutadans europeus.

Dins els canvis que proporcionarà el RGPD, afectaran especialment a la policia catalana els següents ítems:

- Noves categories de dades de caràcter personal: les dades biomètriques (relatives a les característiques físiques, fisiològiques o conductuals d'una persona) i les dades genètiques (característiques heretades o adquirides, extretes d'una mostra biològica).
- Ampliació dels drets de les persones: Fins ara eren vigents els anomenats drets ARCO (accés, rectificació, cancel·lació i oposició). Ara, el dret de cancel·lació es converteix en el de supressió i s'hi afegeixen:

  a) el dret a l'oblit: extensió del dret de supressió o cancel·lació perquè se suprimeixin dades i impedir-ne la difusió a internet.

[18] Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals i a la lliure circulació d'aquestes dades. Disponible a: https://www.boe.es/doue/2016/119/L00089-00131.pdf

b) el dret a la limitació del tractament: restricció de les operacions de tractament de les dades personals.

c) el dret a la portabilitat de les dades: dret de tota persona a rebre les seves dades en un format estructurat, d'ús comú i de lectura mecànica.

- Nova figura del delegat de protecció de dades (DPO[19]): Ha d'informar i assessorar els treballadors sobre les obligacions de la normativa i supervisar-ne el compliment, entre d'altres funcions
- Obligació de fer avaluacions d'impacte per determinar el compliment normatiu. Les empreses i administracions hauran de fer avaluacions d'impacte prèvies a la creació dels fitxers de dades, que ara s'anomenen *tractaments de dades*. Aquest fet impacta directament al Servei d'Assessorament Jurídic (SAJ) de la DGP i a la UCIBER.

[19] Sobre aquesta figura, des del Departament d'Interior ja s'ha treballat per tal que en doni servei a tot el departament, prefixant uns requisits mínims per tal d'assolir-ne el càrrec

3 Creació de la cultura de ciberseguretat en la PG-ME

3.1 Generació

Tal i com hem esmentat abans, el Decret 415/2011 habilita a l'Àrea de Seguretat en Tecnologies de la Informació en els àmbits del disseny, implantació, gestió i avaluació dels mecanismes necessaris per a la seguretat dels sistemes d'informació policial, així com l'assegurament de la utilització de les dades de caràcter personal.

Aquesta tasca juntament amb gestió i assignació d'usuaris i els perfils i nivells d'accés als sistemes d'informació, havien estat les prioritats per a la Prefectura de la Policia.

D'altra banda, des de la Comissaria General d'Investigació Criminal ja feia anys, que per decret, s'havia creat la Unitat de Delictes Informàtics per tal d'investigar tots aquells delictes en els qual s'utilitzés les TIC com a mitjà per cometre el fet delictiu.

No obstant això, el ciberdelicte i la ciberseguretat són aspectes que difícilment poden considerar-se separats en un entorn interconnectat. La ciberseguretat exerceix una funció important en el desenvolupament progressiu de la tecnologia de la informació, i tant és així que la millora de la ciberseguretat i la protecció de la infraestructura d'informació crítica és essencial per a la seguretat de les administracions públiques, i de retruc per la policia.

L'augment a partir del 2010 dels ciberatacs a infraestructures de l'administració exigien una acció coordinada de les unitats policials per augmentar la prevenció, preparació, resposta i recuperació enfront d'incidents.

L'any 2013, és un any d'inflexió a nivell normatiu pel cos de Mossos d'Esquadra i en sentit ampli, per totes les administracions públiques del país, ja que les reformes de l'Esquema Nacional de Seguridad[20], la Estrategia de Seguridad Nacional[21] i la Estrategia de Ciberseguridad Nacional[22] creen un gran ventall d'obligacions i de deures envers les administracions, a part de definir clarament els objectius de l'Estat envers la ciberseguretat.

Donat aquest escenari de regulació i de creació d'estructures estatals de prevenció de ciberatacs, durant el febrer de l'any 2014 s'elevà un informe a través de la Comissaria General de Planificació de la Seguretat (CGTSE) que depèn de la Prefectura de la Policia on s'informa de la necessitat de creació d'una nova unitat policial que depengui de l'ASTI.

En aquesta etapa les organitzacions estaven evolucionant d'una manera ràpida i constant, i a més simultàniament el teatre d'operacions on es movien les amenaces tecnològiques avançava a major velocitat de la que moltes d'aquestes organitzacions poden fer-hi front. La

[20] Esquema Nacional de Seguretat. Disponible a : https://www.boe.es/boe_catalan/dias/2010/01/29/pdfs/BOE-A-2010-1330-C.pdf

[21] Estratègia de Seguretat Nacional de 2013. Disponible a: http://www.dsn.gob.es/es/file/144/download?token=JdtEVkaN

[22] Estratègia de Ciberseguretat Nacional de 2013. Disponible a: http://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf

direcció dels Sistemes d'Informació o de les Tecnologies de la Informació (SI/TI) es trobava en un moment de transició en el qual el delicat equilibri entre possibilitar l'activitat pròpia de l'organització i protegir-la requeria d'un alt nivell d'especialització per part de les unitats encarregades de tenir en compte tots aquests canvis per tal que siguin apreciats alhora de prendre decisions.

Aquell escenari en matèria de ciberamenaces, feia necessari que tota organització realitzés una avaluació de riscos així com establir plans de resposta en cas que fos víctima d'un atac informàtic. No és l'objectiu d'aquest treball de fi de màster entrar a valorar el nivell de risc a que, en aquells moments, podia estar sotmesa la Policia de la Generalitat – Mossos d'Esquadra, si bé era evident tenint en compte el context social i els antecedents de fa 5 anys que les probabilitats de ser objecte d'un atac informàtic eren elevades.

És doncs el primer pas i impuls per la generació d'aquesta cultura de ciberseguretat, doncs per crear un servei del no res, cal impregnar de la necessitat de cobrir nous espais i omplir buits conceptuals.

En l'encàrrec d'aquestes competències, la nova Unitat de Ciberseguretat Policial de la DSIP desenvoluparia accions que fins ara mai no han estat assignades a cap servei policial, com ara les que es descriuen a continuació:

1- La creació d'un Pla Director de Seguretat en matèria de les TIC.

- Realització d'un anàlisi de riscos en referència als sistemes d'informació actuals.
- Detecció de les febleses actuals. Elaboració d'un anàlisi DAFO[23].
- Elaboració d'un full de ruta amb els recursos humans, tècnics i materials disponibles a curt i mig termini.

2- La elaboració i relació d'uns plans de Resposta Integrals davant d'incidents de seguretat.

- Elaboració de procediments de resposta modulats
- Augment de la capacitat de resiliència de l'organització
- Establiment de procediments i protocols relacionals amb CESICAT i d'altres CERTS (Centres d'Emergència i Resposta Temprana)

3- L'adequació de mesures de seguretat d'acord amb les necessitats reals dels diferents serveis policials.

[23] Eina d'anàlisi de la situació d'una organització, on es contemplen les seves debilitats, amenaces, fortaleses i oportunitats

- Elaboració de procediments de resposta modulats
- Augment de la capacitat de resiliència de l'organització
- Establiment de procediments i protocols relacionals amb CESICAT i d'altres CERTS

Figura 1. Exemple de col·laboració[24] del CESICAT a la Intranet corporativa de la DGP durant el 2018

4- L'assegurament d'un control directe dels SIP amb personal propi de la DGP.

- Elaboració de procediments de resposta modulats
- Augment de la capacitat de resiliència de l'organització
- Establiment de procediments i protocols relacionals amb CESICAT i d'altres CERTS

[24] Cada any el CESICAT elabora un informe sobre tendències en ciberseguretat on s'informa de l'anàlisi de les tendències en relació amb amenaces de ciberseguretat detectades durant l'any. D'aquest 2017 està disponible a : https://ciberseguretat.gencat.cat/web/.content/PDF/20180430_Analisi-Tendencies-2017.pdf

5- La capacitació autònoma en matèria d'auditora tècnica a efectes de compliment de la LOPD per part de la DGP.

- Elaboració de procediments de resposta modulats
- Augment de la capacitat de resiliència de l'organització
- Establiment de procediments i protocols relacionals amb CESICAT i d'altres CERTS

L'objectiu d'aquestes accions s'encaminaven dins el projecte comú i integral de dotar la Policia de la Generalitat- Mossos d'Esquadra d'un model sòlid de seguretat informàtica i de la informació, amb la màxima col·laboració com a CERT de referència del CESICAT.

D'una banda calia treballar en dos conceptes clarament diferenciats. El primer respecte la seguretat de la informació sota un prisma clarament estratègic i que havia marcar-se directament des de la part directiva de l'organització, això és l'anàlisi de riscos que calia executar, la redacció de normativa i bones pràctiques i l'elaboració d'un Pla director de seguretat , on s'inclogués per primer cop la ciberseguretat com un principi rector de la seguretat de la informació.

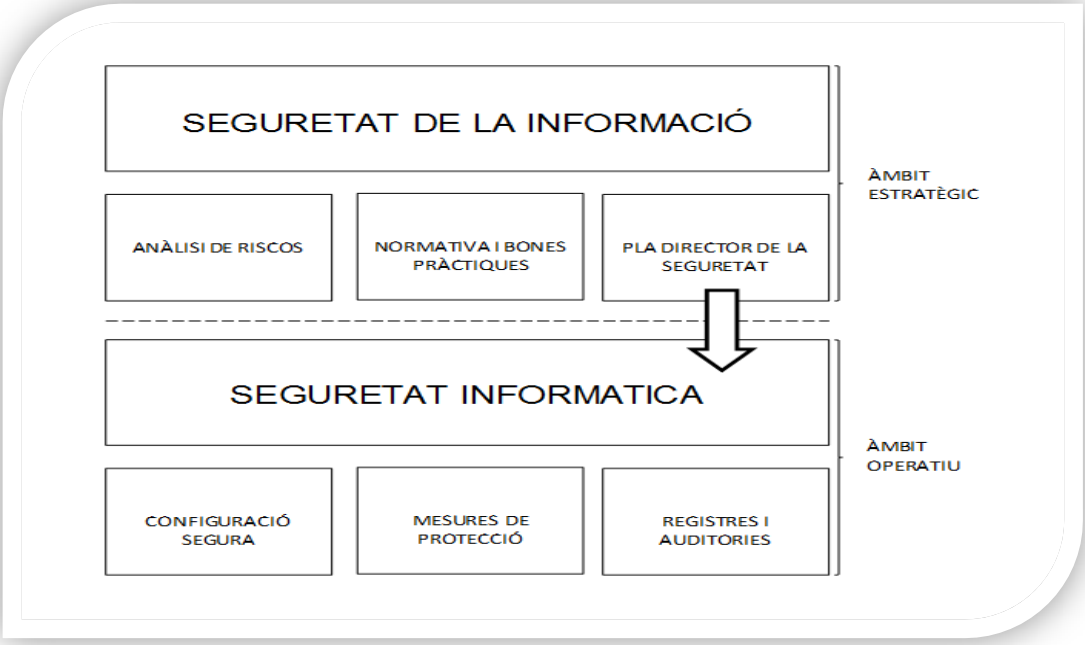


Figura 2. Quadre de diferents àmbits de la seguretat

D'altra banda calia aprofundir sobre l'àmbit operatiu, especialment en l'àmbit de les mesures de protecció, ja que principalment les tecnològiques estaven molt limitades per una clara

retallada del pressupost del Departament d'Interior a causa de la crisi econòmica que travessava encara el país.

La creació d'aquest nou servei suposava assignar una dotació de recursos humans i materials que també s'havien de tenir en compte, i més en un escenari de gran limitació pressupostària arran de la crisi econòmica que estava afectant a gran part del continent europeu.

En quant a recursos humans suposava superar l'escull d'obtenir nous efectius en una plantilla ja estable de 17000[25] agents de policia i sense noves promocions, on la teoria dels "vasos comunicants" es fa més palesa que mai, amb la premissa que un nou servei es proveeix a base de desnodrir d'altres.

Del recursos materials suposava la inversió de noves màquines que no formen part de l'estàndard d'estacions de treball del CTTI, amb RAM suficient per aixecar màquines virtuals[26] i on s'han de pressupostar dins una via de contractació diferent.

El pressupost per la formació també s'havia de contemplar, donar l'específic de la matèria, especialment en l'àmbit forense i pericial[27].

Dotació d'efectius:

- 1 Sergent/Sotsinspector, Cap de la Unitat
- 4 Mossos
- 3 Facultatius de la DGP amb la qualificació tècnica necessària

Dotació de recursos materials:

- 4 Equips portàtils que permetin la connexió VPN a la xarxa de la DGP
- 4 Estacions de treball fixes d'alt rendiment per als membres de la Unitat
- Llicències d'ús de programaris específics d'auditoria de sistemes

Dotació de formació:

- Creació de la 1ª edició del curs de Ciberseguretat de l'Institut de seguretat pública de Catalunya[28] (ISPC)

[25] Actualment en 16536 efectius arran de les excedències, jubilacions, incapacitats i finats que cada any es contemplen dins el cos policial

[26] L'ús de les màquines virtuals cada vegada és més estés ja que permet donar el mateix servei sense disposar de estacions de treball físiques

[27] Els agents de la UCIBER a causa de la seva especialització i formació s'incorporen als processos judicials com a pèrits en la matèria.

[28] L'Institut de Seguretat Pública de Catalunya és el centre de creació i transferència del coneixement del sistema de seguretat pública de Catalunya. Disponible a: http://ispc.gencat.cat/ca/1_linstitut/presentacio/

3.2 Establiment dels nivells

Durant l'any 1988, l'escriptor, investigador i psicòleg Edgar Henry Schein, autoritat en la matèria de la psicologia de les organitzacions, pare del desenvolupament organitzacional, i creador dels conceptes de cultura corporativa, va introduir el concepte de presumpcions i creences, per explicar de forma més àmplia el significat que per a l'organització tenen el concepte de cultura, i la va definir com "... respostes que ha après el grup davant els seus problemes de subsistència en el seu medi extern i davant els seus problemes d'integració interna " (Schein, 1988)[29]. Aquest nivell de presumpcions i creences que comparteixen els grups en l'organització correspon a l'essència mateixa de la cultura. Aquesta s'ha de veure com el conjunt d'experiències importants i significatives tant internes i externes que els individus en una empresa han experimentat i implementat estratègies per adaptar-se a l'organització.

Producte d'això s'ha generat una vivència comuna del que els envolta i el lloc que ocupen dins de l'organització. Com suggereix Schein (1988), "en un concepte formal per a la cultura organitzacional, en aquest sentit és un producte après de l'experiència, i per tant alguna cosa localitzable només allà, on hi hagi un grup definible i posseïdor d'una història significativa"

Segons l'autor, en l'essència de la cultura de les organitzacions, es reserva el nivell més profund de presumpcions bàsiques i creences (Nivell 3), que permeten als individus cada dia expressar i experimentar els seus esdeveniments, donar resposta a les seves problemes de subsistència interna i externa. Aquestes presumpcions bàsiques, són l'essència, el que realment és la cultura organitzacional, un model desenvolupat per un grup per anar aprenent a enfrontar-se amb els seus problemes d'adaptació. Els valors i conductes des de les seves produccions i creacions, són en efecte manifestacions derivades de l'essència cultural.

Schein (1988) conceptualitza tres nivells de cultura i manifesta que aquests no són estàtics ni independents, i s'interrelacionen i conformen mitjançant les creences i presumpcions bàsiques de la cultura organitzacional.

[29] SCHEIN, E. (1988). La cultura empresarial y el liderazgo. Una visión dinámica.

Figura 3. Piràmide dels nivells de cultura segons Edgar Shein

El primer nivell, és el dels artefactes visibles, que comprèn l'ambient físic d'organització, la seva arquitectura, els mobles, els equips, el vestuari dels seus integrants, el patró de comportament visible, documents, cartes, etc. Són dades bastant fàcils d'aconseguir però difícils d'interpretar. L'anàlisi d'aquest nivell pot ser enganyós, ja que, moltes vegades, no s'aconsegueix comprendre la lògica que està per darrere d'aquestes dades. En aquest nivell podem observar la manifestació de cultura però mai podrem saber la seva essència. És el més visible, amb més consciència i alhora el que es pot aconseguir amb un curt termini de temps sempre i quan la direcció de la nostra organització hi estigui d'acord. En el cas dels Mossos d'esquadra correspondria a la creació d'una nova tecnoestructura policial que mira d'adaptar-se als nous reptes de ciberseguretat.

El segon nivell, és el dels valors que dirigeixen el comportament dels membres de la organització. En definitiva, com s'entén la ciberseguretat dins la organització i sobretot, si tots els seus components l'entenen igual. La seva identificació, segons Schein (1988), només és possible a través d'entrevistes amb els membres claus de l'organització. Un risc que es corre en l'observació d'aquest nivell és que el pot mostrar-nos un resultat idealitzat o racionalitzat, és a dir, les persones relatarien com els agradaria que fossin els valors i no com efectivament són. Aquest nivell respon a una major de consciència, a mig termini, on es troben les estratègies, les fites, les filosofies i els valors inherents de l'organització.

El tercer nivell finalment, és el dels supòsits inconscients que revelen mes confiadament la forma com un grup percep, pensa, sent i actua. Aquests supòsits són construïts a mesura que es soluciona un problema eficaçment i que, amb el pas del temps, aquestes premisses deixen de qüestionar-se, constituint-se "veritables veritats", tornant-se inconscients. Inclouen les creences sobre les persones, les percepcions, els pensaments i els sentiments. S'assoleixen

a llarg termini i són invisibles, en definitiva són les fonts últimes dels valors. En el cas dels Mossos d'Esquadra, ho apliquem a com s'entenia abans el ciberdelicte i com ha anat impregnant-se la ciberseguretat arran del creixement exponencial dels delictes tecnològics i cibernètics.

Aquesta perspectiva es resumeix assenyalant que la cultura d'una organització pot ser estudiada en aquests tres nivells, però, si no es desxifra el patró de supòsits bàsics que giren al voltant de l'organització, no es sabrà com interpretar els altres aspectes correctament. Una vegada que es comprenen els supòsits bàsics, es pot comprendre fàcilment els altres nivells que són més superficials (Schein, 1988).

Schein (1988) també planteja que ha d'haver-hi qüestions internes que tota empresa ha de desenvolupar, com per exemple:

- Llenguatge comú i categories conceptuals, si el grup no pot comunicar ni entendre bé, el grup és impossible.
- Límits grupals i criteris per a la inclusió i exclusió, idea comuna sobre els que estan dins i els que estan a fora.
- Poder i jerarquia, com a element vital perquè els membres puguin controlar els seus sentiments agressius.
- Intimitat, amistat i amor, com són les relacions entre iguals i entre els sexes.
- Recompenses i càstigs, tot equip humà ha de saber quins són d'una manera clara i sense possibles interpretacions.
- Ideologia i religió

En aquest sentit, Schein (1988) sosté que les cultures de les organitzacions es generen i es mantenen a causa perquè han permès la resolució de problemes bàsics d'adaptació al medi que envolta l'empresa i d'integració interna. En aquest procés, el paper dels líders és fonamental ja que són aquests els que inspiren a un nou grup amb les seves idees, les quals arriben a convertir-se en definicions compartides i validades pels membres de l'organització. D'aquesta manera, l'autor proposa un model de desenvolupament de la cultura organitzacional que es defineix en una relació recursiva entre processos de lideratge, processos d'interacció grupal i processos d'aprenentatge. Encara que Schein (1988) concep el procés de producció de la cultura organitzacional com un fet complex, el seu objectiu és donar compte de com els líders efectivament poden implantar i transmetre aquesta cultura que en els següent punt detallarem.

Durant aquest treball s'ha pretès comprendre, identificar i reconèixer el nivell en què es troba la cultura organitzacional de ciberseguretat dins la PG-ME, tal i com planteja en sentit genèric l'autor.

3.3 Elements que la conformen

Dins la cultura de la policia catalana, concretament la que afecta a la cultura de ciberseguretat policial, distingirem varis punts per tal de desgranar-la segons afecti a les persones, als procediments o als resultats.

3.3.1 Les persones i els equips

- Recursos econòmics en formació: tot i qualificar-la com a despesa per la inversió en cursos de ciberseguretat, si realment quantifiquem tot el que s'estalvia en serveis exteriors i en disponibilitat d'actius, ens adonem que surt a compte tenir personal altament qualificat.

- Expertesa tècnica: els màxims coneixements del servei s'acumulen en els agents de base, que a part de venir d'un món tècnic (enginyeria, telecomunicacions), es proveeixen d'uns coneixements que fan que el que informen, dins l'aspecte exclusivament tècnic, no es qüestioni per part de la superioritat.

- Escolta: el gestor que comanda aquests equips d'alta capacitat ha de saber escoltar i dirigir, incorporant a les reunions el personal qualificat, ja que els coneixements tècnics són superiors.

- Recursos tècnics: dotar els agents d'equips tècnics d'alt rendiment per desenvolupar les seves tasques.

- Horaris: trobar personal tècnic qualificat que a sobre pertany al cos dels Mossos d'Esquadra no és gens fàcil. En el moment que l'has trobat, cal adequar-se a les necessitats de les persones, amb una flexibilitat que no es dóna en altres serveis de territori. L'equilibri professional i familiar és rellevant en aquests tipus d'equips

- L'accés a la informació: l'equip tècnic policial té un accés a la informació molt elevat així com un grau de coneixement dels sistemes i el seu funcionament, que fa que la confiança dipositada en ells sigui màxima.

- Vulnerabilitat: A més coneixement dels mecanismes de ciberatac i del dany que poden produir, més conscienciació de la importància de cadascun dels actes que com a usuaris fem. La dita que expressa "la ignorància és atrevida", pren un valor significatiu quan s'aborda l'àmbit tecnològic

- El llenguatge: Precís, extremadament tècnic. Vocables específics per l'àmbit de la ciberseguretat es barregen amb sigles derivades de l'anglès amb continguts provinents de la enginyeria informàtica i les telecomunicacions. Un cop ets absorbit per aquesta cultura, sense adonar-te'n comences a diferenciar-te d'altres comandaments que estan en serveis ordinaris policials, fen-te objectivar amb els seus comentaris, que el registre lèxic del dia a dia ha canviat. El més semblant a parlar un idioma diferent, el qual crea uns lligams entre els que el domin en molt importants.

- Cultura: Molt associat al llenguatge, es determinen una sèrie de comunicacions i valors, en quan a gustos, oralitat i domini del món cibernètic, no o estàs dins aquesta àrea o no formes part d'aquest àmbit

- L'actualització: Tal i com passa amb els equips i els sistemes, els agents s'han actualitzar diàriament. El mètode de ciberatac d'ahir es pot haver modificat i per tant tenir un coneixement desfasat. Les preguntes freqüents entre els membres de l'equip són diàries, i es reconeix qui respon correctament o sap i/o aplica les últimes notícies relacionades amb les seves tasques.

- L'espai: Donat l'alta rellevància i informació de la qual són dipositaris, la UCIBER està situada a prop del personal tècnic que gestiona els equips informàtics de la DGP, però en una sala a part en la qual l'accés és restringit només al personal adscrit a la unitat i als seus superiors jeràrquic. Qualsevol accés diferent ha d'avisar-se amb suficient antelació per tal tenir-ne la previsió.

- L'ambient: És principalment silenciós però tenint en compte que s'operen directrius i que cal, molts cops, debatre sobre certs aspectes tècnics del dia a dia. Tot i comptar la Divisió de Sistemes Policial de 3 sales de reunions per la recepció de proveïdors i poder-la reserva mitjançant aplicació informàtica sense cap mena de restricció, els dia a dia es realitzen a la pròpia unitat. La importància de tot l'equip és rellevant. Tots tenen veu i vot, amb el vist i plau final dels caps superiors.

- Vincles: La UCIBER és una unitat policial petita que no arriba a la desena d'efectius entre funcionaris policials i facultatius. Això crea vincles i lligams important a l'hora d'encarar les adversitats, donat que quan les hi han, la pressió dels alts comandaments és molt elevada.

- Estabilitat laboral: Qui es forma, val i gaudeix d'aquests condicionants laboral tot i estar en una plaça no definitiva, té un futur d'estabilitat plena ja que la formació en el personal és molt específica i costosa. Per aquest motiu, aquest tipus de perfils són molt buscats entre les unitats tecnològiques del cos.

- Reputació: L'especialització i l'alta qualificació i formació dels agents, fa d'ells un grup de reputació i prestigi. És un orgull per l'equip formar part d'un servei central que dóna servei a tota la organització i de retruc a les 206 policies locals que hi tenen accés.

- L'enginy: Al ser un camp en constant creixement i múltiples possibilitats tecnològiques, fa que l'aportació dels agents sigui molt rellevant i que sigui més fàcil de dur a terme que en altres àmbits de la seguretat clàssica. Això afavoreix als agents a desenvolupar capacitats de millora rellevants pel bé comú. Una manera de deixar empremta dins l'organització.

- Localitat: el serveis centrals estan ubicats a la localitat de Sabadell per defecte. Només pocs serveis resten ubicats a Barcelona, entre els quals està la UCIBER. Això

té un condicionant de certa rellevància de cara als agents, ja que el fet d'estar a la ciutat altament comunicada i a prop del lloc de residència, la fa tenir un punt a favor.

- Formador de formadors: l'alta especialitat tècnica es nodreix de cursos cars i amb dedicació. Això dóna capacitació als tècnics els quals han de vetllar, sota directrius de comandament, de fer-ne difusió i transferir coneixement. Això es tradueix en formacions menys específiques a l'Institut de Seguretat Pública de Catalunya, on els nostres efectius faran de formadors, per tal que els seus alumnes facin arribar el coneixement a la resta d'usuaris del territori. La cultura de ciberseguretat s'ha de propagar.

3.3.2 Els procediments

- La missió: Ser garants de la ciberseguretat en quan a la disponibilitat, integritat i qualitat de les bases de dades policials així com de les aplicacions que les gestionen.
- Elaboració: S'han d'establir procediments, normes i instruccions tècniques que impactaran directament en tots els usuaris dels SIP. Cal tenir en compte doncs, que tot allò que redacti la UCIBER afectarà potencialment a 30000[30] usuaris, amb la responsabilitat i les conseqüències que això comporta.
- Normativa: S'ha de ser escrupolós en tot el referent a normativa i el seu compliment, en especial a tot allò que fa referència a l'Esquema Nacional de Seguretat (ENS).
- Conscienciació: tots els usuaris que tenen accés als SIP han de tenir un mínim de conscienciació adquirida envers la ciberseguretat. Les auditories que cerquen males praxis al sistema, alhora serveixen també de conscienciació.
- Personal tècnic: hi ha elements perifèrics de seguretat que recauen en mans de tècnics externs i el CTTI, en definitiva personal no policial però que dóna servei a les TIC en el global de la Generalitat. Cal doncs, redactar i establir procediments encara més rigorosos per a ells també, ja que l'accés potencial als sistemes i a la informació que s'hi conté és elevat, segmentant les seves actuacions i fent-les parcials.
- Auditoria: forma part de la idiosincràsia de la unitat, que qui accedeix a la informació és permanentment auditat, i qui audita és controlat davant la possibilitat

[30] Són el total d'usuaris producte de la suma de PG-ME, policies locals, administratius de la DGP, administratius locals dels ajuntaments i administratius de la Generalitat de Catalunya

d'accedir a certa informació. Es basa doncs en una relació de confiança entre la unitat de ciberseguretat i la unitat d'auditories.

3.3.3 Els resultats i la qualitat

- Solucions: Tota mesura i solució cal abordar-la sota l'esperit de servei a la organització, en la recerca del bé comú per sobre de les opcions personalistes. El bé comú està per sobre del bé particular.
- Comunicacions: Dins el caràcter genèric de les intervencions i mesures que s'apliquin, que la organització tingui coneixement de qualsevol mesura que s'apliqui és d'alta importància. Els usuaris es senten insegurs davant qualsevol canvi tecnològic.
- Previsió: Qualsevol mesura aplicable a la organització s'ha de comunicar amb un temps raonable, per tal que els usuaris dels SIP tinguin temps a adaptar-se i també a comunicar algun imprevist que no s'hagi contemplat, tant a nivell operatiu (implementació d'una millora en mig d'un operatiu policial) com estratègic.
- Consens: Les polítiques de seguretat de la informació apliquen a tothom. Quan els canvis a aplicar són substancials, és d'alta importància comptar amb la veu i opinió dels serveis més rellevants.
- Alineació amb la direcció: qualsevol, política, procediment o norma ha d'estar validada per la superioritat. Al ser un cos jeràrquic, a qui li recau certa política pot ser de rang superior al qui l'aplica. Per aquest motiu, el paper de la Prefectura de la Policia és clau, com a òrgan director.
- Monitoratge: els sistemes de control i seguretat que vetllen per la integritat i continuïtat del servei a la DGP han d'estar contínuament monitoritzats. Per aquest motiu, i a mode de quadre de control, s'ha equipat de grans pantalles una de les parets on està ubicada la UCIBER, per tal que, a primer cop d'ull, pugui haver observança de qualsevol ciberincident que pugui afectar els sistemes.
- Treballant pel futur. Les TIC i la seva dependència de l'organització augmenten exponencialment, també els perills que hi són associats. Això fa que la cerca en la qualitat sigui constant, perquè el que es llaura ara servirà de fonaments de cara al futur
- Potencial creixement. El ciberdelicte ha vingut per quedar-se. La ciberseguretat ha d'augmentar i per tant els recursos humans i materials que s'hi dediquen creixeran exponencial. Professió de servei, professió de futur.

- Felicitacions i condecoracions: Els llocs tècnics han sabut guanyar-se un lloc rellevant dins el reconeixement estratègic de la organització. Al donar servei continu i d'alta repercussió, fa que els èxits siguin clarament notoris pels caps.
- Innovació: "Allò que val per avui, no val per demà. Allò que ens defensa avui, no servirà pel demà". Sota aquest paraigües de premisses i l'evolució constant de la ciberseguretat, els productes tecnològics que sorgeixen no s'aturen, cada cop millors i més adaptables. És un camp en contínua evolució.

3.4 Orientació

Quan utilitzem la dita "una cadena és tan forta com la seva part més feble" en referim a que tot i que les organitzacions inverteixin molt en dispositius tecnològics i en solucions tècniques per a protegir de manera adequada els sistemes d'informació, si algun d'ells falla, tota la seguretat es veu compromesa.

En aquest sentit, l'usuari és una part més de la cadena i l'experiència ens demostra que és una de les parts més febles, precisament per on aquesta cadena de seguretat es sol trencar. Per canviar revertir aquesta situació, cal invertir en la formació en seguretat dels usuaris, sota la premissa que "l'usuari és la part més important de la cadena de la seguretat".

Per aquest motiu hem de ser conscients que a l'hora de parlar de seguretat de la informació, la tecnologia mai és suficient, ja que a l'hora de la veritat els autèntics protagonistes de la seguretat en el nostre cos són els usuaris finals, el mossos, que són els que gestionen i utilitzen els sistemes d'informació policial de la nostra organització.

Alhora cal tenir en compte que desenvolupar i integrar una cultura de seguretat dins de la nostra organització és un dels objectius més complexos d'assolir. En primer lloc perquè la seva aplicació requereix d'uns terminis de temps amplis i d'accions continuades en el temps; en segon lloc, i molt més important, perquè parlem d'agents de la policia, que al cap i a la fi són persones amb problemes inherents de la vida. Aconseguir que els nostres agents interioritzin en les seves tasques ordinàries una manera de treballar que garanteixi que les coses es fan bé en matèria de seguretat de la informació no és una tasca gens senzilla.

Tot sovint els agents veuen els protocols de seguretat que hem implantat des de l'Àrea de Seguretat en Tecnologies de la Informació de la DSIP com una complicació, com un entrebanc o fins i tot una molèstia. La percepció que tenen és que la seguretat és incòmoda i dificulta les seves activitats quotidianes imposant limitacions. Les frases com "així no podem treballar" o fins i tot "amb el que acabeu de fer no ens deixeu treballar", ressonen dins la nostra consciència cada vegada que implementem una nova mesura de seguretat.

Ha calgut doncs revertir aquesta visió negativa i abordar les accions necessàries per aconseguir crear una autèntica cultura de ciberseguretat dins la PG-ME.

3.4.1 Accions de formació en seguretat per als usuaris dels SIP

Tradicionalment la seguretat de la informació en les organitzacions s'ha entès com una despesa que no aporta valor al negoci, ja que és molt difícil veure el retorn de la inversió en mesures que no es perceben com productives. La formació en matèria de ciberseguretat, fins ara ha tingut un protagonisme gairebé nul en els plans de formació de l'Institut de Seguretat Pública de Catalunya*. I si s'arriba a abordar, aquesta es realitza de manera puntual o a un grup reduït d'empleats.

De fet, si preguntem per iniciatives relacionades amb la formació en seguretat, veurem que únicament es tracten accions relacionades amb la seguretat en el lloc de treball i la prevenció de riscos laborals, deixant fora els àmbits de la seguretat de la informació.

Amb l'aparició el 1999 de la LOPD (Llei Orgànica de Protecció de Dades Personals) es va produir un petit canvi en aquest sentit, i les organitzacions més afectades pel compliment d'aquesta normativa, van començar a dur a terme sessions de formació relacionades amb els requeriments de protecció de la privacitat dels usuaris.

De fet, el Reglament de Desenvolupament de la LOPD, contempla com una obligació de totes les empreses i administracions, formar els usuaris de l'organització en matèria de seguretat de les dades de caràcter personal, garantint així que són gestionats d'una manera adequada i d'acord amb la llei.

És fonamental que siguem conscients de la importància de formar els nostres empleats en matèria de seguretat de la informació per als nostres interessos com a organització, i no només en matèria de protecció de dades personals, sinó també des del punt de vista de tota la informació que tracta l'organització: dades de facturació, tarifes, marges, sistemes de producció, clients, proveïdors, acords, etc.

No obstant això, no tot el personal d'una organització necessita el mateix tipus ni grau de formació en matèria de seguretat. La formació que necessita el personal tècnic que gestiona els servidors o el Host* no ha de ser la mateixa que rebin els agents que només disposen d'accés a una petita part de la informació corporativa.

3.4.1.1 Els agents de la Unitat de Ciberseguretat Policial

El agents de la UCIBER són el que necessiten més formació en matèria de seguretat de la informació i amb un major grau d'especialització. Cal posar a disposició dels administradors de sistemes dels recursos i mecanismes adequats per formar-se i auto formar-se en aspectes relacionats amb la seguretat dels SIP i les 82 aplicacions policials[31] que donen servei al

[31] S'inclouen les purament de gestió policial, com les d'investigació i les administratives. El conjunt de les aplicacions es coneix com PGME

nostre cos, tant les purament policials, com les de seguretat ciutadana, investigació o policia científica, com les administratives, gestió de vestuari o butlletes de denuncia.

Dins d'aquests aspectes podem assenyalar alguns tan crítics com:

. Gestió i administració d'elements de seguretat perimetral: tallafocs, antivirus, Sistema de Detecció d'Intrusions (IDS)[32]

. Còpies de seguretat i d'altres mecanismes de contingència

. Sistemes de seguretat de les estacions de treball policials

. Gestió i resolució dels incidents de ciberseguretat

. Polítiques de seguretat sobre els discs durs externs i llapis USB

. Altres mecanismes de seguretat: eines de xifratge, mecanismes d'accés i autenticació als SIP, gestió de les contrasenyes tant de Plataforma[33] com de la PGME

A més, la constant evolució de la tecnologia exigeix que els agents de la UCIBER hagin d'estar en un continu procés de formació, ja que el nostre cos té una alta dependència de la tecnologia.

I no només això, sinó que en alguns casos aquests agents es converteixen, si Help Desk[34] no ho soluciona, en assessors dels usuaris finals del territori en l'ús de la tecnologia i les necessitats de seguretat, incloent-hi per exemple l'ús de eines per gestionar els dispositius d'emmagatzematge externs.

I a més d'això, haurem d'afegir una nou repte a la seva tasca ja que la PG-ME ha fet extern l'administració de la infraestructura TIC a través d'un proveïdor especialitzat, com és el Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) de la Generalitat de Catalunya. S'ha de tenir en compte que s'ha de vetllar perquè aquest centre sigui competent en matèria de seguretat de la informació: no només ha de gestionar la nostra infraestructura TIC d'una manera eficient; també ho ha de fer d'una manera segura, sota la supervisió de l'ASTI.

3.4.1.2 Els agents com a usuaris finals

No només els agents de la UCIBER han de ser els destinataris exclusius de la formació en matèria de seguretat de la informació. Actualment tots els agents de la PG-ME són susceptibles de l'ús d'estacions de treball, ja sia perquè tenen una tasca de suport al

[32] Prevención de intrusos y gestión de eventos para sistemas de control. Disponible a: https://www.certsi.es/blog/prevencion-intrusos-y-gestion-eventos-sistemas-control

[33] Paquet d'ofimàtica amb el qual s'accedeix des de les estacions de treball de la DGP.

[34] Correspon al Servei d'Atenció a l'Usuari (SAU) de les empreses ordinàries

comandament de l'ABP, perquè estan a la Oficina d'atenció al ciutadà (OAC), perquè estan destinats a les Sales Regionals de Comandament (SRC) o simplement perquè han d'elaborar una minuta policial durant el seu torn de patrullatge. En qualsevol moment de torn poden acabar treballant amb ordinadors o amb dispositius que els permetin connectar-se als sistemes corporatius.

Per tant, la seguretat avui dia no s'ha de limitar només als aspectes tècnics, sinó que ha d'incorporar altres àmbits com l'organitzatiu i el legal, anant més enllà de les competències del de la UCIBER o el CTTI.

Cal tenir en compte a més, que hi ha departaments d'administració com la Subdirecció General de Recursos Humans (SGRH) o la Subdirecció Gestió Econòmica i Logística (SGEL), totes dues dependents de la Direcció General de la Policia, que han de conèixer aspectes vitals en la gestió de la seguretat de les dades, com la LOPD, amb els quals treballen com a part de les seves funcions quotidianes.

No fer-ho pot provocar que la DGP incorri en situacions de risc, tant a nivell de protecció de dades com a nivell d'infraccions legislatives. En aquest cas, la DSIP conta amb una facultativa[35] en dret com a primera opció de consulta bàsica i amb el Servei d'Assessoria Jurídica (SAJ) de la DGP que assessoren en l'aplicació de la legislació de protecció de dades en l'entorn corporatiu.

De fet, com en els Sistemes d'informació policial s'emmagatzemen dades de persones físiques, moltes de les quals resten en el nostre sistema sense consentiment de la persona, resulta fonamental la formació en l'àmbit de protecció de dades de caràcter personal, ja que el nivell de risc associat pot ser molt alt.

Per aquest motiu, també durant l'any 2014 es crea la UGDA Unitat de Drets ARCO (drets d'accés, rectificació, cancel·lació o oposició) per realitzar el tractament de les dades de les persones físiques introduïdes als SIP, partint d'unes determinades condicions, tant a nivell tècnic com legal, que són establertes tant per la LOPD com pel seu Reglament que la desenvolupa, ja que hi ha uns terminis molt ajustats per atendre aquest tipus de peticions.

Tanmateix, no hem de limitar la formació en seguretat únicament al correcte tractament de les dades personals. Hi ha altres molts aspectes a considerar en la formació del personal de la PG-ME:

a) Aprendre a reconèixer un atac d'enginyeria social i a evitar-lo, de forma que es garanteixi que no es proporciona informació policial ni corporativa a persones no autoritzades

[35] Dins el cos de Mossos d'Esquadra existeix una escala de suport a la funció policial, coneguda amb el nom de facultatiu i relacionada normalment amb les àrees d'enginyeria, biologia, telecomunicacions i dret

b) Protegir adequadament els dispositius als quals tinguin accés, especialment els mòbils i les tauletes les quals no tenen unes mesures de seguretat corporativa i per tant, depenent en gran part de la voluntat de l'usuari final

c) Usar una correcta política de contrasenyes i de taules netes als despatxos, sense deixar a l'abast d'altres informació sensible i/o confidencial

d) Entendre els riscos que comporten l'accés a planes web externes, aplicacions de mòbil de tercers i descàrregues o actualitzacions no validades* (PI09) per la UCIBER

En definitiva, tots els usuaris del cos amb accés als sistemes d'informació policial han de rebre formació relacionada amb bones pràctiques en matèria de seguretat de la informació en el seu lloc de treball i en l'exercici de les seves funcions.

3.4.2 Establiment de polítiques, normatives i procediments de seguretat interns

Els coneixements adquirits per la UCIBER en matèria de seguretat de la informació s'han traduït en diferents procediments i protocols d'actuació a seguir dins de l'organització.

Per exemple, quan s'han incorporat noves promocions dins l'organització, actualment hi ha un procés selectiu que incorporarà 500 nous agents el proper juny de 2019, cal dur a terme una sèrie de tasques relacionades amb el procés d'alta als SIP perquè quan surti de l'ISPC, pugui començar a desenvolupar les seves funcions:

. Tasques tècniques: alta de l'usuari en el domini corporatiu[36] (Active Directory), assignació de permisos i privilegis d'accés a carpetes del servidor (plataforma), accés a aplicacions corporatives, etc.

. Tasques administratives: el nou agent haurà de signar la documentació relacionada amb la LOPD i acord de confidencialitat, un formulari de petició informàtica -codificat com PI09*- en la qual l'ASTI gestiona, lliura i emmagatzema si calen posteriors usos derivats de males praxis o de fuita d'informació. En aquest sentit, els agents de la Divisió d'Afers Interns (DAI) dins la seva funció d'aplicació del règim disciplinari també tenen un interès especial en el correcta emplenament d'aquest formulari.

Tots aquests passos cal formalitzar-los, documentant totes les etapes, i contemplant-hi els aspectes relacionats amb la seguretat que s'han de tenir en compte i aplicar adequadament.

El mateix s'aplica als diferents protocols d'actuació de ciberseguretat del cos, on s'han de fer procediments i documentar-los per escrit. Cal tenir en compte que és en els moments de calma i reflexió, on es poden realitzar reunions de coordinació i documentar com s'han de fer les coses d'una manera establerta i adequada. Quan s'és víctima d'un ciberatac, no es pot

[36] Mitjançant aquesta eina de l'empresa Microsoft es gestionen els privilegis d'accés al paquet d'ofimàtica de la DGP

deixar res per determinar i tot ha d'estar correctament establert. Els nervis i les presses són males conselleres per determinar correctes decisions. L'estrès bloqueja el pensament.

I de la mateixa manera que documentem com es fan les coses, cal especificar el que es pot i el que no es pot fer dins l'organització, com per exemple:

. El correu electrònic corporatiu

. L'accés a planes web d'internet

. Els dispositius d'emmagatzematge extern

. L'enviament de dades de confidencial o reservat

. La correcta aplicació de la LOPD.

. El coneixement i aplicació de normes, procediments, instruccions i decrets.

En definitiva, hem de posar per escrit la normativa del en matèria de ciberseguretat que contempli la filosofia i cultura del cos, de manera consensuada amb els diferents serveis que els són d'afectació.

Aquestes normes i procediments formaran part de la Política de Seguretat[37] de la Direcció General de la Policia. Aquest és, en la seva essència, un document que recull les intencions i objectius que l'organització marca en quant a seguretat de la informació i el propòsit és declarar formalment que la seguretat és una part fonamental de la cultura de la nostra empresa.

Per aquest motiu, els procediments i les normatives que definim s'eleven a la Prefectura de la Policia per tal que siguin formalment aprovats, ja que en gran mesura marquen el funcionament de l'organització i s'apliquen a tots els serveis i escales, on s'inclouen tots els usuaris sense distinció.

En aquest sentit és molt important que un cop aprovades de manera formal les normatives i procediments que afecten als SIP, o les modificacions que s'esdevinguin, les comuniquem també als usuaris finals. De res serveix que es redactin i s'aprovin si no són conegudes pels seus destinataris, ja que no s'aconseguirà ni la conscienciació dels empleats ni la implantació de les normatives.

En aquest sentit des de la UCIBER es disposen de les següents vies de difusió:

- Correu electrònic perquè es distribueixi per la via jeràrquica
- Intranet corporativa amb "Comunicats de la DSIP"

[37] L'institut de Ciberseguretat Espanyol recomana mitjançant la seva web l'establiments de polítiques de seguretat tant a nivell empresarial com pel personal tècnic. Disponible a: https://www.incibe.es/protege-tu-empresa/herramientas/politicas

- Comunicats Interns que arribaran via jeràrquica als bríefings de servei
- Reunions de comandaments dels diferents serveis del cos
- Jornades de ciberseguretat obertes a tots els membres de la PG-ME i també a les policies locals[38] (també membres dels SIP)
- Jornades per a càrrecs directius de l'escala superior del cos

3.4.3 Supervisió de compliment de bones pràctiques en seguretat

L'elaboració dels procediments de seguretat forma part dels controls preventius orientats a millorar el nivell de seguretat del nostre cos. No obstant això, cal comprovar que efectivament s'està seguint i aplicant.

Per aquest motiu, mitjançant la resolució* on s'encarrega al Cap de l'ASTI com a responsable de seguretat encarregat de vetllar per:

- La vigència i corresponent actualització de les normes i procediments definits, atenent a la detecció de noves situacions, de canvis legislatius o organitzatius, de pràctiques tecnològiques en l'organització que recomanin la revisió dels mateixos.
- La implantació dels mateixos i seu compliment atenent la 15/99 LOPD per part dels usuaris dels SIP

D'altra banda, també hem de disposar d'eines i mecanismes per comprovar que els usuaris segueixen els procediments definits i que compleixen les normatives vigents.

Per a això es realitzen auditories, periòdiques internes. L'ASTI disposa, entre les seves unitats policials, de la Unitat d'Auditories (UAD) que disposa de les eines més avançades d'auditoria que hi ha al mercat. Mitjançant aquestes es registren les accions -accessos, còpies, esborrades i modificacions- de dades, que realitzen els usuaris a les aplicacions informàtiques i bases de dades corporatives, per tal de garantir la traçabilitat d'aquestes operacions.

Cal remarcar la importància que, més enllà de la signatura al formularia PI09, d'accés als SIP i on es regulen les accions permeses i no permeses per les polítiques de seguretat de la DGP, l'ús d'eines de monitoratge i auditoria han d'anar acompanyades d'unes notificacions a les aplicacions policials, informant prèviament i d'una manera clara als usuaris de la seva existència i finalitat.

[38] Les jornades de ciberseguretat que la UCIBER organitza a l'Institut de Seguretat Pública de Catalunya s'obren sempre a les policies locals que estiguin interessades i als membres de seguretat privada, dins el compromís del cos de la conscienciació i millora de la ciberseguretat dins la policia de Catalunya

La sola existència de sistemes de monitorització i auditoria, o d'un règim sancionador -exercit per la Divisió d'Afers Interns de la DGP- associat a l'incompliment de les normes té un efecte dissuasiu, que també ha de formar part de la cultura de ciberseguretat.

3.4.4 Realització d'accions de sensibilització i conscienciació en seguretat als usuaris

Tot i que s'ha remarcat la necessitat que els usuaris del cos rebin formació en matèria de seguretat, en els seves diferents vessants (tècnica, organitzativa i legal), aquesta no era possible sense la creació d'una estructura definida i consolidada, com és l'ASTI i la creació de la UCIBER per tal de delimitar un sistema de normes i procediments detallats i estandarditzats.

Però tot això no és suficient perquè l'àmbit de la ciberseguretat s'integri dins la cultura corporativa. L'establiment de normes i procediments, la formació dels agents encarregats de definir-los, l'existència d'una tecnoestructura jerarquitzada que doni suport a tot l'anterior, són una condició necessària però no suficient.

Aquesta normativa de seguretat l'hem escalat piramidalment segons rang de jerarquia on cada nivell inferior desenvolupa el que marca l'àmbit superior, això és:

1. Polítiques de seguretat
2. Normes
3. Procediments
4. Instruccions tècniques

És important que la cultura de ciberseguretat sigui un dels pilars del cos de Mossos d'Esquadra. Per aquest motiu, des de la DSIP i la Prefectura[39] de la Policia s'impulsa la implicació de tots els usuaris i també dels comandaments que els supervisen. Per aquest motiu s'han impulsat accions d'adequacions d'accés a la informació a certes aplicacions informàtiques, de tal manera que per obtenir informació fora del àmbit territorial o competencial de l'agent cal la supervisió d'un comandament. Com hem vist abans, el vist i plau i la implicació de la Prefectura de Policia i del propi Director General de la Policia són vitals.

Però no només és necessari l'aprovació directiva d'aquestes millores i canvis, per aconseguir aquest grau de comprensió primer per part dels agents i després d'implicació per part dels comandaments que ho supervisen, cal emprendre accions de sensibilització i conscienciació, necessàries per al manteniment dels nivells de seguretat adequats.

[39] Òrgan superior de la DGP des d'on pengen les Comissaries Generals Territorials, d'Investigació Criminal i Tècnica

Si els agents com a usuaris finals no es consideren part fonamental d'aquest procés, el fracàs està garantit, ja que ells són els grans protagonistes d'aquest procés d'enfortiment. No només perquè són els encarregats de complir les normes i els procediments, sinó perquè també són part fonamental en el mecanisme intern de revisió i millora proactiva del nivell de seguretat.

En alguns casos els usuaris no necessiten «formació en seguretat» en el sentit tradicional, sinó «informació sobre seguretat». Es tracta sobretot d'informar als agents de com aplicar certs aspectes relacionats amb la seguretat en l'exercici de les seves funcions policials. El nostre objectiu ha de ser conscienciar-los sobre el paper que juguen en el manteniment de la seguretat de la informació del cos.

Alhora que la tecnologia evoluciona, també evolucionen els riscos associats a la seguretat de la informació. La Direcció General de la policia disposa de més de 2000 terminals mòbils i s'enfronta de nou a un gran repte. A part dels terminals premium[40], que consisteixen en un telèfon intel·ligent Samsung S7 lliurats a alts comandaments, els terminals estàndard són Samsung J3 de 8GB i que es lliuren a comandaments intermedis i agents operatius de certes unitats centrals, el qual és un terminal amb unes capacitats de procés i d'emmagatzematge a totes llums just per certs nivell de comandament.

Davant d'aquest limitacions ens trobem amb el BYOD[41] (Bring Your Own Device), que consisteix en la utilització de dispositius propis dels agents com telèfons intel·ligents o tauletes, i que es connecten a la xarxa corporativa de la DGP, ja sigui per consultar el correu electrònic, o per accedir a certes dades contingudes a documents ofimàtics.

La connexió a la xarxa corporativa de dispositius "no controlats" o l'emmagatzematge d'informació corporativa confidencial en aquests dispositius sense les adequades mesures de seguretat són aspectes sobre els quals cal encara conscienciar als usuaris, establint polítiques de seguretat per a aquestes situacions i creant mesures de seguretat per evitar-ho. Tenint en compte que els comandaments mai han tingut cap tipus de restricció en la telefonia mòbil, realitzar aquesta tasca serà complexa d'implementar.

També ha proliferat l'ús de tècniques d'enginyeria social, per part dels ciberdelinqüents, per aconseguir accés a la informació o als sistemes corporatius. Aquestes pràctiques es tradueixen, per exemple, en trucades telefòniques suposadament realitzades per Help Desk sol·licitant les credencials de l'usuari, per a una prova que s'està realitzant, o l'enviament d'un correu electrònic suplantant a un remitent legítim i conegut amb un document annex que conté un codi maliciós. Les campanyes d'Hisenda, Correus o de certs bancs, han estat àmpliament difoses a través del correu electrònic o de la Intranet corporativa.

[40] Depenent del càrrec de l'usuari es dota de servei de telefonia amb diferents games i models: terminals Samsung models S7 per tarifa premium i Samsung model J3 per tarifa estàndard

[41] Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario. Disponible a: https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el

Cal doncs, que els usuaris coneguin els riscos als quals estan exposats, perquè sàpiguen reaccionar correctament davant de possibles situacions similars. Si no coneixen aquestes amenaces, no podran identificar-les ni protegir-se davant d'elles.

Dins de les tasques assignades a l'Àrea de Seguretat en Tecnologies de la Informació i de retruc a la UCIBER, relatem els punts on, juntament amb les recomanacions[42] que realitza el Instituto Nacional de Ciberseguridad (INCIBE), s'ha fet més incís de ciberconscienciació als usuaris dels SIP per entendres com a important per la seguretat de la informació de la nostra organització:

- Ús segur de xarxes WiFi
- Ús segur del correu electrònic
- Pràctiques de navegació segura
- Identificació de virus i codi maliciós
- Gestió de contrasenyes
- Classificació de la informació[43] (Instrucció 8/2005)
- Esborrat segur de la informació[44]
- Ús de dispositius USB
- Seguretat en dispositius mòbils
- Ús de programes de missatgeria instantània
- Riscos de les xarxes socials
- Tècniques d'enginyeria social

Els temes a tractar no només estan relacionats amb l'ús de la tecnologia, sinó que abasten altres àmbits relacionats amb la seguretat de la informació en sentit ampli:

- Política de taules netes

[42] Kit de concienciación para empresas de INCIBE. Didponible a: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[43] La informació policial es classifica per instrucció en diferents nivells de seguretat de l'1 al 5 depenent del seu nivell de confidencialitat, essent el nivell 1 la informació pública que pot ser difosa fora de l'entorn policial i la 5 la secreta que només pot ser impresa amb numeració i destinatari concret.

[44] Cada cop que es substitueix un equip informàtic cal esborrar de manera segura totes les dades que estiguin enmagatzemades, tant en el disc local com en les carpetes temporals. Sobre aquesta esborrada segura, hi ha elaborat un procediment per tal de garantir-ne que no hi hagi cap fuita accidental d'informació

- Destrucció segura de la documentació en suport paper *(destructores ABP i Complex)
- Possibles escenaris de fuga d'informació.

L'objectiu per part nostra és que l'usuari adopti una sèrie d'hàbits saludable en matèria de ciberseguretat tant a nivell personal com professional, el que redundarà també en la millora del nivell de seguretat de la PG-ME.

Si la formació es planteja com un tràmit a complir, l'usuari també ho viu igual; es limita a assistir a la xerrada, sense que l'acció formativa tingui cap repercussió en els seus hàbits. Cal donar al pla de conscienciació la importància que mereix, i dissenyar accions formatives adaptades i enfocades a la realitat de l'organització.

En el cas de l'escala superior del cos, especialment en el rang de comissari i major, les accions s'han centrat en un enfocament personalitzat, tenint en compte el rellevant accés a la informació que tenen i la seva classificació, el seu entorn de treball, el seu staff com a grup de confiança -incloses les secretàries- i els riscos específics associats.

Un exemple d'aquestes accions, han estat les jornades de conscienciació per l'escala superior l'any 2015, on s'explicà un cas típic d'APT[45] (Advanced Persistent Threat) on mitjançant enginyeria social o injecció de codis maliciosos, una empresa o administració pública pot tenir fuites d'informació, escalada de privilegis il·lícita o pèrdua dels sistemes informàtic de manera permanent, provocant pèrdues de diners, de continuïtat de negoci o de reputació. Tots tres punts serien desastrosos per la policia catalana.

[45] Existeixen diversos estudis sobre com abordar aquest tipus de ciberamenaces i de com detectar-les. INCIBE durant el 2013 publicà un informe d'ajut a empreses. Disponible a: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf

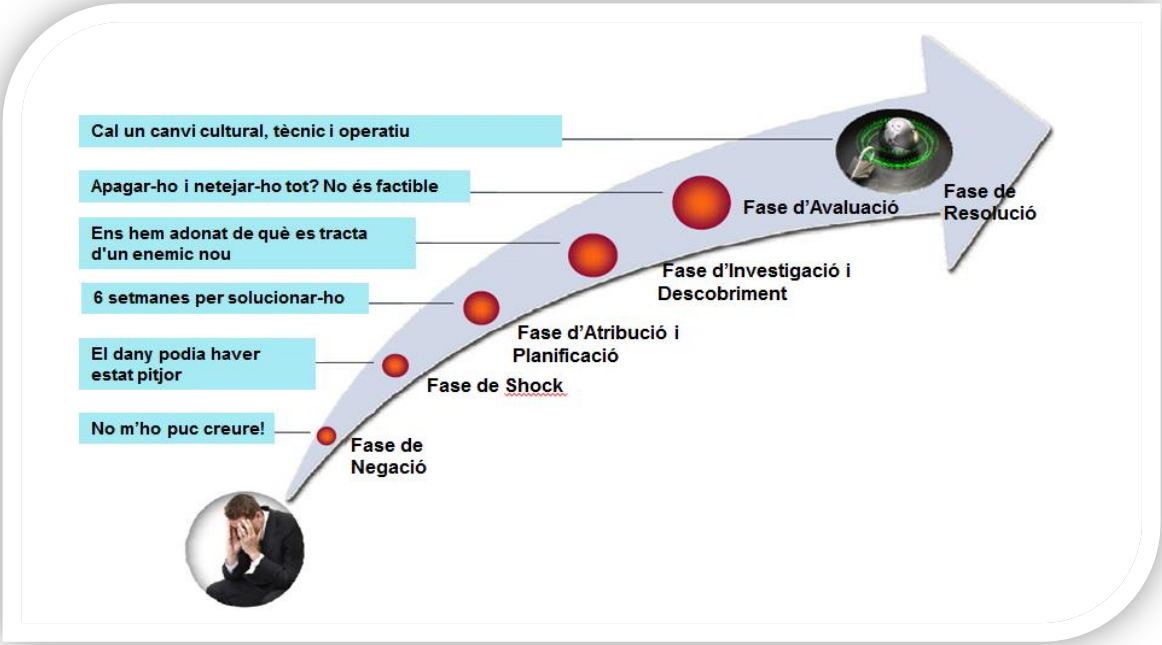


Figura 4. Fases d'un ciberatac típic mitjançant APT (Advanced Persistent Threat)

En definitiva, la conscienciació incrementa el nivell de seguretat de la informació de la nostra organització. Si incrementem la ciberseguretat minimitzem els riscos de pèrdua d'informació i de disponibilitat i integritat de les dades.

4 Perspectives estratègiques de futur

Tot i la tasca que s'ha detallat que s'està duent a terme des de febrer de 2014, en el món de la ciberseguretat, conjuntament amb les recomanacions de INCIBE i CESICAT, des de la UCIBER es plantegen nous reptes i perspectives de futur.

Cal continuar millorant, incrementant i potenciant els reptes següents, que s'han de recollir en un pla estratègic com a mínim a 4 anys de termini.

- Augmentant la capacitat de vigilància de les xarxes i els sistemes. És indispensable comptar amb un equip de ciberseguretat correctament dimensionat per tal d'abordar un flux creixent i exponencial d'informació i d'usuaris que la gestionen.
- Augmentant la monitorització i correlació d'esdeveniments amb l'adquisició de noves eines. Aquestes hauran de ser capaces de monitoritzar el tràfic de xarxa, els usuaris remots, les contrasenyes d'administració, etc. Aquesta capacitat de correlació és molt important per la posterior generació d'intel·ligència, fruit de l'anàlisi policial.
- Millorant la política de seguretat corporativa. Adequant progressivament els permisos d'usuari, serveis en el "núvol" i regular mitjançant eines de control remot la utilització de dispositius i equips propietat de l'usuari Bring Your Own Device (BYOD).
- Millorant les configuracions de seguretat en tots els components de la xarxa corporativa policial. S'inclouran els dispositius mòbils i portàtils, ja que la tendència europea i mundial és la d'incorporar progressivament equips de mobilitat per qualsevol activitat policial.
- Potenciant l'ús de productes, equips i serveis de confiança i certificats, garantint l'accés als sistemes sense intrusions alienes no admeses. Establir i segmentar xarxes i sistemes acreditats per a informació sensible o classificada.
- Automatitzant i incrementant l'intercanvi d'informació amb d'altres centres de ciberseguretat, tant de l'administració pública com del sector privat. Potenciant la reciprocitat amb d'altres organitzacions i equips de Resposta a Incidents de Seguretat de la Informació, tant els CERT com els CSIRT[46].
- Consolidant el compromís de la Direcció (Prefectura de la Policia) amb la ciberseguretat. La escala superior[47] del cos (comissaris i intendents) han de ser els primers en assumir i acceptar que hi ha riscos i promoure amb fermesa les polítiques de seguretat.

[46] Durant aquest any 2018, la UCIBER dels Mossos d'Esquadra s'ha incorporat als equips de ciberseguretat i gestió d'incidents espanyols. Disponible a: https://www.csirt.es/index.php/es/

[47] La PG-ME es divideix en escales de comandament, on en el vèrtex de la piràmide es troba l'escala superior, amb els graus de Major, Comissari i Intendent

- Augmentant la formació i la sensibilització d'usuaris (part més feble de la cadena). Tots i cada un dels usuaris de l'organització han de ser conscients dels riscos inherents al sistema. Dissenyar nous cursos a l'Institut de Seguretat Pública de Catalunya (ISPC), establint noves jornades de formació pels serveis que disposin d'informació altament confidencial i formant part des de la UCIBER dels mòduls/crèdits de formació del curs bàsic de la policia. *(aquest serà el primer any que s'incorpora)

- Potenciant la difusió de la legislació i les bones pràctiques, augmentant les intervencions de la UCIBER a la intranet corporativa i mitjançant correu electrònic. Aprofitar els esdeveniments sobre ciberincidents amb alt ressò als mitjans de comunicació per continuar creixent amb la cultura de ciberseguretat.

- Adequant-nos als diferents estàndards (en el cas de les Administracions Públiques a l'Esquema Nacional de Seguretat -ENS-) i a la nova legislació europea que tot el just el 25 de maig de 2018 ha entrat en vigor amb aplicació directa.

- Treballant sempre com si els nostres sistemes estiguessin compromesos. Suposant que ho estan o que ho estaran en breu, en ajudarà a treballar en la resiliència de la organització i a protegir els actius fonamentals. En aquest sentit i durant el setembre de 2018 es preveu l'adquisició d'eines per realitzar ciberexercicis que simulin un atac cibernètic en seu policial o dins el seu entorn.

5 L'estudi

5.1 Objectius

Sota un prisma i àmbit estratègic que es cenyeix a coneixements genèrics de seguretat de la informació, establirem un qüestionari que faci referència a bones pràctiques i normativa.

En aquest estudi es pretén comprovar d'una manera pràctica, si hi ha relació entre les variables de destinació operativa dels agents i els coneixements seguretat de la informació

5.2 Hipòtesi

La conscienciació en seguretat de la informació i cultura de ciberseguretat que es genera, és superior en el servei que la crea que en els serveis que la reben, situant primerament als serveis centrals que, per qüestions d'especialitat, tenen més tendència absorbir-la i incorporar-la en el seu si d'expertesa.

5.3 Justificació

La hipòtesi inicial consisteix en la premissa que l'Àrea de Seguretat en Tecnologies de la Informació, mitjançant la Unitat de Ciberseguretat Policial i la Unitat de Gestió d'Usuaris, tenen una cultura de ciberseguretat, com a generadors de la cultura de ciberseguretat, superiors i amb marcada diferència d'altres serveis centrals –amb nivells d'especialització d'altres àmbits- i dels serveis territorials, que són els que reben en definitiva la conscienciació, i les polítiques de seguretat més operatives.

Només tenint en compte l'àmbit de treball i les tasques que com agents de policia de la funció pública li són encomanades i que treballen diàriament en el seu servei ordinari, és altament probable que el grau de conscienciació sigui percentualment superior.

De retruc, també ens trobem que a franges d'edat més elevada, més conscienciació i coneixement de normativa de seguretat de la informació existeix. Cal tenir en compte a més, que a edats més avançades, més anys de servei duen els enquestats, tenint en compte que especialment en els serveis centrals, la mobilitat dels agents fa anys que és reduïda a causa de la finalització dels desplegament el 2008.

5.4 Subjectes i mètodes

Per tal d'agilitzar al màxim l'entrega i gestió dels resultats, es va decidir crear un qüestionari utilitzant la plataforma Google Docs, que va permetre una recopilació de dades en línia de manera gratuïta i ordenada. L'enquesta, doncs, es va respondre mitjançant dispositius mòbils

on rebien els usuaris un enllaç escurçat amb l'enllaç mitjançant l'aplicació mòbil WhatsApp, oferint privacitat als usuaris.

Seguint aquest procediment, els enquestats disposaven de tot el temps que necessari per reflexionar i marcar cada una de les seves respostes, tenint en compte que a les instruccions prèvies ja s'advertia que, pel caràcter genèric de les qüestions, en 5 minuts ho podien enllestir

El qüestionari es va realitzar en català a partir d'una combinació de preguntes amb resposta curta tancada i d'altres amb resposta de veritat o fals. Tanmateix, totes les preguntes possibles van anar acompanyades d'una codificació per facilitar la posterior extracció i tractament de les dades.

Un cop finalitzat el qüestionari, es donava retorn als enquestats on podien veure, d'una banda les preguntes encertades i les errades, i d'altra banda els comentaris de l'autor a les preguntes quan aquestes eren incorrectes. S'ha aprofitat les preguntes per fer una tasca més de conscienciació i de cultura de ciberseguretat dins els cos.

Una mostra total de 42 usuaris dels SIP entre tots els enquestats han participat en aquest qüestionari adscrits als següents serveis:

Àrea de Seguretat en Tecnologies de la Informació (14):

7 agents de la Unitat de Ciberseguretat Policial

7 agents de la Unitat de Gestió d'Usuaris

Serveis Territorials (14):

5 agents de l'Àrea Bàsica Policial de l'Hospitalet de Llobregat.

4 agents de l'Àrea Bàsica Policial de Les Corts (Barcelona)

1 agent de l'Àrea Bàsica Policial de Manresa

2 agents de l'Àrea Bàsica Policial de Mataró

2 agents de l'Àrea Bàsica Policial de Vielha e Mijaran

Serveis Centrals (14):

1 Grup Especial d'Intervenció (GEI)

1 Àrea d'Instructors de l'ISPC

6 Àrea de Coordinació Interpolicial de la CGTSE

2 Àrea Tècnica de Dispositius de la CGTSE

1 Àrea de Mitjans Tècnics de la CGIC

1 Oficina de l'Entorn Penitenciari de la CGIC

1 Àrea d'Escortes de la CGRO

1 Àrea de Mitjans Tècnics de la CGINF

5.4.1 Estructura i disseny del qüestionari

El qüestionari es va dividir en un bloc previ amb dades preliminars genèriques referides als usuaris pròpiament i dos blocs temàtics de coneixement, un d'ells genèric i l'altre específic propi de la PG-ME

5.4.1.1 Bloc 0

El bloc inicial de dades preliminars buscava saber, dins l'anonimat del qüestionari, a quin servei estava destinat l'agent.

Serveis territorials: Correspon al global de tots els agents que estan destinats a les comissaries d'arreu del territori amb tasques de patrullatge, a les oficina d'atenció d'atenció al ciutadà (OAC) i els Grups d'Atenció a la Víctima, així com els destinats a les Sales Regionals de Comandament. Formen el gran gruix dels efectius de cos, sobre un 80%.

Serveis centrals: Correspon al global dels efectius que donen servei a tota Catalunya, són serveis que corresponen a la majoria de famílies d'especialitats que disposa el cos, com GEI, TEDAX, Escortes, Brigada Mòbil, Investigació avançada, Policia científica o Informació.

Àrea de seguretat en tecnologies de la informació: Aquesta Àrea està englobada dins de la Divisió de Sistemes d'Informació Policial (DSIP), adscrita a la Comissaria General de Planificació de la Seguretat, i encara que englobada dins els serveis central, és l'Àrea que per decret (Decret 415/2011) vetlla pel disseny, implantació, gestió i avaluació dels mecanismes necessaris per a la seguretat dels sistemes d'informació policial.

D'altra banda, la segona qüestió abordava sobre la franja d'edat de l'agent en qüestió, tenint en compte que, en qualsevol cas, el cos de Mossos d'Esquadra s'ha estat desplegant arreu del territori des del 1994, i per tant hi ha agents que ja han començat a retirar-se o que han agafat la segona activitat.

5.4.1.2 Bloc 1

Aquest bloc estava centrat en conceptes genèrics de seguretat de la informació amb l'objectiu d'oferir informació sobre els coneixements bàsics que disposen els agents sobre la cultura de ciberseguretat que els pot afectar habitualment en la seva vida diària, el riscos i perills als quals estan sotmesos sovint, més enllà de les tasques professionals que tinguin assignades.

Comprèn les primeres 14 preguntes amb la següent distribució:

. 10 preguntes que s'associen a 3 respostes curtes, del les quals només una és l'encertada. Al ser conceptes relacionats amb la conscienciació és possible arribar a deduir algunes respostes correctes a partir de descartar les altres opcions.

. 4 preguntes de veritat o fals. Busquen discriminar mitjançant afirmacions la claredat del concepte, en aquest cas, sobre les xarxes WiFi i les contrasenyes d'accés a serveis genèrics d'internet.

5.4.1.3 Bloc 2

Aquest bloc estava centrat en conceptes específics de ciberseguretat dins la PG-ME amb l'objectiu d'oferir informació sobre els coneixements que apliquen els agents sobre la cultura de ciberseguretat que els pot afectar diàriament en la seva vida professional.

Compren les últimes 6 preguntes amb la següent distribució:

. 5 preguntes de veritat o fals. Busquen discriminar mitjançant afirmacions la claredat del concepte sobre els el riscos i perills als SIP, el correu corporatiu i els llapis USB.

. 1 pregunta que s'associen a 3 respostes curtes, del les quals només una és l'encertada. És específica respecte la LOPD15/99.

5.5 Anàlisi i resultats

La recollida de dades va quedar bolcada de manera automàtica en un full d'Excel de Google que integrava totes les respostes aportades en el disseny del qüestionari. L'estructura d'aquest document, també allotjat "al núvol", va ser vital de cara a la consulta i anàlisi dels resultats.

Paral·lelament, mitjançant la plataforma de formularis de Google, es va auto generar un document associat a aquest full de respostes que mostrava un sumari de les respostes rebudes de forma visual. La disposició gràfica d'aquestes també va ser important de cara a la interpretació dels resultats a partir d'un anàlisi de contingut de les preguntes amb resposta tancada.

El global dels enquestats es distribueixen doncs segons els següents gràfics, on es representen les franges d'edat (figura 5) i les destinacions dels enquestats (figura 6):

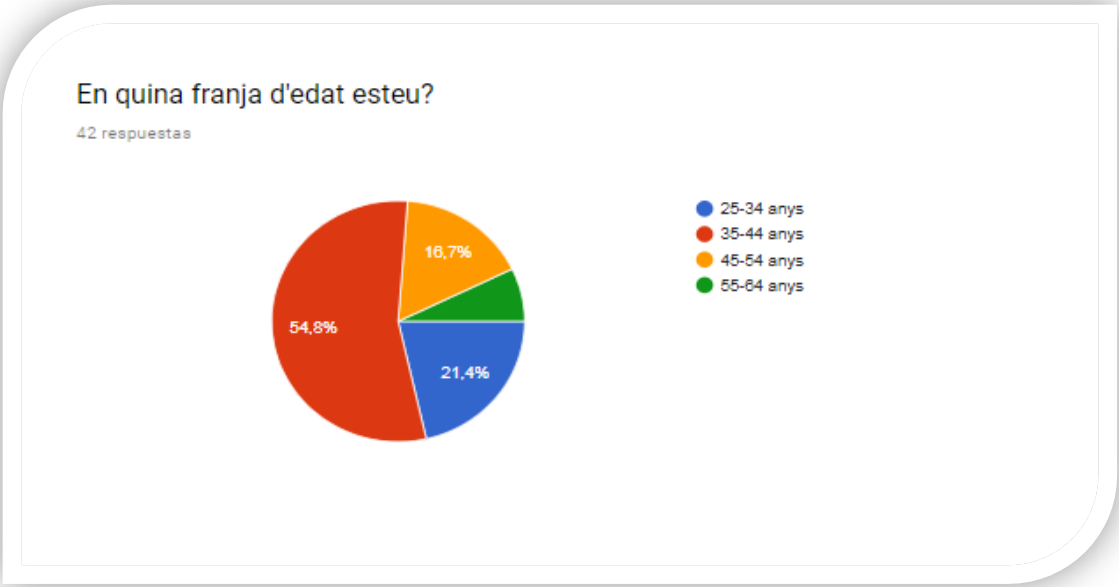


Figura 5. Distribució d'efectius per franja d'edat

Tal i com s'observa al primer gràfic, la franja d'edat que més ha col·laborat en aquest qüestionari ha estat la de 35 a 44 anys amb un 54,8%, que justament correspon amb la mitja d'edat de la PG-ME, i que per tant és la més freqüent en els serveis. La següent franja ha estat la dels més joves, de 25 a 34 anys amb un 21,4%, seguida de la dels 45-54 anys amb un 16,7% i finalment la de 55-64 anys amb un 7,1% com a més minoritària.

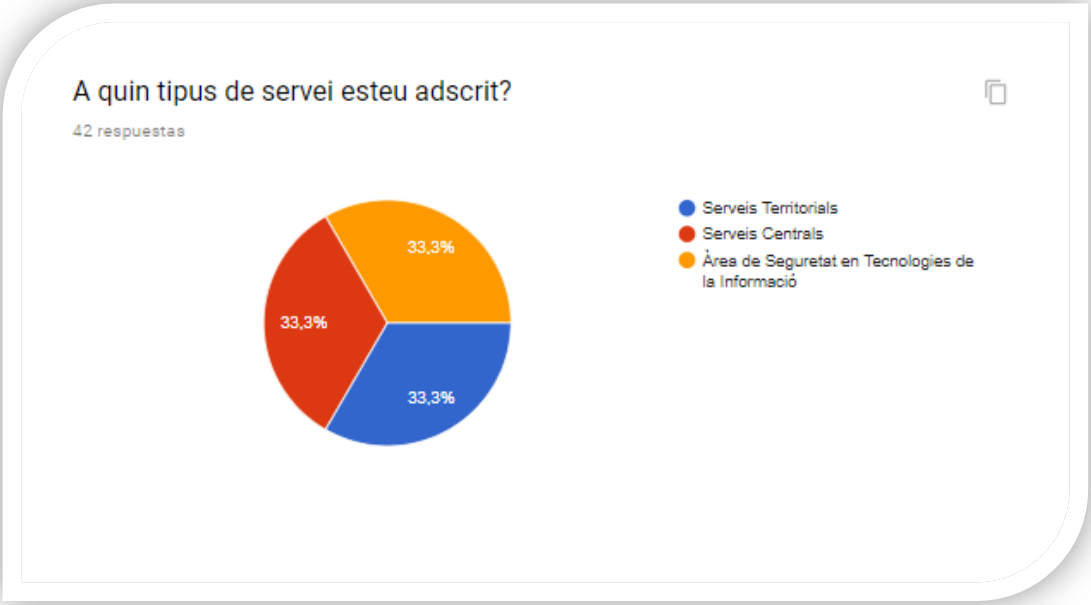


Figura 6. Distribució d'efectius per servei

En referència a l'origen del servei on està adscrit l'agent, s'ha guardat una proporció estricta en la mostra estimada en un 33,3% per grup, diferenciant clarament els generadors de la cultura que aborda l'estudi i on està englobada la UCIBER i la UGU dins l'ASTI (Àrea de Seguretat en Tecnologies de la Informació), i els perceptors d'aquesta cultura que són els serveis territorials i els serveis centrals, amb certes divergències dins els seu àmbit territorial i competencial tot cercant la major amplitud de visions possibles.

La distribució en l'encert de les qüestions i distribució d'edat s'ha distribuït de la següent manera:

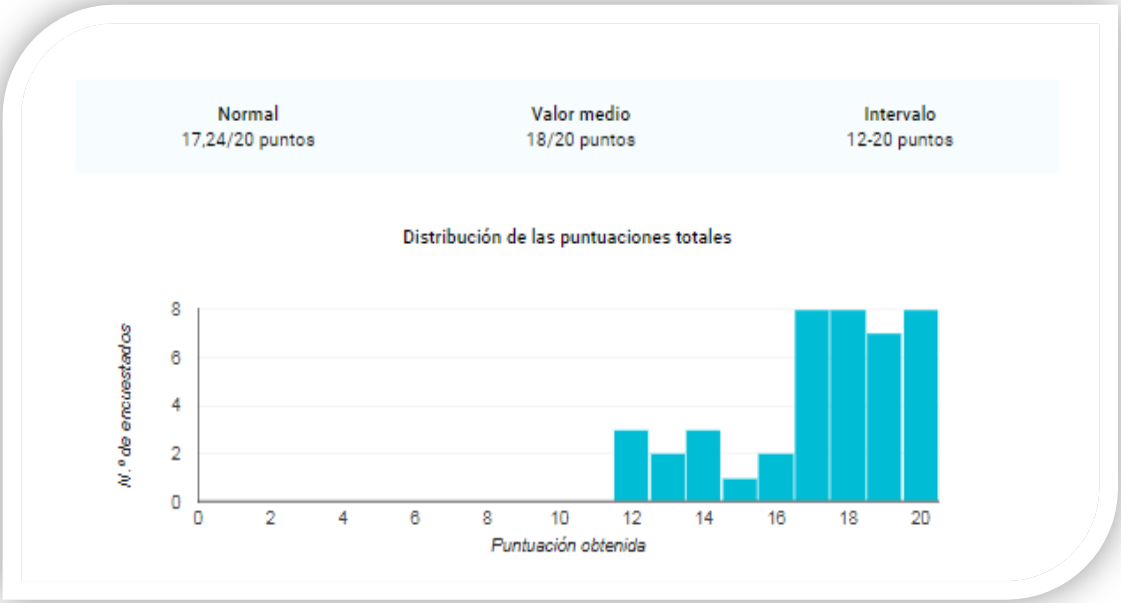


Figura 7. Distribució d'encerts

Com es veu en el gràfic, el major nombre d'encerts es situa en el bloc entre 17 respostes encertades i el màxim, amb 20 respostes encertades, amb un total de 17,24 respostes encertades de mitjana aritmètica. El mínim d'encerts, la pitjor puntuació, es situa en 12 respostes correctes, aprovant tots els participants els mínims de coneixements requerits per l'enquesta.

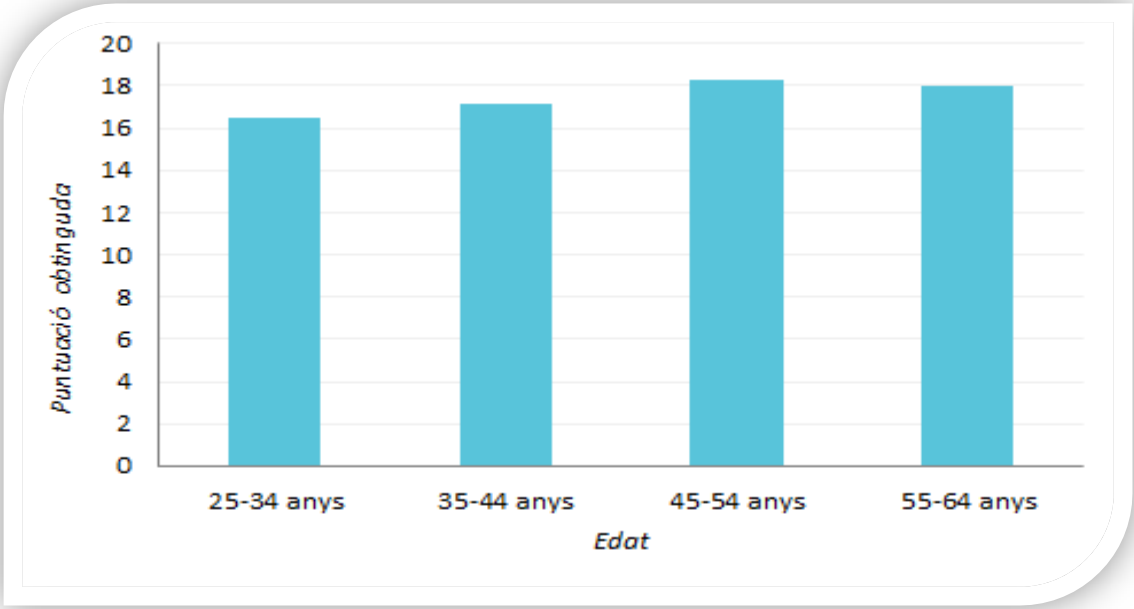


Figura 8. Distribució d'encerts per franja d'edat

La puntuació obtinguda respecte la franja d'edat es situa en uns paràmetres molts similars, oscil·lant entre les 18,28 respostes encertades entre 7 participants de 45-54 i 18 respostes encertades entre 3 participants de 55-64 anys com a millors valoracions, fins les 17,13 respostes encertades entre 23 participants de la franja 35-44 anys i 16,44 respostes encertades entre 9 participants de 25-34 anys.

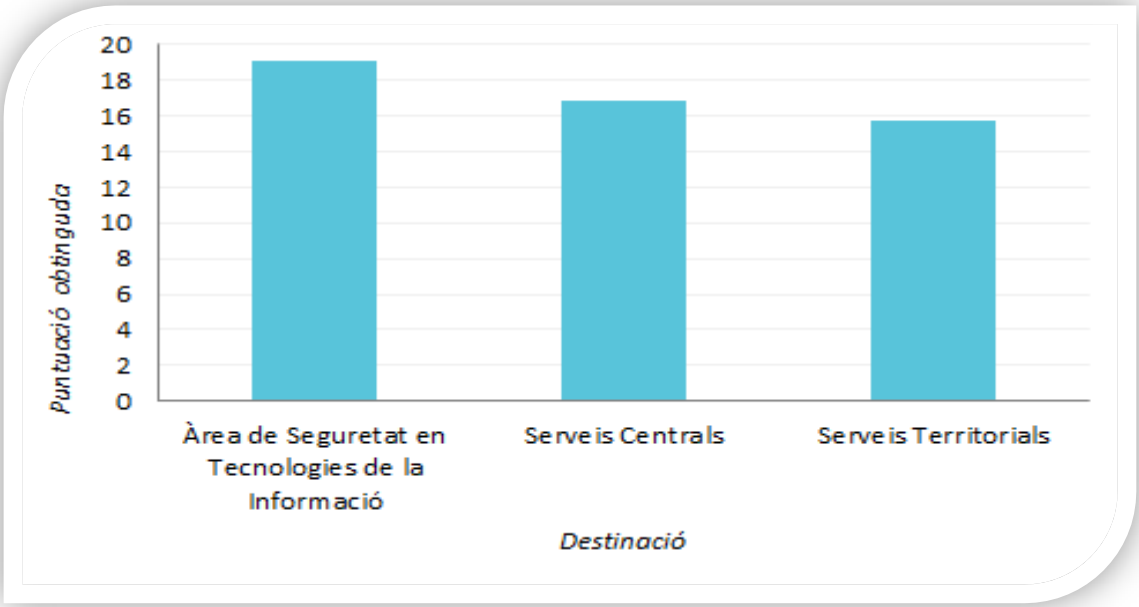


Figura 9. Distribució d'encerts per destinació

L'Àrea de Seguretat en Tecnologies de la Informació ha obtingut els millors resultats amb 19,07 encerts. El serveis centrals han quedat per darrera amb 16,85 encerts i en darrer lloc els serveis territorials amb una mitjana de 15,78 encerts. Totes les puntuacions sobre un total de 20 preguntes.

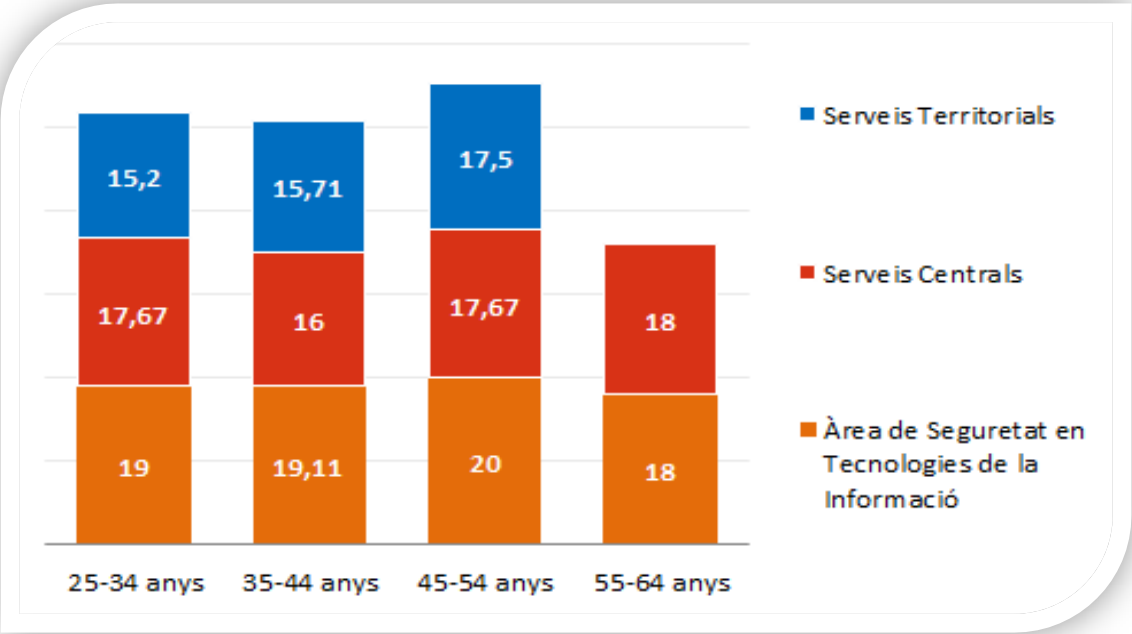


Figura 10. Distribució mitjana d'encerts per edat i destí

Un primer cop d'ull, s'observa que el grau de conscienciació i coneixements en ciberseguretat és més alt en l'Àrea de Seguretat de Tecnologies de la Informació en global, però concretament dins la franja de 45 a 54 anys, els encerts són plens i no s'observa cap errada en les respostes. Després en segon lloc estan els serveis centrals on la franja d'edat amb més respostes correctes ha estat la de 55 a 64 anys i per últim els serveis territorials on la màxima mitjana d'encerts s'ha trobat dins la franja de 45 a 54 anys. Cal destacar que no hi ha representació dins els serveis territorials entre els 55 a 64 anys.

En referència al resultat de les respostes crida l'atenció primerament les encertades sense cap errada per part dels participants:

- La pregunta número 6 fa referència a l'ús de les xarxes socials i la potencialitat en divulgar informació de manera inconscient i que potencialment pugui posar en risc dades personals de la pròpia persona o les persones que l'envolten.
- La pregunta número 8 fa referència a la recepció de correus de pesca que suplanten la identitat d'una entitat financera o un organisme públic per tal de obtenir dades confidencials de la persona i que potencialment li puguin generar un perjudici personal o econòmic.

En referència a les preguntes que han errat més els participants i que per tant hauran de ser motiu de reflexió, són les següents:

- La pregunta número 13 fa referència al canvi de contrasenya de WiFi que, tot i ser una bona pràctica per evitar intrusions, òbviament no és la única acció ni mesura a realitzar per minimitzar els riscos associats, tenint un ampli camp de millora dins la configuració del propi router*.
- La pregunta número 20 és la única que fa referència al marc normatiu de la protecció de dades de caràcter personal i on els participants han errat més (54,8%) que no pas han encertat (45,2%). La resposta a, que és errònia, arriba fins al 50% de les respostes errònies.

5.6 Discussió

5.6.1 Resum de resultats i validació

En referència al qüestionari, cal destacar que un cop analitzats els resultats, veiem primerament que la franja d'edat més participativa ha estat la que es comprèn entre els 35 i 44 anys. Tenint en compte que la mitjana d'edat al cos de Mossos d'Esquadra és propera als 40 anys, encaixa dins el que era d'esperar dins la mostra.

En quant als resultats per edats, no s'observen grans diferències entre les 4 franges analitzades. Hi ha una línia homogènia entre totes elles que fa que no calgui destacar cap per sobre de l'altra. Per molt jove que sigui l'agent, amb la recessió econòmica dels últims anys i donat que no hi ha hagut convocatòries noves per a agents, qualsevol efectiu del cos té com a mínim 6 anys d'antiguitat, i per tant tots ells han vist néixer la Unitat de Ciberseguretat policial fruit dels nous reptes tecnològics i de les amenaces inherents al qual el cos dels Mossos d'Esquadra estava exposat.

D'altra banda, s'ha cercat la participació proporcionada entre els serveis a estudiar i d'aquesta mostra i dels resultats que ha donat l'enquesta es desprèn que el servei que genera la cultura de ciberseguretat és el que ha tret el resultat més alt, qüestió lògica i que era d'esperar donat que cada agent participa d'aquesta cultura, tant informalment com de manera formal.

El segon millor resultat ha estat pels serveis centrals. S'ha de tenir en compte que aquestes unitats policials, que aglutinen serveis d'informació, d'investigació criminal avançada o de grups especials, treballen amb informació altament sensible i durant els anys s'han proveït d'una sensibilitat més elevada a l'hora de protegir la seva informació i estar alerta de possibles fuites no controlades o involuntàries. En els anys analògics aquesta reserva era exclusivament en l'àmbit físic i progressivament amb el pas dels anys, han anat evolucionant en la seguretat digital.

Per últim els serveis territorials. Era aquest un resultat esperable, donat que en la seva majoria són serveis que es donen amb ple contacte amb la ciutadania i on l'àmbit físic supera amb escreix l'àmbit tecnològic. Això provoca que la formació que la consciencia que es rebi sigui més per l'àmbit formal de l'organització i la difusió de continguts a través dels mecanismes de comunicació que s'han desgranat durant el treball, que no pas per aquesta cultura interna, invisible i que es genera diàriament i durant el pas del temps entre els companys de treball. En aquest sentit s'ha de continuar treballant.

En quant a la globalitat dels resultats, la mitjana de respostes encertades ha estat de 17,24 sobre un total de 20, amb un interval de 12 a 20 punts. Aquesta mitja s'ha vist penalitzada en especial per efectius dels serveis territorials. En aquest sentit, l'experiència del dia a dia i de l'evolució que com a comandament he anat percebent en els efectius del cos, es veu validada pels resultats amb l'aprovat amb nota tendint a l'excel·lència. Els resultats que s'han donat, per tant, corresponen amb la percepció subjectiva que es tenia preconcebuda.

Respecte a les respostes que com a resultats més han cridat l'atenció, bé sia per una resposta perfecte entre tots els enquestats, com per una clara desviació en l'encert, cal destacar que els agents tenen molt clar dels riscos de les xarxes socials com a eines de difusió massiva tant de notícies com de continguts. En aquest sentit, la revisió de les polítiques de privacitat dins les xarxes està garantida, presumiblement, dins el nostre cos policial.

També crida l'atenció el ple encert en els correus pesca[48] ("phishing") que puguin rebre els agents. S'ha fet un gran treball de difusió dels riscos que suposa clicar un enllaç davant un correu potencialment sospitós. Les jornades de conscienciació, els correus recordatoris de mesures d'autoprotecció digital, i la intranet corporativa han fet els seus efectes. Aquest a més, és un paràmetre que també pot afectar la vida particular dels agents, ja que l'ambició lucrativa dels cibercriminals no té mesura.

Si analitzem les preguntes amb més errades, ens trobem primerament amb la qüestió de la WiFi. Si bé els agents són conscients de la perillositat de les WiFi compartides o gratuïtes a través de les quals es poden connectar a la via pública, és remarcable que només es basin en la seguretat d'una contrasenya robusta. La desconeixença en la configuració d'un router juntament amb la tipologia de la pregunta amb el terme "completament", fa que el qui respon pugui acabar induint en error per manca de coneixements tècnics. D'altra banda, la única pregunta que versa sobre pura normativa, ha estat de lluny la més errada. No cal dir que era d'esperar que qui respon, davant la manca de coneixement literal de la norma, tendeixi a ser expansiu en la seva interpretació i per tant acabi englobant tant persones físiques com jurídiques dins l'àmbit estricte de la llei orgànica.

[48] Els correus pesca o "phishing" és un frau que es fa amb un correu electrònic o missatgeria instantània amb el que es demanen dades sobre les targetes de crèdit, claus bancàries, o altres tipus d'informació. Els missatges empren tot tipus d'arguments relacionats amb la seguretat de la nostra empresa per justificar la necessitat d'introduir les dades d'accés

Respecte a l'àmbit global d'aquest estudi, i tenint en compte els 3 nivells que categoritza l'escriptor, investigador i psicòleg Edgar Henry Schein (1988), autoritat en la matèria de la psicologia de les organitzacions, pare del desenvolupament organitzacional, i creador dels conceptes de cultura corporativa, cal destacar els següents paràmetres;

La consolidació del primer nivell, visible i conscient, que ha comprès tant la diferenciació de l'entorn físic d'organització, amb la creació d'una nova unitat policial i per tant modificant la tecnoestructura de la organització i la seva arquitectura, la nova provisió de recursos humans amb uns requeriments de coneixements elevats i de constant actualització i amb uns equips informàtics altament sofisticats, molt per sobre de la mitja de la organització. Amb patrons de comportament clarament diferenciats i visibles, i encara que sense un vestuari que els diferenciï, el llenguatge verbal fruit de la seva expertesa els fa de fàcil reconeixença. També aquí s'inclou el compromís de la direcció, en aquest cas el de la Prefectura de la Policia com a ens que lidera el comissari en cap del cos, la qual dóna el vist i plau final per tal que es creïn les estructures necessàries per garantir la ciberseguretat i enfortir la resiliència de l'organització en cas de ciberatac consumat. És doncs, una forma clara de manifestació d'aquest cultura de ciberseguretat, però tal i com indica Schein (1988) no podrem saber-ne de la seva essència sense un estudi més rigorós i metodològic dels altres dos nivells.

La consolidació del segon nivell, menys visible i semi inconscient, en quant als valors que dirigeixen el comportament dels membres de la organització. Com s'entén la ciberseguretat dins la organització i si tots els seus components que la integren l'entenen igual. Tot i que, segons Schein (1988) la seva identificació només és possible a través d'entrevistes amb els membres claus de l'organització, aquesta tasca s'ha anat elaborant progressivament amb els retorn amb reunions i jornades directives de l'organització on el retorn ha estat altament positiu. Per aquest motiu, s'ha fet un esforç en no concórrer en l'error d'idealitzar aquest fenomen, ja que fins i tot ho podríem entendre com una clara limitació de l'estudi. Tot i així, dins aquest esforç d'objectivitat, s'han enumerat durant el treball les diferents estratègies emprades, les fites i objectius a assolir, la filosofia en ciberseguretat que s'ha endegat envers els usuaris dels sistemes d'informació policial, la sèrie de valors que s'han creat dins la cultura, i el que és més important, quines accions cal continuar realitzant per tant que aquesta creixi, maduri i s'instal·li permanentment en l'organització.

La consolidació del tercer nivell , invisible i inconscient, com a forma com el cos de Mossos d'Esquadra percep, pensa, sent i actua dins l'àmbit de la ciberseguretat. Aquest nivell és el que costa més d'assentar i requereix una inversió de temps superior al dels altres dos. S'ha anat construint a mesura que el cos policial ha anat rebent ciberatacs, quan han hagut pèrdues d'informació, quan s'han produït fuites d'informació malintencionades, s'ha hagut de cercar els responsables, i s'han proveït l'organització de mesures tecnològiques i humanes per tal que no es produeixin ciberincidents de les mateixes característiques. Tot plegat s'ha anat construint aquesta cultura a mesura que s'han anat solucionant problemes de manera eficaç i eficient, on tant la direcció com la base de la organització s'han vist involucrades en circumstàncies que han estat resoltes per la UCIBER, contingut i detall del qual no es susceptible de ser desgranat en el present treball per motius de confidencialitat de la

informació. El pas dels anys ha fet doncs, una unitat policial de creació relativament nova, un recurs gairebé imprescindible pel cos, tenint en compte més que mai, els criteris de ciberseguretat davant qualsevol solució tecnològica que adopti la organització.

5.6.2 Limitacions

Les principals limitacions que m'he trobat dins el context del present treball han estat per una banda les dimensions de la mostra en l'enquesta. Certament, quan més s'amplia la mostra més aproximació a la realitat es produeix. A més, la homogeneïtat s'ha centrat exclusivament amb la distribució dels efectius policials per serveis, però no s'ha tingut en compte la franja d'edat de l'enquestat, fent d'aquest ítem quelcom residual. En aquest sentit, la manca d'efectius de la última franja, la situada entre 55 i 64 anys, és més que notòria per realitzar un anàlisi més complet.

D'altra banda la manca d'articles dins la cultura de les organitzacions que s'englobin dins el context policial és molt minsa i per tant l'adequació de les teories dels nivells de cultura de les organitzacions només s'ha pogut realitzar amb la coneixença àmplia de la organització i essent partícip del procés de creació. Sense aquesta visió descriptiva, aquest estudi hagués estat certament incomplet o minvat de les possibilitats reals d'estudi.

5.6.3 Transportabilitat

Si ens plantegem l'ús d'aquest estudi com a cas d'èxit dins la creació d'una nova cultura dins un entorn policial, dins les policies locals es plantegen seriosos dubtes en quant a la seva aplicació. D'una banda perquè els sistemes d'informació policial són gestionats i dirigits pel cos de Mossos d'Esquadra, amb el qual l'àmbit d'actuació queda molt reduït. D'altra banda, les dimensions de recursos humans dels ajuntaments són limitats en número amb d'altres prioritats per àmbits d'actuació i de tasques encomanades, i no permeten el fet de mantenir personal altament qualificat que vetlli per garantir aquesta cultura. En definitiva, són purs receptors dels procediments, normatives i mesures implementades que des del cos autonòmic s'aplica als SIP. No obstant això, hi ha un òrgan de coordinació del conjunt de policies locals que donen servei a Catalunya, la Subdirecció General de Coordinació de Policies Locals, la qual pot fer de pont i lligam especialment en el nivell 2 de cultura de les organitzacions, en quan a valors i normativa i també en el 3 en quant a ciberconscienciació.

D'altra banda, la resta de policies, ja dins l'àmbit estatal i europeu, han tendit igualment a la creació de tecnoestructures amb dotació de personal i recursos tecnològics per nodrir el nivell 1 de la piràmide, amb el qual més que aplicació serveixen les trobades nacionals i europees per intercanvi d'experiències i de casos d'èxit en la gestió d'incidents, però en cap cas aplicable ja que aquesta cultura ja és aplicada dins les seves organitzacions.

5.7 Conclusió de l'estudi

Pels motius anteriorment exposats, tenint en compte els resultats del qüestionari de conceptes bàsics en ciberseguretat i els conceptes específics de ciberseguretat dins la PG-ME, es dóna per validada la relació directa que hi ha entre destinació operativa dels agents i els coneixements seguretat de la informació.

D'una banda perquè tots els integrants del qüestionari han superat el test arribant a les 17,24 respostes encertades sobre 20 preguntades de mitjana aritmètica i d'altra perquè la nota de l'avaluació ha crescut progressivament començant pels serveis territorials amb 15,78 encerts, ascendint en els serveis centrals amb 16,85 encerts i finalitzant amb excel·lència per part de l'Àrea de Seguretat en Tecnologies de la Informació amb 19,07 encerts, el qual denota la certesa de la hipòtesi plantejada inicialment.

6 Conclusions finals

La cultura en ciberseguretat s'ha arrelat d'una manera ferma dins el cos de Mossos d'Esquadra. Sens dubte, l'aparició de normativa i noves estructures que obliguen a l'administració pública a realitzar unes accions per protegir les seves infraestructures ha ajudat i molt a crear-la, especialment en el seu nivell piramidal més alt, tal i com detalla l'autor Edgar Shein en la seva classificació dels nivells de cultura organitzacionals, el dels artefactes i les estructures. Per aquest motiu s'ha desgranat com s'ha creat cultura de ciberseguretat dins el cos de Mossos d'Esquadra, en quin context i quina evolució ha suposat per l'organització. L'aparició de normativa que desenvolupa la ciberseguretat, que detalla quines mesures preceptives s'han de prendre mitjançant anàlisi de riscos i com s'han d'aplicar sens dubte han ajudat també a desenvolupar-la.

Certament, aquest fenomen no es pot produir només amb un canvi de tecnoestructures dins el si del cos, sinó suposa quelcom més profund, més invisible, més impregnat de l'experiència i del dia a dia dels professionals que la integren. Per tal d'estudiar-la doncs, especialment des d'un prisma descriptiu, cal viure-la dia a dia i així poder-la analitzar i identificar els elements que la desenvolupen, especialment des de la creació de la Unitat de Ciberseguretat Policial.

Però no ens hem aturat només en aquest àmbit descriptiu, sinó que s'ha volgut anar més enllà per tal de verificar, mitjançant qüestionari amb mostra, si hi ha diferència de visions entre la Unitat que vetlla per la ciberseguretat dins la policia i la resta d'Unitats que la reben com a producte. En aquest sentit s'ha validat la hipòtesi plantejada tenint en compte la variable del nombre d'encerts en qüestionari, que ha donat com a resultat que l'Àrea de Seguretat en Tecnologies de la Informació ha obtingut una nota excel·lent respecte els serveis centrals i els territorials, que són als que arriba aquesta cultura en ciberseguretat de major a menor respectivament.

És en aquest punt on, a banda de les limitacions en el mètode que s'han descrit anteriorment, s'ha validat que aquesta cultura és present i arrelada però es desdibuixa progressivament a mesura que s'allunya de l'emissor i es transmet, com una cadena d'informació, fins a l'últim funcionari que està a peu de carrer.

Així mateix i arran també del resultat, s'han validat els nivells 2 i 3 de cultura organitzacional, corresponents als valors i a com s'entén la ciberseguretat dins els agents i comandaments que conformen l'organització respectivament, i on queda un llarg recorregut a fer que s'haurà de preveure en les estratègies de futur que s'han descrit per tal de mantenir-la i fer-la créixer.

Alhora i com a punt feble de l'organització, com en la resta de l'administració pública, es troba en el personal que s'hi troba adscrit i en el qual, només amb la conscienciació, la difusió, l'assimilació de continguts i la coresponsabilitat pròpia de la ciberseguretat, s'hi podrà fer front d'una manera òptima als reptes del futur que cada vegada són més elaborats i complexes.

Per aquest motiu i agafant com a referència els nivells de cultura organitzacionals descrits per Edgar Henry Schein durant l'any 1988, concloem la cultura de ciberseguretat com una cultura

forta, arrelada, ferma, consolidada, dominant i present dins el cos de Mossos d'Esquadra, sens perjudici del llarg recorregut que, dins el món de les tecnologies i les comunicacions, queda per recórrer.

Bibliografia

S'ha utilitzat la norma d'estandardització suggerida per la Universitat de Barcelona en la seva plana web respecte els documents digitals. S'ha comprovat la validesa de cadascun dels enllaços a sota relacionats abans de la impressió del present treball.

BOCG de 24 de novembre de 2017. Projecte de Llei Orgànica de Protecció de dades de caràcter personal 121/000013 Disponible a : http://www.congreso.es/backoffice_doc/prensa/notas_prensa/57631_1518684517278.PDF

BOE-A-1999-23750 Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. Disponible a: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

BOE-A-2003-20253 Llei 32/2003, de 3 de novembre, general de telecomunicacions. Disponible a: https://www.boe.es/boe/dias/2003/11/04/pdfs/A38890-38924.pdf

BOE-A-2003-23399 Llei 59/2003, de 19 de desembre, de signatura electrònica. Disponible a: https://www.boe.es/buscar/pdf/2003/BOE-A-2003-23399-consolidado.pdf

BOE-A-2010-1330-C Reial Decret 3/2010, de 8 de gener. Esquema Nacional de Seguretat. Disponible a : https://www.boe.es/boe_catalan/dias/2010/01/29/pdfs/BOE-A-2010-1330-C.pdf

BOE-A-2011-007630-C Llei 8/2011, de 28 d'abril, mesures per la protecció d'infraestructures crítiques. Disponible a: https://www.boe.es/boe_catalan/dias/2011/04/29/pdfs/BOE-A-2011-7630-C.pdf

BOE-A-2013-5771-C ReIal Decret 385/2013, de 31 de maig, de modificación del Reial Decret 1886/2011, de 30 de desembre. Estratègia de Seguretat Nacional de 2013. Disponible a: http://www.dsn.gob.es/es/file/144/download?token=JdtEVkaN

BOE-A-2015-10565-C de 02/10/2015. Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques. Disponible a: https://www.boe.es/boe_catalan/dias/2015/10/02/pdfs/BOE-A-2015-10565-C.pdf

BOE-A-2017-15181 Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017. Disponible a: https://www.boe.es/boe/dias/2017/12/21/pdfs/BOE-A-2017-15181.pdf

BOE-Codi electrònic, 31 de gener de 2018, Código del derecho de la ciberseguridad. Disponible a: https://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=173_Codigo_de_Derecho_de_la_Ciberseguridad.pdf

CESICAT (2018), Informe sobre tendències en ciberseguretat 2017. Disponible a: https://ciberseguretat.gencat.cat/web/.content/PDF/20180430_Analisi-Tendencies-2017.pdf

DOGC número 1923. LLEI 10/1994, d'11 de juliol, de la policia de la Generalitat - Mossos d'Esquadra. Disponible a: http://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_resultats_fitxa/?documentId=93461&action=fitxa

DOGC número 5005. DECRET 243/2007, de 6 de novembre, d'estructura del Departament d'Interior, Relacions Institucionals i Participació. Disponible a : http://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_resultats_fitxa/?action=fitxa&versionId=1520856&versionState=02&language=ca_ES&documentId=423614&mode=single

DOGC número 5359. ACORD GOV/53/2009, de 24 de març, pel qual s'encarrega la prestació de serveis de tecnologies de la informació i comunicacions al Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya. Disponible a: http://portaldogc.gencat.cat/utilsEADOP/AppJava/PdfProviderServlet?versionId=997618&type=01

DOGC número 6025. DECRET 415/2011, de 13 de desembre, d'estructura de la funció policial de la Direcció General de la Policia, article 76.2b i 78 Disponible a: http://dogc.gencat.cat/ca/pdogc_canals_interns/pdogc_resultats_fitxa/?action=fitxa&mode=single&documentId=594021&language=ca_ES

DOGC número 6237. ACORD GOV/103/2012, de 16 d'octubre, pel qual s'encarrega a la Fundació Centre de Seguretat de la Informació de Catalunya la planificació, la gestió i el control de la seguretat de les TIC de l'Administració de la Generalitat i el seu sector públic. Disponible a: https://ciberseguretat.gencat.cat/web/.content/PDF/ACORD-GOV1032012.pdf

DOUE- Reglament (UE) 2016/679 del Parlament europeu i del consell - de 27 d'abril de 2016 - relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46 / CE (Reglament general de protecció de dades). Disponible a: https://www.boe.es/doue/2016/119/L00001-00088.pdf

DOUE- Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals i a la lliure circulació d'aquestes dades. Disponible a: https://www.boe.es/doue/2016/119/L00089-00131.pdf

Estratègia de Ciberseguretat Nacional 2013. Disponible a: http://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf

INCIBE (2017). Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario. Disponible a: https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el

INCIBE (2017). Prevención de intrusos y gestión de eventos para sistemas de control. Disponible a: https://www.certsi.es/blog/prevencion-intrusos-y-gestion-eventos-sistemas-control

INCIBE (2017). Kit de concienciación para empresas de INCIBE. Didponible a: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

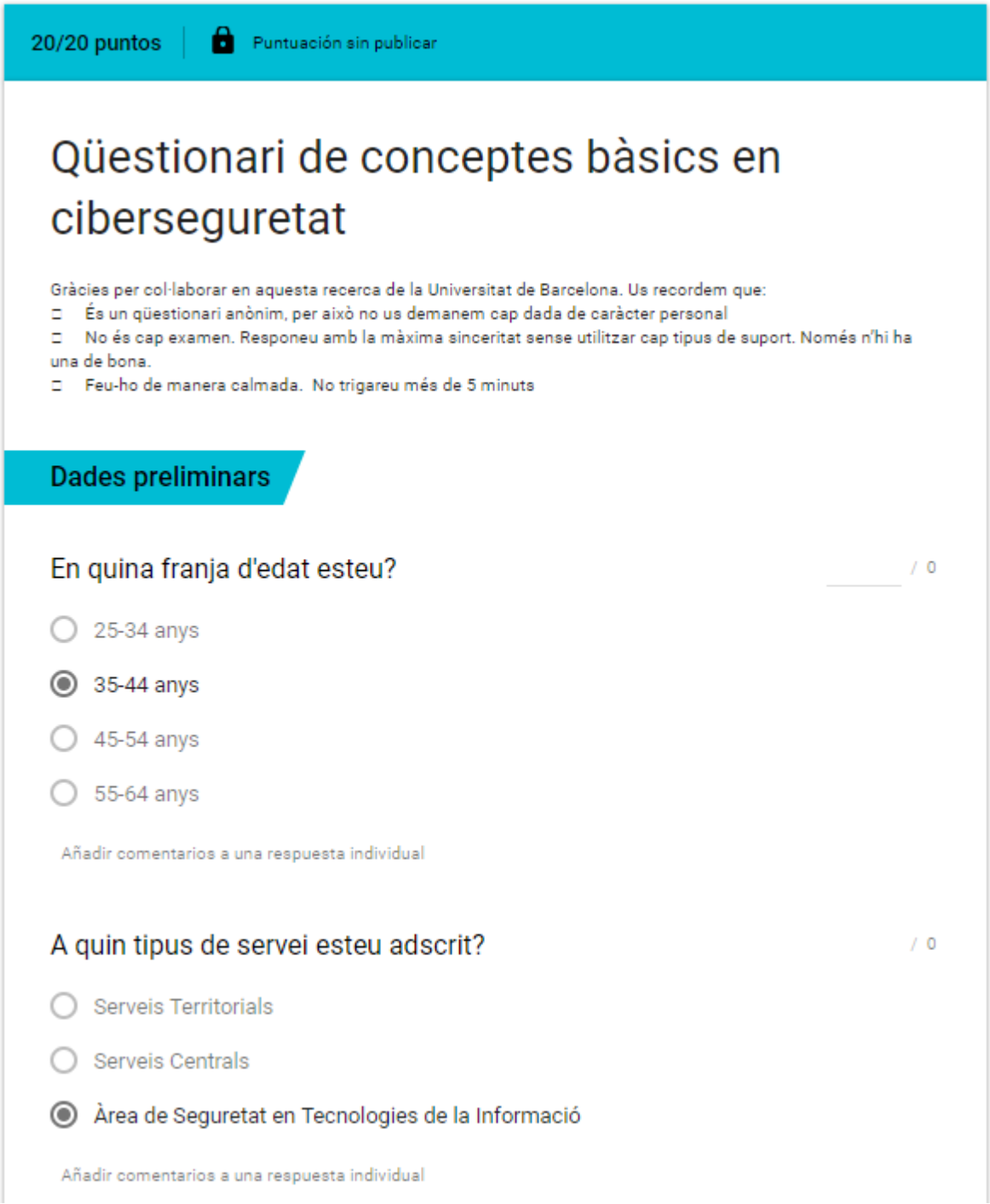
ISO 27001-SGSI. 2013. Estàndard per la Seguretat de la Informació. Sistema de gestió de seguretat de la informació. Disponible: http://www.iso27000.es/download/doc_sgsi_all.pdf

NICCS 2017, National Initiative for Cybersecurity Carriers and Studies. Department of Homeland Security. Disponible a: https://niccs.us-cert.gov/glossary

SCHEIN, E. (1988). La cultura empresarial y el liderazgo. Una visión dinámica. Plaza & Janes Editores. P.

Annexos

Annex 1. Model de qüestionari de conceptes bàsics en seguretat



20/20 puntos | Puntuación sin publicar

Qüestionari de conceptes bàsics en ciberseguretat

Gràcies per col·laborar en aquesta recerca de la Universitat de Barcelona. Us recordem que:

- És un qüestionari anònim, per això no us demanem cap dada de caràcter personal
- No és cap examen. Responeu amb la màxima sinceritat sense utilitzar cap tipus de suport. Només n'hi ha una de bona.
- Feu-ho de manera calmada. No trigareu més de 5 minuts

Dades preliminars

En quina franja d'edat esteu? / 0

- ○ 25-34 anys
- ◉ 35-44 anys
- ○ 45-54 anys
- ○ 55-64 anys

Añadir comentarios a una respuesta individual

A quin tipus de servei esteu adscrit? / 0

- ○ Serveis Territorials
- ○ Serveis Centrals
- ◉ Àrea de Seguretat en Tecnologies de la Informació

Añadir comentarios a una respuesta individual

BLOC 1. Conceptes genèrics de seguretat de la informació

✓ 1. És una bona pràctica utilitzar la mateixa contrasenya per accedir als Sistemes d'Informacio Policial (SIP) que a altres serveis d'Internet d'àmbit personal? 1 / 1

- (●) No, és millor utilitzar una contrasenya diferent per a cada servei. ✓
- ( ) Depèn, només si la contrasenya compleix els requisits mínims de seguretat: contenen majúscules, minúscules, números i caràcters especials.
- ( ) Si, d'aquesta manera no se t'oblida i evites haver de apuntar-la en algun paper o qualsevol altre lloc.

Añadir comentarios a una respuesta individual

✓ 2. Les xarxes socials són un servei que et permeten estar en contacte amb altres persones, per això ... 1 / 1

- ( ) Comparteixes tot el que fas amb tots els teus contactes, per això és una xarxa social.
- (●) Ets curós amb la informació que comparteixes i amb qui ho fas, per això has dedicat temps en configurar els nivells de privacitat. ✓
- ( ) Acceptes totes les sol·licituds d'amistat que reps, t'agrada tenir molts amics i companys, així teves publicacions tenen més èxit (més "likes", compartits, etc.).

Añadir comentarios a una respuesta individual

✓ 3. De manera general, en quins casos no es recomana fer ús del núvol 1 / 1

- ( ) Per compartir la informació amb altres persones.
- (●) Per emmagatzemar informació sensible (DNI, contrasenyes, dades personals en general), ja sigui propi o aliè, de tipus personal o corporatiu. ✓
- ( ) Per guardar arxius a manera de còpia de seguretat.

Añadir comentarios a una respuesta individual

✓ 4. Què és una xarxa zombi? 1 / 1

- Un tipus de connexió a Internet en la qual, la principal característica és que a les nits permet una major velocitat de navegació.
- És una xarxa privada d'ordinadors que està protegida enfront d'amenaces d'Internet.
- **És un conjunt d'ordinadors infectats per un mateix tipus de virus i que és controlat per un ciberdelinqüent per dur a terme accions malicioses.** ✓

Añadir comentarios a una respuesta individual

✓ 5. A Internet, quan parlem de galetes, a què ens referim? 1 / 1

- **Petits fitxers que els navegadors emmagatzemen a l'ordinador amb dades de l'usuari sobre les pàgines web que visita.** ✓
- A un tipus de virus que és capaç d'interceptar les comunicacions dels usuaris.
- Correus electrònics que es reenvien en cadena i que tenen com a objectiu enganyar els usuaris perquè facilitin informació confidencial.

Añadir comentarios a una respuesta individual

✓ 6. Un virus informàtic és capaç d'esborrar les fotos emmagatzemades en un ordinador? 1 / 1

- Mentida, això és una notícia falsa que circula per posar por als usuaris. Els virus el que fan és espatllar l'ordinador impedint que funcioni correctament.
- **Sí, alguns virus poden provocar la destrucció o esborrat dels arxius i quedar irrecuperables.** ✓
- Sí, encara que una vegada que eliminem el virus de l'ordinador podem recuperar tota la informació sense problemes.

Añadir comentarios a una respuesta individual

✓ 7. L'ús d'empreses d'enviament de diners instantani s'ha d'utilitzar per... 1 / 1

- ○ Realitzar compres per Internet, ja que permeten recuperar els diners en cas de frau.
- ○ Realitzar compres per Internet de manera anònima, així evites haver de facilitar les teves dades bancàries al venedor
- ◉ Enviar diners a persones conegudes, però mai per fer pagaments per Internet. ✓

Añadir comentarios a una respuesta individual

✓ 8. Heu rebut un correu del teu banc en el qual et demana confirmar les teves dades personals i bancàries de manera urgent, suposadament per motius de seguretat... 1 / 1

- ◉ Us sembla una mica estrany que el banc et sol·liciti aquestes dades. Decideixes contrastar la informació directament amb el banc abans de realitzar cap acció. ✓
- ○ Et preocupen molt els temes de seguretat. Per aquest motiu, fas clic a l'enllaç que et faciliten al correu per veure què és exactament el que necessiten.
- ○ És cert que el correu et resulta estrany ... però et pot la curiositat i fas clic a l'enllaç.

Añadir comentarios a una respuesta individual

✓ 9. Quins indicis han de fer-te sospitar sobre un possible anunci fraudulent publicat en una pàgina web? 1 / 1

- ○ Preus xollo.
- ◉ Sol·licitud de diners per avançat. ✓
- ○ Pagaments mitjançant PayPal.

Añadir comentarios a una respuesta individual

✓ 10. Els teus companys t'han demanat que els enviïs per telèfon una foto d'un finat per causes violentes, al qual has assistit per raó del servei... 1 / 1

- (●) No l'envies, ets prudent i et fa por que la foto caigui en mans de persones que no vols per alguna circumstància: t'enfades amb el company per algun motiu, li roben el mòbil, el perd en alguna actuació i surt a premsa, etc,,, ✓
- ( ) L'envies. Confies plenament en el teu company perquè has passat moltes penúries amb ell durant el servei i saps que mai et trairà.
- ( ) L'envies sense més, encara que algú la vegi en el seu mòbil no t'importa, saps que no dirà pas que li has enviat tu.

Añadir comentarios a una respuesta individual

✓ 11. És recomanable tenir apuntades les contrasenyes en algun lloc, així si s'obliden per algun motiu, podem consultar-les ràpidament. 1 / 1

- ( ) Veritat
- (●) Fals ✓

Añadir comentarios a una respuesta individual

✓ 12. Quan em connecto a una xarxa WiFi pública corro el risc que em robin les meves dades emmagatzemades dins el meu dispositiu (portàtil, mòbil, tauleta) 1 / 1

- (●) Veritat ✓
- ( ) Fals

Añadir comentarios a una respuesta individual

✓ 13. Canviar la contrasenya del WiFi de casa periòdicament evita completament que qualsevol intrús es connecti a la meva xarxa. 1 / 1

- ○ Veritat
- ◉ Fals ✓

Añadir comentarios a una respuesta individual

✓ 14. Totes les claus d'accés que disposo dins el meu món virtual són d'interès per als delinqüents. 1 / 1

- ◉ Veritat ✓
- ○ Fals

Añadir comentarios a una respuesta individual

Conceptes específics de ciberseguretat dins la PG-ME.

✓ 15. Els SIP són un entorn plenament segur, els fitxers de la policia no es poden infectar mai. 1 / 1

- ○ Veritat
- ◉ Fals ✓

Añadir comentarios a una respuesta individual

✓ 16. Les imatges són dels pocs arxius que, a dia d'avui, es poden obrir amb tranquil·litat ja que no contenen virus. 1 / 1

- ○ Veritat
- ◉ Fals ✓

Añadir comentarios a una respuesta individual

✓ 17. Si rebo un correu a la meva adreça corporativa @gencat.cat puc estar ben segur encara que provingui d'un desconegut, ja que haurà passat pels tallafocs i antivirus policials necessaris per tal de detectar-ne codis maliciosos als arxius. 1 / 1

- ○ Veritat
- ◉ Fals ✓

Añadir comentarios a una respuesta individual

✓ 18. No em cal xifrar els arxius amb dades de caràcter personal quan ho copio dins un "llapis de memòria USB", ja que es quedarà a comissaria i no sortiré pas al carrer amb ell. 1 / 1

- ○ Veritat
- ◉ Fals ✓

✓ 19. Amb només un clic a un enllaç d'un correu puc infectar la meva estació de treball i comprometre la resta que estiguin dins el mateix segment de xarxa. 1 / 1

- (●) Veritat ✓
- ( ) Fals

Añadir comentarios a una respuesta individual

✓ 20. Segons la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, entenem com dada de caràcter personal... 1 / 1

- ( ) Qualsevol informació referent a persones físiques o jurídiques identificades o identificables
- (●) Qualsevol informació referent a persones físiques identificades o identificables ✓
- ( ) Qualsevol informació referent a persones jurídiques identificades o identificables

Añadir comentarios a una respuesta individual

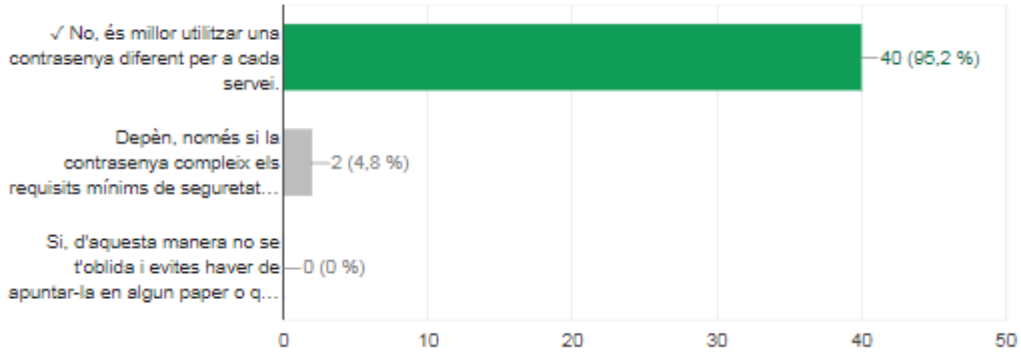
Moltes gràcies per la vostra col·laboració!

Annex 2. Detall de les respostes del qüestionari

BLOC 1. Conceptes genèrics de seguretat de la informació

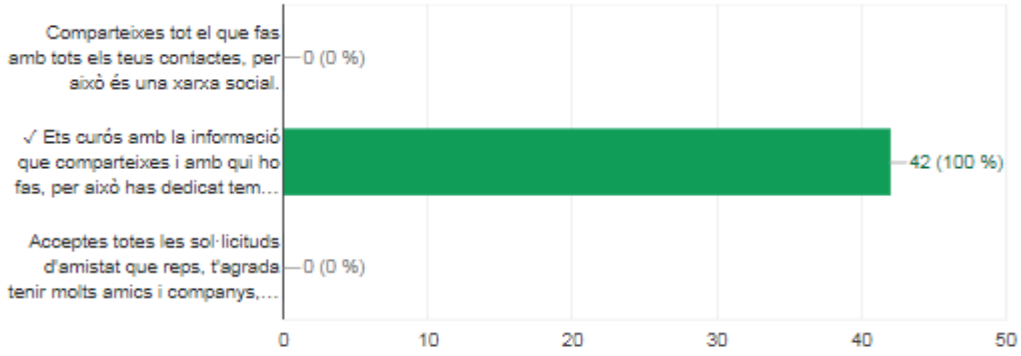
1. És una bona pràctica utilitzar la mateixa contrasenya per accedir als Sistemes d'Informacio Policial (SIP) que a altres serveis d'Internet d'àmbit personal?

40 de 42 respuestas correctas



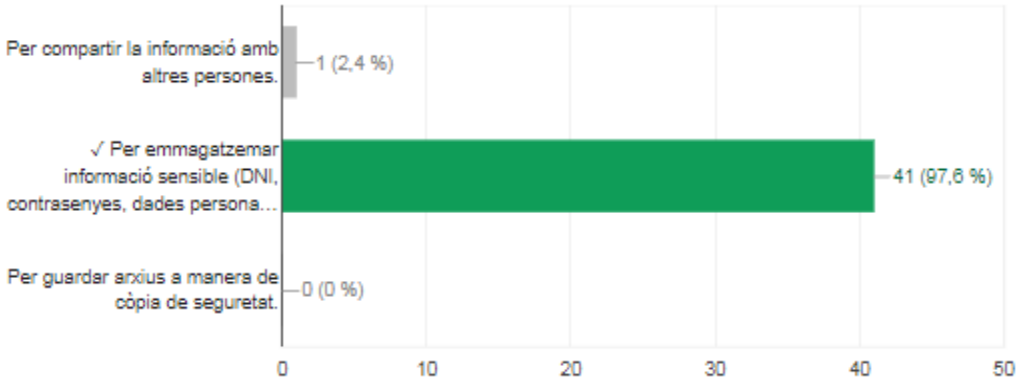
2. Les xarxes socials són un servei que et permeten estar en contacte amb altres persones, per això ...

42 de 42 respuestas correctas



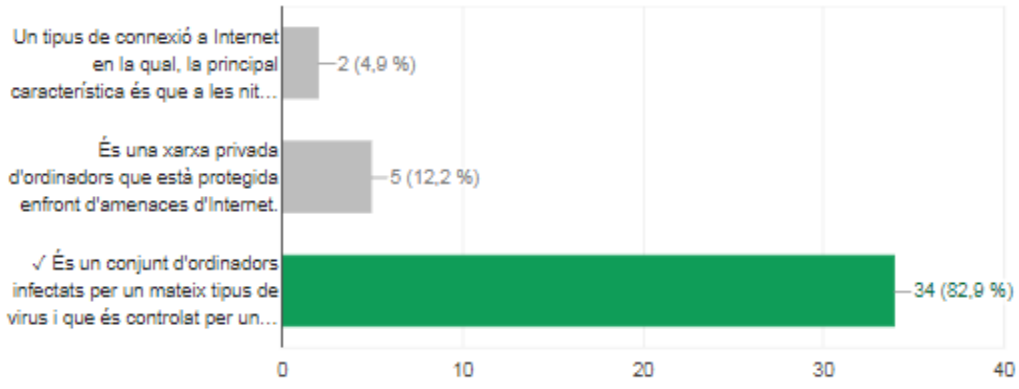
3. De manera general, en quins casos no es recomana fer ús del núvol

41 de 42 respuestas correctas



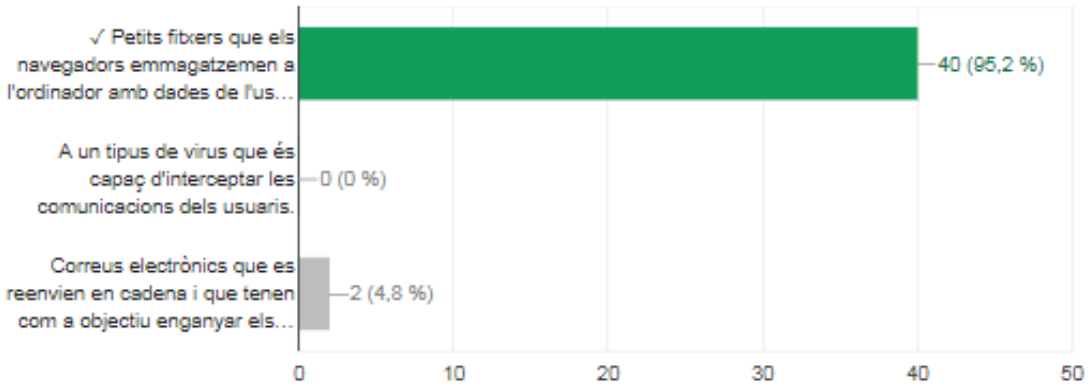
4. Què és una xarxa zombi?

34 de 41 respuestas correctas



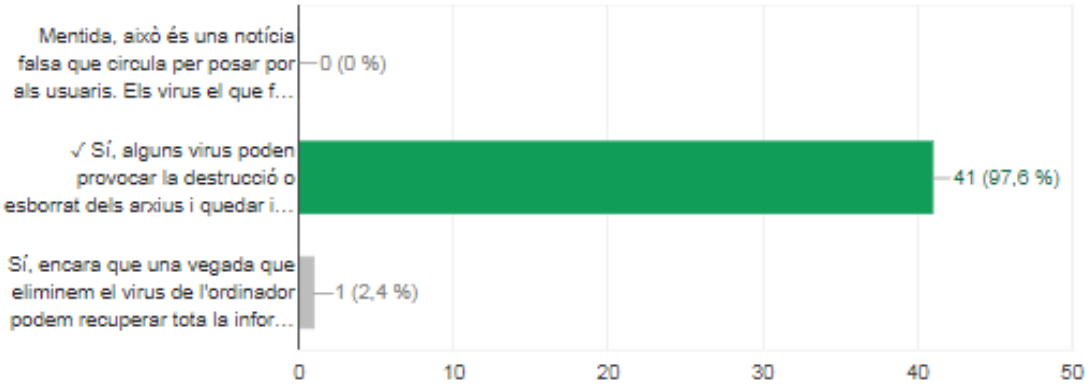
5. A Internet, quan parlem de galetes, a què ens referim?

40 de 42 respuestas correctas



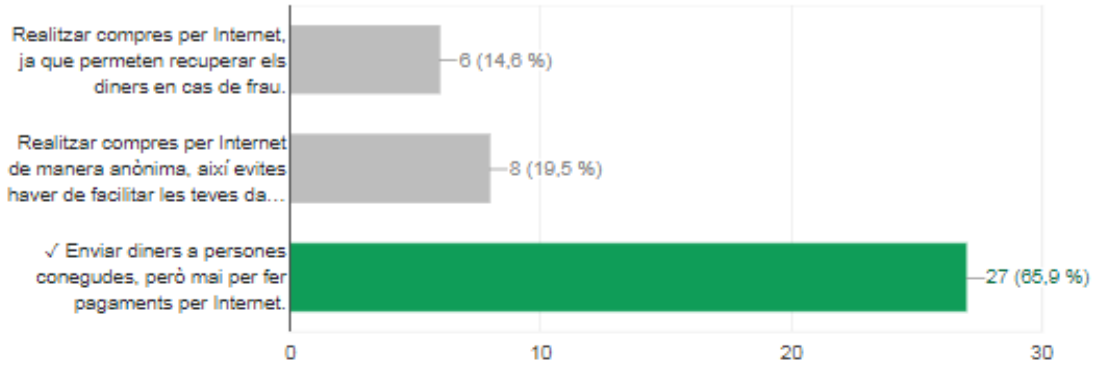
6. Un virus informàtic és capaç d'esborrar les fotos emmagatzemades en un ordinador?

41 de 42 respuestas correctas



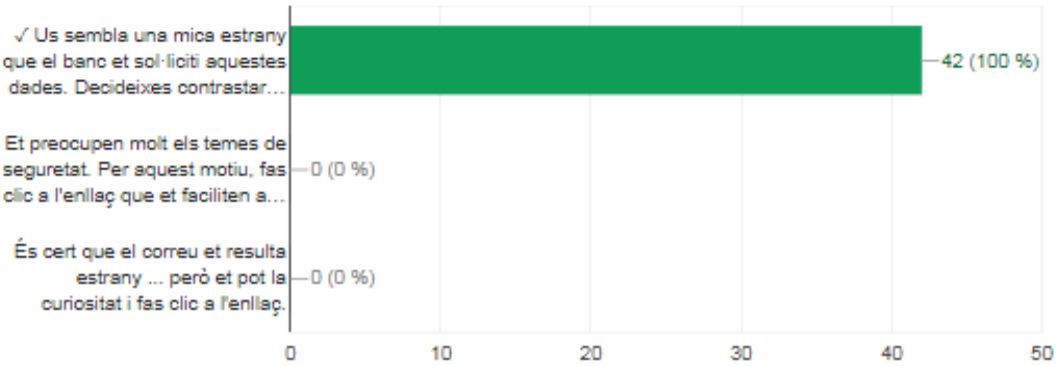
7. L'ús d'empreses d'enviament de diners instantani s'ha d'utilitzar per...

27 de 41 respuestas correctas



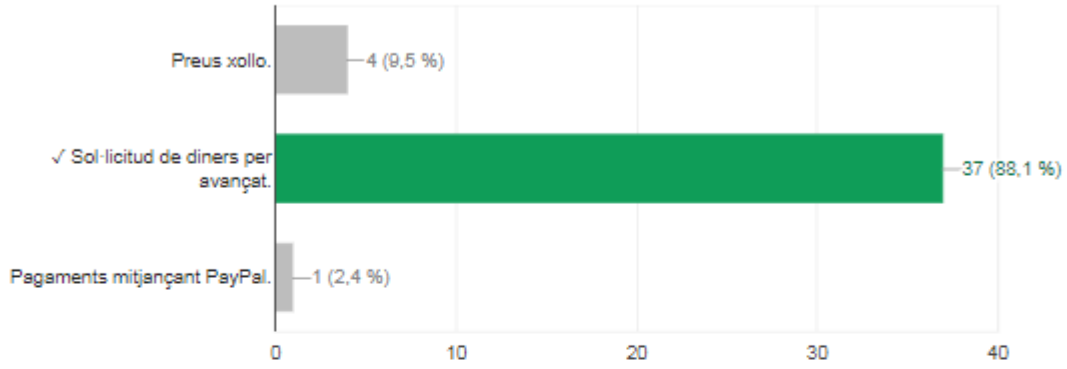
8. Heu rebut un correu del teu banc en el qual et demana confirmar les teves dades personals i bancàries de manera urgent, suposadament per motius de seguretat...

42 de 42 respuestas correctas



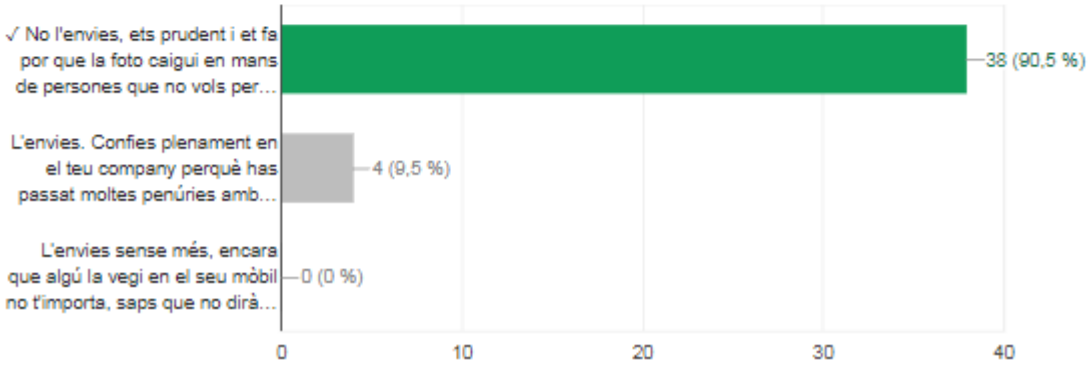
9. Quins indicis han de fer-te sospitar sobre un possible anunci fraudulent publicat en una pàgina web?

37 de 42 respuestas correctas



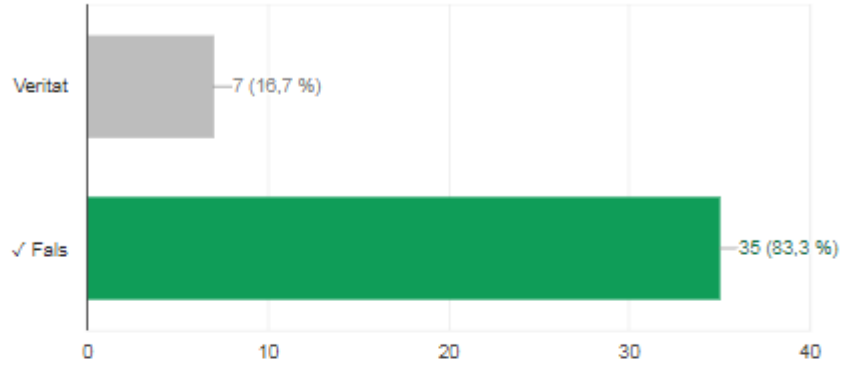
10. Els teus companys t'han demanat que els enviïs per telèfon una foto d'un finat per causes violentes, al qual has assistit per raó del servei...

38 de 42 respuestas correctas



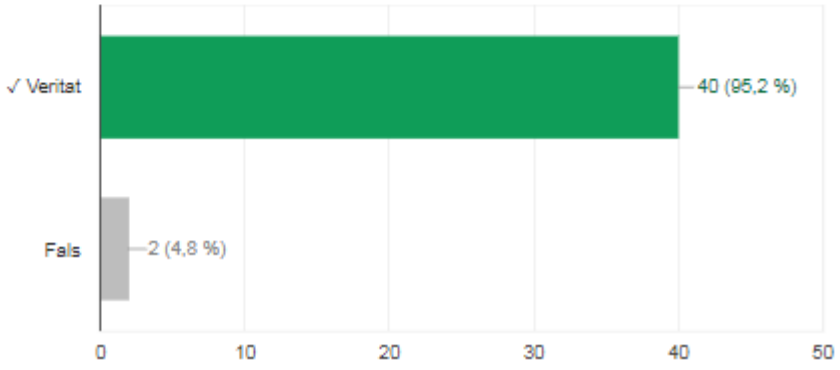
11. És recomanable tenir apuntades les contrasenyes en algun lloc, així si s'obliden per algun motiu, podem consultar-les ràpidament.

35 de 42 respuestas correctas



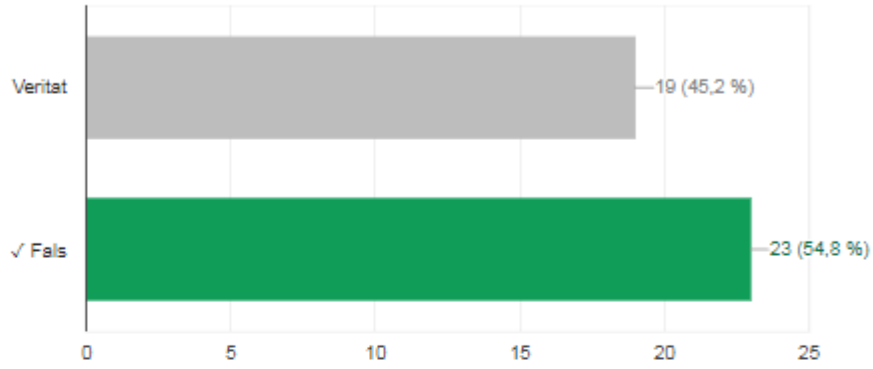
12. Quan em connecto a una xarxa WiFi pública corro el risc que em robin les meves dades emmagatzemades dins el meu dispositiu (portàtil, mòbil, tauleta)

40 de 42 respuestas correctas



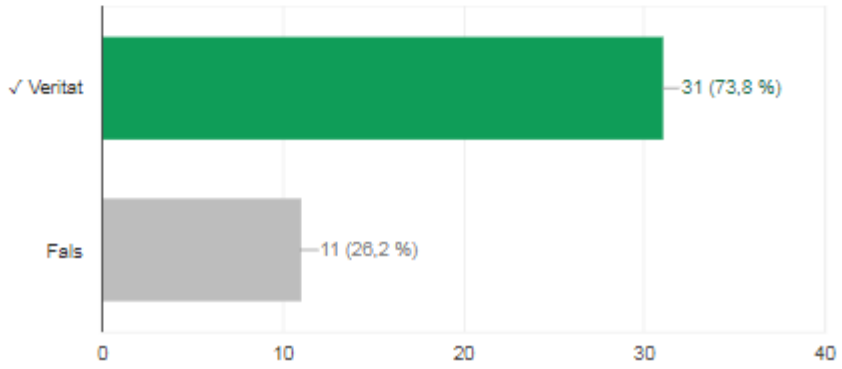
13. Canviar la contrasenya del WiFi de casa periòdicament evita completament que qualsevol intrús es connecti a la meva xarxa.

23 de 42 respuestas correctas



14. Totes les claus d'accés que disposo dins el meu món virtual són d'interès per als delinqüents.

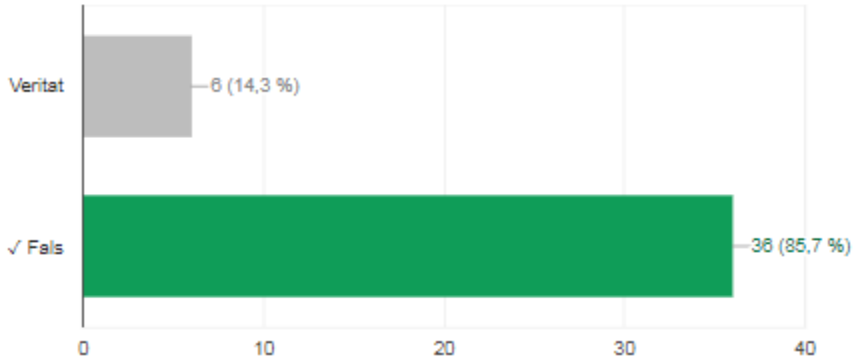
31 de 42 respuestas correctas



Conceptes específics de ciberseguretat dins la PG-ME.

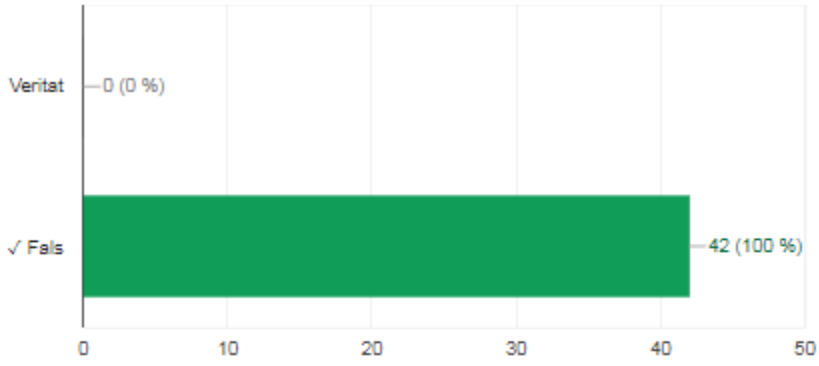
15. Els SIP són un entorn plenament segur, els fitxers de la policia no es poden infectar mai.

36 de 42 respuestas correctas



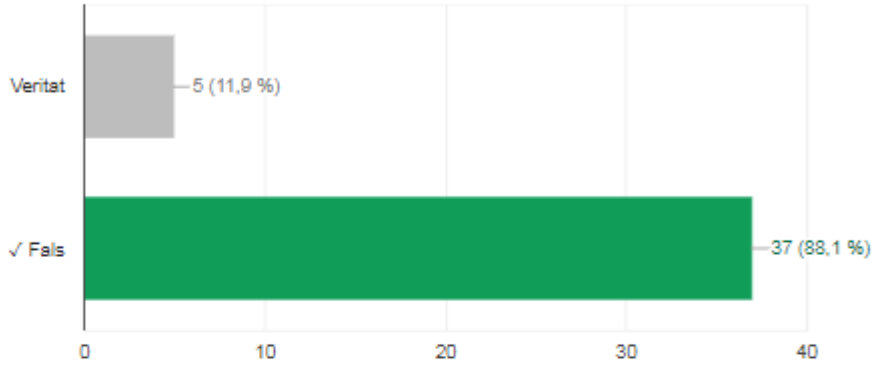
16. Les imatges són dels pocs arxius que, a dia d'avui, es poden obrir amb tranquil·litat ja que no contenen virus.

42 de 42 respuestas correctas



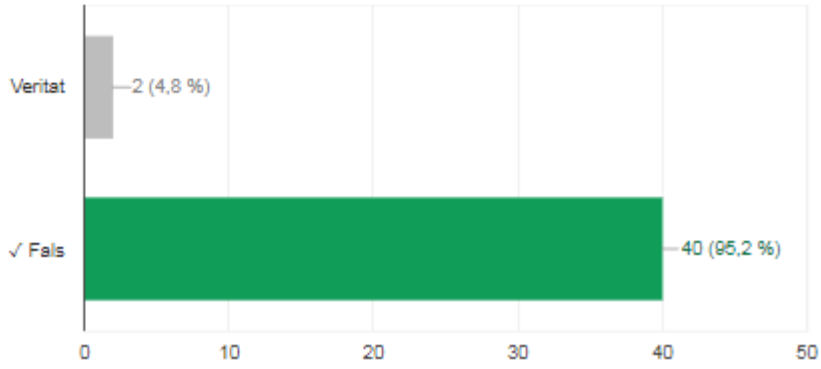
17. Si rebo un correu a la meva adreça corporativa @gencat.cat puc estar ben segur encara que provingui d'un desconegut, ja que haurà passat pels tallafocs i antivirus policials necessaris per tal de detectar-ne codis maliciosos als arxius.

37 de 42 respuestas correctas



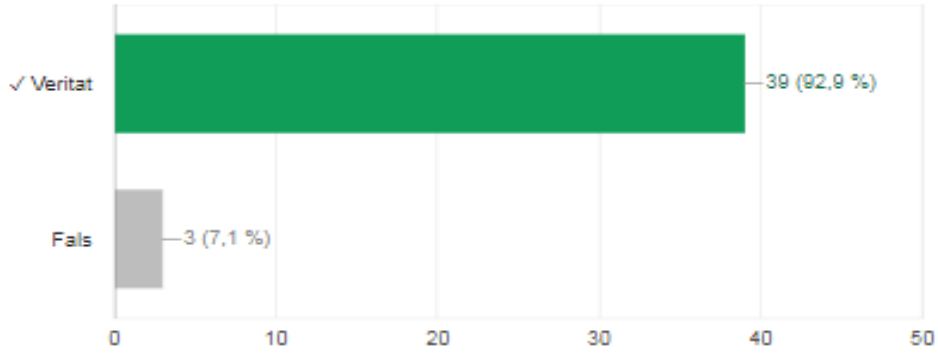
18. No em cal xifrar els arxius amb dades de caràcter personal quan ho copio dins un "llapis de memòria USB", ja que es quedarà a comissaria i no sortiré pas al carrer amb ell.

40 de 42 respuestas correctas



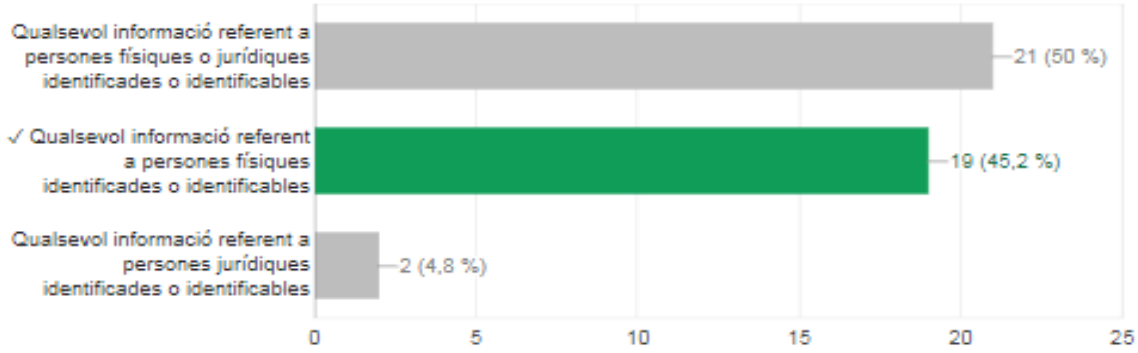
19. Amb només un clic a un enllaç d'un correu puc infectar la meva estació de treball i comprometre la resta que estiguin dins el mateix segment de xarxa.

39 de 42 respuestas correctas



20. Segons la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, entenem com dada de caràcter personal...

19 de 42 respuestas correctas



Moltes gràcies per la vostra col·laboració!

Annex 3. Model PI09

Generalitat de Catalunya
Departament d'Interior
Direcció General de la Policia

Document d'autorització d'accés a les aplicacions i fitxers dels Sistemes d'Informació de la Direcció General de la Policia del Departament d'Interior de la Generalitat

Per mitjà d'aquest document, s'autoritza l'accés a les aplicacions, als fitxers i a les dades automatitzades dels Sistemes d'Informació de la DGP del Departament d'Interior de la Generalitat de Catalunya a:

Nom

Codi usuari / DNI

Destinació

Per accedir i utilitzar les aplicacions i els fitxers de dades automatitzades dels Sistemes d'Informació de la DGP, s'han assignat a les persones autoritzades uns codis d'usuari als quals s'ha definit un nivell d'accés determinat en funció de les seves necessitats i/o responsabilitats en l'ús d'aquests Sistemes. Cada codi d'usuari porta associada una paraula de pas, que ha de ser usada conjuntament amb el codi per a autenticar-se i accedir a les aplicacions.

Al mateix temps, se us informa de les consideracions legals següents:

D'acord amb la LO 15/1999, de 13 de desembre, de protecció de dades de caràcter personal; el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal; el Decret legislatiu 1/1997, refosa en un text únic dels preceptes de determinats textos legals vigents a Catalunya en matèria de funció pública; la Instrucció 1/2012, de 15 de juny, sobre l'ús de les tecnologies de la informació i la comunicació (TIC) per part del personal al servei de l'Administració de la Generalitat de Catalunya, i la Circular 2/2000, de 2 de febrer, sobre els deures i les responsabilitats del personal al servei de l'Administració de la Generalitat de Catalunya que intervingui en qualsevol tractament automatitzat de dades personals, els usuaris que accedeixen a les aplicacions i fitxers automatitzats de dades dels Sistemes d'Informació de la DGP tenen les obligacions següents:

1. **Està prohibit comunicar a una altra persona l'identificador d'usuari i la clau d'accés**. Si l'usuari / la usuària sospita que una altra persona coneix les seves dades d'identificació i accés, ho ha de comunicar immediatament al responsable de seguretat, perquè li assigni una nova clau.

2. L'usuari / La usuària està obligat/da a fer servir el sistema i les seves dades sense incórrer en activitats que puguin ser considerades il·lícites o il·legals, que infringeixin els drets de la DGP o de tercers.

3. Els números d'identificació i les claus d'accés assignats a cada usuari/ària del sistema són personals i intransferibles, i l'usuari / la usuària és l'únic/a responsable de les conseqüències que es puguin derivar del mal ús, la divulgació o la pèrdua.

4. L'usuari / La usuària que deixi de prestar serveis a l'administració a la qual es va donar d'alta té l'obligació de comunicar la seva baixa per desactivar el codi d'usuari corresponent.

5. Estan **expressament prohibides** (entre altres) les activitats següents:

   - Compartir o facilitar l'identificador d'usuari i la clau d'accés a una altra persona física o jurídica, incloent-hi el personal de la mateixa DGP. En cas d'incompliment d'aquesta prohibició, l'usuari / la usuària és l'únic/a responsable dels actes efectuats per la persona física o jurídica que utilitzi d'una manera no autoritzada l'identificador de l'usuari.
   - Intentar desxifrar les claus, els sistemes o els algorismes de xifratge i qualsevol altre element de seguretat que intervingui en els processos telemàtics.
   - Destruir, alterar, inutilitzar o danyar de qualsevol altra manera les dades, els programes o els documents electrònics de la DGP o de tercers (aquests actes poden constituir un delicte de danys, previst en l'article 264.2 del Codi penal).
   - Instal·lar còpies il·legals de qualsevol programa, incloent-hi els estandarditzats.
   - Introduir voluntàriament programes, virus, macros, miniaplicacions (*applets*), controls ActiveX o qualsevol altre dispositiu lògic o seqüència de caràcters que causin, o siguin susceptibles de causar, qualsevol tipus d'alteració en els sistemes informàtics de la DGP o de tercers.
   - Realitzar qualsevol comunicació il·lícita de dades personals, i l'usuari / la usuària és responsable de la bona gestió de les còpies temporals, totals o parcials i en qualsevol tipus de suport, d'aquells fitxers als quals tingui accés, ja sigui dins o fora dels centres de treball (Circular 2/2000, de 2 de febrer, article 6).

UNIVERSITAT DE BARCELONA

- Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament, o qualsevol altre tipus d'obra o material els drets de propietat intel·lectual o industrial dels quals pertanyin a tercers, quan no se'n tingui l'autorització.
- Intentar augmentar el nivell de privilegis d'una persona usuària en el sistema.
- Utilitzar recursos telemàtics de la DGP, incloent-hi la xarxa Internet, per a activitats que no tinguin una relació directa amb el lloc de treball de l'usuari / la usuària.

Confidencialitat de la informació:

1. Està prohibit enviar informació confidencial de la DGP a l'exterior, mitjançant suports materials o a través de qualsevol mitjà de comunicació, incloent-hi la simple visualització o accés.
2. Els / Les usuaris/àries dels sistemes d'informació han de guardar, per un temps indefinit, la màxima reserva i no divulgar ni utilitzar directament, ni a través de terceres persones o empreses, les dades, els documents, les metodologies, les claus, les anàlisis, els programes i la resta d'informació a què tinguin accés durant la seva vinculació o funció a la DGP, tant en suport material com electrònic. Aquesta obligació continua essent vigent després de l'estada o vinculació a la DGP o a l'Administració local.
3. Cap usuari/ària pot posseir, per a usos no propis de la seva responsabilitat, cap material o informació d'ús exclusiu de la DGP, tant ara com en el futur.
4. En el cas que, per motius directament relacionats amb el lloc de treball, l'usuari / la usuària entri en possessió d'informació confidencial en qualsevol tipus de suport, s'entén que aquesta possessió és estrictament temporal, amb obligació de secret i sense que això li irrogui cap dret de possessió, o titularitat o còpia sobre la informació esmentada. Així mateix, l'usuari / la usuària ha de retornar aquests materials immediatament després de la finalització de les tasques que n'han originat l'ús temporal i, en tot cas, immediatament després d'acabar la seva relació amb la DGP o l'Administració local. La utilització continuada de la informació en qualsevol format o suport d'una manera distinta de la esmentada no ha de comportar, en cap cas, una modificació d'aquesta clàusula.
5. L'incompliment d'aquesta obligació pot constituir un delicte de revelació de secrets, previst en els articles 197 i següents i en el capítol IV del títol XIX del Codi penal, així com una infracció de la Llei orgànica 15/1999, de protecció de dades de caràcter personal, i de la normativa estatutària respectiva.
6. La DGP manté un registre de totes les accions que els usuaris fan dins el sistema, tant si són accions autoritzades com si no ho són.

Per part de l'Àrea de Seguretat en Tecnologies de la Informació,

inspector Marc Tortellà i Muns, cap de l'ASTI Lloc i data:

Estic informat/ada de les condicions en què m'han autoritzat a accedir i utilitzar les aplicacions, els fitxers i les dades automatitzades dels Sistemes d'Informació de la Direcció General de la Policia.

Signatura de la persona interessada

Nom i cognoms: DNI / TIP: Data:

Nota: Per tenir accés al SIP heu de retornar aquest document un cop l'hagueu omplert i signat correctament al més aviat possible a l'**Àrea de Seguretat en Tecnologies de la Informació** de la Divisió dels Sistemes d'Informació Policial de la Comissaria General Tècnica de Planificació de la Seguretat.

Annex 4 . Cartell Jornada sobre Ciberseguretat 2015