TRANSCRIPCIÓ EN BRUT

Aquesta transcripció està pendent de verificació i correcció. Pot contenir, doncs, errades de fidelitat i incorreccions lingüístiques i no es pot considerar com una publicació oficial

XV legislatura · cinquè període · sèrie C · número 455

Comissió d'Afers Institucionals

Sessió 26, dijous 5 de febrer de 2026

Presidència de la I. Sra. Judith Toronjo i Nofuentes

Sessió 26 de la CAI

La sessió de la Comissió d'Afers Institucionals (CAI) s'obre a ****. Presideix Judith Toronjo i Nofuentes, acompanyada de la vicepresidenta, Gisela Navarro Fuster, i del secretari, Oriol López Mayolas. Assisteix la Mesa el lletrat Miquel Lluís Palomares Amat.

Hi són presents Alberto Bondesio Martínez, Cristòfol Gimeno Iglesias, Ivana Martínez Valverde i Ferran Pedret i Santos, pel G. P. Socialistes i Units per Avançar; Albert Batet i Canadell, Agustí Colomines i Companys i Glòria Freixa i Vilardell, pel G. P. de Junts; Josep M. Jové Lladó i Marta Vilalta i Torres, pel G. P. d'Esquerra Republicana de Catalunya; Alejandro Fernández Álvarez i Juan Fernández Benítez, pel G. P. del Partit Popular de Catalunya; Joan Garriga Doménech, pel G. P. de VOX en Cataluña; Lluís Mijoler Martínez, pel G. P. Comuns; Dani Cornellà Detrell, pel G. P. de la Candidatura d'Unitat Popular - Defensem la Terra, i Sílvia Orriols Serra, pel G. Mixt[membres comissió].

[Assisteix] a aquesta sessió [assistents].

ORDRE DEL DIA DE LA CONVOCATÒRIA

1. Sol·licitud de compareixença d'una representació del col·lectiu d'alertadors davant la Comissió d'Afers Institucionals perquè informi sobre el contingut que considera que hauria d'incorporar la futura llei d'alertadors (tram. 356-01218/15). Dani Cornellà Detrell, Grup Parlamentari de la Candidatura d'Unitat Popular - Defensem la Terra. Debat i votació de la sol·licitud de compareixença.

2. Sol·licitud de compareixença d'una representació de la secció sindical de la Confederació General del Treball a l'Institut Cartogràfic i Geològic de Catalunya perquè exposi la situació salarial i laboral de l'Institut (tram. 356-01219/15). Dani Cornellà Detrell, Grup Parlamentari de la Candidatura d'Unitat Popular - Defensem la Terra. Debat i votació de la sol·licitud de compareixença.

3. Sol·licitud de compareixença d'una representació de la III Cimera contra les Causes Estructurals de la Corrupció davant la Comissió d'Afers Institucionals perquè es faci un control de seguiment periòdic del compliment dels acords de la Cimera (tram. 356-01242/15). Anna Navarro i Descals, Grup Parlamentari de Junts, Josep M. Jové Lladó, Grup Parlamentari d'Esquerra Republicana de Catalunya. Debat i votació de la sol·licitud de compareixença.

4. Sol·licitud de sessió informativa de la Comissió d'Afers Institucionals amb el conseller de Presidència sobre les accions previstes contra els ajuntaments que permeten els empadronaments fraudulents (tram. 354-00269/15). Hugo Manchón García, Grup Parlamentari del Partit Popular de Catalunya. Debat i votació de la sol·licitud de sessió informativa.

5. Compareixença del director de l'Agència de Ciberseguretat de Catalunya davant la Comissió d'Afers Institucionals per a presentar la memòria del 2023 (tram. 359-00001/15).

6. Compareixença del director de l'Agència de Ciberseguretat de Catalunya davant la Comissió d'Afers Institucionals per a presentar la memòria corresponent al 2023 (tram. 359-00010/15).

7. Compareixença de la directora de l'Agència de Ciberseguretat de Catalunya davant la Comissió d'Afers Institucionals per a presentar la memòria del 2024 (tram. 359-00016/15).

8. Proposta de resolució per a la creació d'un fons de sobirania tecnològica (tram. 250-00850/15). Grup Parlamentari Comuns. Debat i votació de la proposta de resolució i de les esmenes presentades (text presentat: BOPC 345, 171; esmenes: BOPC 394, 23).

La vicepresidenta

Bon dia a tothom, bon dia a tots i totes. Primer, disculpar la presidenta de la comissió que està atenent una altra comissió i m'encarregaré jo mateixa de presidir aquesta sessió.

Comencem l'ordre del dia i els hi tinc un parell de comunicacions. La primera és que fa ja unes sessions vam aprovar aquí a comissió la Ponència de la llei de l'amiant i en aquest sentit hi ha un canvi de relator i els hi passo a comunicar. El senyor Jesús Becerra Ramírez, del Grup Socialista, seria substituït pel senyor David González Chanca per fer aquesta tasca en la llei de l'amiant i com és una comunicació crec que no hem d'emetre vot.

I l'altra qüestió que els hi volia compartir per veure com procedim és que ara farem les votacions de les sol·licituds de compareixença, però després tenim, com ja vostès saben, la directora de l'Agència de Ciberseguretat, però en aquest sentit hi ha dues compareixences, una demanada per la pròpia directora i una altra demanada pel Grup de Junts. Per tant, en el torn, si els hi sembla, al torn d'intervencions –en aquest cas coincideix–, però faríem com sempre, començaríem per Junts, fem tota la ronda i acabar el grup que dona suport al Govern. Els hi sembla bé a tothom? *(Pausa.)* Molt bé, volíem consensuar això.

Ara sí que passo a fer les votacions de l'ordre del dia, de les sol·licituds... *(Forta remor de veus.)* Disculpin, substitucions?

Glòria Freixa i Vilardell

Miri, per Junts per Catalunya la diputada Anna Navarro substitueix el diputat Albert Batet i el diputat Francesc de Dalmases substitueix la Judith Toronjo.

La vicepresidenta

Moltes gràcies. Senyor...

Juan Fernández Benítez

Sí, del Partit Popular el diputat Cristian Escribano substitueix el diputat Alejandro Fernández.

La vicepresidenta

Esquerra?

Marta Vilalta i Torres

Sí, la diputada Mar Besses substitueix el diputat Josep Maria Jové.

Gràcies.

La vicepresidenta

La CUP?

Dani Cornellà Detrell

No és per anunciar substitució, sinó que em quedo ara a votar, però que marxo perquè tinc la Comissió d'Interior i Territori conjunta.

La vicepresidenta

Moltes gràcies, diputat. PSC?

Ivana Martínez Valverde

La diputada Andrea Zapata substitueix el diputat Ferran Pedret.

La vicepresidenta

Moltes gràcies. I Comuns no?

Núria Lozano Montoya

Sí, Núria Lozano en substitució del diputat Lluís Mijoler.

Gràcies.

La vicepresidenta

Moltes gràcies. Ara sí que passem a la votació de les sol·licituds. Com n'hi ha molt poquetes, els sembla que fem d'una en una o volem fer algun paquet? *(Pausa.)* D'una en una?

Sol·licitud de compareixença d'una representació del col·lectiu d'alertadors perquè informi sobre el contingut que considera que hauria d'incorporar la futura llei d'alertadors

356-01218/15

Vinga, començaríem pel punt número 1, que és la sol·licitud de compareixença d'una representació del col·lectiu d'alertadors davant, evidentment, d'aquesta comissió.

Vots a favor?

Per unanimitat.

Moltes gràcies.

Sol·licitud de compareixença d'una representació de la secció sindical de la Confederació General del Treball a l'Institut Cartogràfic i Geològic de Catalunya perquè exposi la situació salarial i laboral de l'Institut

356-01219/15

Passem al punt número 2 que, en aquest cas és una sol·licitud de compareixença d'una representació de la secció sindical de la Confederació General de Treball a l'Institut Cartogràfic i Geològic de Catalunya.

Vots a favor?

Gràcies.

Junts, bé, Junts, PSC, Esquerra Republicana i la CUP.

Vots en contra? *(Forta remor de veus.)* Ai, perdó. No, perdó, perdoni, diputada. És que la tinc alineada amb el senyor Cristòfol que és una mica gran i no la veia. *(La vicepresidenta riu.)*

D'acord, repetim si els hi sembla.

Vots a favor de la compareixença?

PSC, Comuns, Esquerra Republicana, CUP i Junts.

Vots en contra?.

El partit de VOX.

I abstencions?

Partit Popular.

Moltes gràcies.

Sol·licitud de compareixença d'una representació de la III Cimera contra les Causes Estructurals de la Corrupció perquè es faci un control de seguiment periòdic del compliment dels acords de la Cimera

356-01242/15

Passem al punt número 3, que en aquest cas és la sol·licitud de compareixença d'una representació de la tercera cimera contra les causes estructurals de la corrupció davant de la Comissió d'Afers Institucionals.

Vots a favor de la sol·licitud?

PSC, Comuns, Esquerra Republicana, la CUP, ah, PP i Junts. *(Remor de veus.)* D'acord, doncs abaixin les mans. *(La vicepresidenta riu.)*

Vots a favor?

PSC, Comuns, Esquerra Republicana, la CUP i el Grup de Junts.

Vots en contra?

Abstencions?

Partit Popular i VOX.

Molt bé, moltes gràcies.

Sol·licitud de sessió informativa amb el conseller de Presidència sobre les accions previstes contra els ajuntaments que permeten els empadronaments fraudulents

354-00269/15

I passem a la quarta, que és la sol·licitud de sessió informativa davant de la Comissió d'Afers Institucionals del conseller de la presidència sobre les accions previstes contra els ajuntaments que permeten els empadronaments fraudulents.

Vots a favor de la proposta?

Junts, PP i VOX.

VOX, ai, VOX, vots en contra?

PSC, Esquerra Republicana, la CUP i Comuns.

Per tant, la rebutjaríem.

D'acord.

I ara sí, passem a... Moltes gràcies, passem a demanar els compareixents si estan... Cristina, mirem si estan?

(Pausa llarga.)

Compareixences

359-00001/15, 359-00010/15 i 359-00016/15

Bé, doncs, com dèiem, donem en aquest cas la benvinguda a la directora de l'Agència de Ciberseguretat de Catalunya, la senyora Laura Caballero. En aquest sentit, avui tenim diferents compareixences que substanciarem en el mateix torn. Pel que fa a la presentació de les memòries tant del 23 com del 24, per tant, vostè té la paraula, sigui molt benvinguda vostè i els acompanyants. Té un torn de vint minuts o vint-i-cinc minuts, estem..., perquè pugui explicar. Després farem un torn dels grups i podrà també respondre totes les qüestions que facin falta. Per tant, endavant i benvinguda.

(L'exposició va acompanyada d'una presentació de xarts, que es pot consultar a l'Arxiu del Parlament.)

Laura Caballero Nadales (directora de l'Agència de Ciberseguretat de Catalunya)

Molt bé, gràcies, presidenta. Diputats i diputades, bon dia, primer de tot. Gràcies per atendre la meva compareixença davant la Comissió d'Afers Institucionals. Avui em toca presentar les memòries anuals 2023-2024. Tot i que és la primera vegada que comparec per presentar l'activitat de l'Agència, no és la primera vegada que sóc aquí, que em dirigeixo a vostès. Recordaran que vaig tenir l'oportunitat de presentar-me davant de tots vostès fa poc més d'un any, concretament el 16 de gener del 2025, i ho vaig fer en virtut de l'article 5.2 de la Llei de l'Agència, que estableix l'obligació que la proposta de la persona designada per la direcció comparegui abans de la seva contractació efectiva.

Així, doncs, tot i que podríem dir que no soc nova, sí que és la primera vegada que assisteixo a aquesta Comissió d'Afers Institucionals per presentar les memòries de l'Agència. En aquest sentit, m'agradaria esclarir-los, com ja segurament hauran deduït, que encara no era la directora de l'Agència de Ciberseguretat a Catalunya en els exercicis que avui presentaré, però amb tot, l'Administració té una continuïtat que celebro i que reivindico i que és la que em permet avui exposar-los l'activitat dels anys 2023-2024.

Abans d'endinsar-me en les línies de treball i les actuacions de les memòries que avui presento, permetin-me fer una breu referència al què som l'Agència i l'encàrrec que tenim l'Agència de Ciberseguretat a Catalunya. Es tracta d'un servei públic essencial, encarregat de governar la ciberseguretat del país i treballar diàriament en la prevenció de les estafes i la protecció d'una internet molt més segura. D'aquest mandat se'n deriva, en primer lloc, la responsabilitat de conscienciar i formar la ciutadania, però no només això, les empreses i les institucions públiques de Catalunya.

I en segon lloc, prestem directament serveis de ciberseguretat a totes les institucions públiques, proporcionant acompanyament, supervisió en el seu procés d'adaptació als requisits de seguretat vigents, per tal d'assegurar la confidencialitat, la integritat, la traçabilitat, l'autenticitat de les dades dels nostres ciutadans i ciutadanes i de les pròpies administracions públiques. Així mateix, com a Agència tenim un altre rol, que és el de la resposta a incidents, el que anomenem el Catalònia-Cert. Nosaltres prestem serveis reactius, és a dir, que responem a una amenaça o a un incident de ciberseguretat, així com a serveis de gestió i de coordinació que tenen per objectiu millorar els processos de treball tan externs com interns.

I finalment, tenim un altre rol, que és recent, que és el que l'Agència està reconeguda com un òrgan d'auditoria tècnica. I això què vol dir? Aquest fet ens capacita per realitzar auditories de conformitat amb l'Esquema Nacional de Seguretat per l'àmbit de l'Administració pública de la Generalitat de Catalunya, del seu sector públic, també i de totes aquelles entitats que estan sota l'àmbit competencial de l'Agència, com poden ser, per exemple, hospitals o universitats entre d'altres. En conseqüència, l'Agència executa les polítiques públiques en matèria de

ciberseguretat i desenvolupa l'estratègia pròpia de ciberseguretat de l'àmbit de la Generalitat de Catalunya. Dit d'una altra manera, som l'organisme responsable de governar la ciberseguretat a Catalunya.

Entro ara, si els sembla, en la matèria específica que motiva la meva compareixença d'avui i és el balanç de l'Agència corresponent als exercicis 2023-2024. Començaré amb una radiografia global de quines van ser les principals amenaces en l'àmbit de la ciberseguretat a escala internacional. I és que l'any 2023 va ser un any d'una gran rivalitat geopolítica, una rivalitat que es va traslladar amb molta força al ciberespai. Recordem, per exemple, el conflicte bèl·lic, la continuïtat del conflicte bèl·lic entre Ucraïna i Rússia. Això va propiciar una sèrie d'atacs molt sofisticats i, per exemple, atacs de denegació de servei, atacs de DDOS, que volien desestabilitzar els països. Però és que no només això, també van haver-hi moltes campanyes de desinformació associades a aquests conflictes bèl·lics.

Un patró molt similar es va produir també a les tensions del Pròxim Orient, això a nivell d'escala internacional. I en aquest context social, la tendència dels ciberdelinqüents va ser fixar un objectiu, que eren els operadors assumint extremament bàsics, era el seu objectiu, amb una especial incidència, amb l'atac que s'anomena de ransomware, un segrest de dades que fa inútil una organització. L'objectiu d'aquests cibercriminals, el que tenen és, amb aquest segrest de les dades, extorsionen directament aquestes organitzacions. Malauradament, vam tenir un cas molt sonat, que va ser el de l'Hospital Clínic a Catalunya, en el 2023, i va fer posar al centre els esforços que havíem de realitzar en aquest sentit.

Va ser un impacte molt important, es van anul·lar cent cinquanta intervencions, més de dues mil visites, i no només a l'Hospital Clínic, va haver-hi també un cas en aquell any, que va ser a l'Hospital Moïsès Broggi. Aleshores, el que ens va demostrar això és que l'Agència havíem de donar resposta. I com es va donar resposta en aquell moment? Doncs es va presentar un model de ciberseguretat específic pel sector sanitari. Aquí l'objectiu era protegir aquest sector i aquest àmbit tan crític com és l'àmbit sanitari, a través de la protecció i la prestació de serveis de l'Agència, prestació de serveis de ciberseguretat per part de l'Agència, dintre d'un model integral de protecció. Els ficàvem, d'alguna manera, en el nostre paraigües.

I és que, parlant de ransomware, que precisament va ser el tipus d'atac que es va utilitzar a l'Hospital Clínic per generar aquest impacte, no és casual que en el 2024 aquest tipus d'atac tingués records històrics. Això vol dir que, a nivell mundial, el tipus d'atac ransomware va arribar a xifres històriques, fins als 5.710 incidents. Això volia dir un 11,6 per cent més que l'any anterior. Aleshores, això seguia reforçant, aquesta realitat ens va reafirmar la necessitat de seguir treballant en línia i en la protecció d'aquestes entitats i, especialment, dels sectors més vulnerables.

A tot això, també, en el 2023-2024, comença a aparèixer la intel·ligència artificial generativa. És cert que va ser a l'inici, ara s'està consolidant com un vector d'amenaça clar, però sí que és cert que en el 2023-2024 es van començar a veure els primers atacs que utilitzaven la intel·ligència artificial generativa per fer més sofisticades, per exemple, les ciberestafes. O, per exemple, es van donar alguns primers casos d'atacs dels tipus hipertrucatge o els anomenats *deepfakes*, que això amb veu, amb imatges, doncs podran generar com si fos un vídeo en temps real i poden suplantar la identitat de les persones. Llavors, en el 2023-2024 comencem a trobar aquests primers casos.

Pel que fa a altres tipus d'atacs que ens vam trobar en aquella època, a banda del que comentàvem del ransomware, a banda de la irrupció de la intel·ligència artificial, també va haver-hi un creixement notable dels robatoris massius de dades personals, especialment amb finalitats delictives. Vam veure que això era un negoci molt lucratiu als ciberdelinqüents. I aquests robatoris es feien a través de dues tècniques, tècniques d'enginyeria social, que era enganyar les persones, o bé tècniques infectant directament dispositius, amb un tipus de programari maliciós que es coneix com a *infostealer*.

Això el que buscaven era robar usuaris i contrasenyes. Després d'aquests usuaris, contrasenyes i la resta de dades personals, què es feia? Doncs es ven al mercat negre, a la anomenada *dark web*, i d'aquí després se'n deriven, en aquest cicle virtuós de la ciberestafa, se'n deriven intents d'estafes a través del correu, de trucades, SMS, etcètera. Per tant, els delinqüents van veure aquí un camí clar en el fet delictiu i que, a més, era molt lucratiu. Per tant, amb tota aquesta foto, aquests anys el que es va posar de manifest és que les amenaces eren cada cop més

sofisticades i que, a més, eren més persistents. I no només afectaven directament les organitzacions, sinó que també afectaven tota la cadena de subministrament i per tant els proveïdors que donaven servei en aquestes organitzacions.

Pel que fa a les vulnerabilitats, que no als incidents, sinó vulnerabilitats com a tal, cal destacar que durant aquells anys el nostre centre d'operacions de ciberseguretat va identificar set vulnerabilitats *zero-day*, són aquelles que encara no hi ha una protecció disponible en el mercat per poder protegir-les. El nostre centre d'operacions de seguretat va identificar aquestes vulnerabilitats amb suficient temps com per assegurar que no hi havia un impacte directe sobre els nostres actius i els nostres sistemes d'informació. I això és molt important, aquesta part de prevenció, aquesta part de detecció, perquè així evitem que després es produeixin incidents com els que s'estan mencionant. Per tant, seguint amb les dades, crec que és important seguir amb les dades perquè representa una miqueta la dimensió del que estem parlant i perquè també representa l'activitat de la nostra pròpia agència, i aquí especialment parlaré del 2023 i del 2024.

Aleshores, durant el 2023 l'Agència va gestionar fins a 2.760 incidents de ciberseguretat. ¿Es tracta d'una xifra elevada? Sí, en la línia amb la tendència dels últims anys, que és incremental. Però és que en el 2024 aquesta dada va augmentar fins a un vint-i-sis per cent més, fins als 3.372 incidents. Cal precisar que aquests incidents alts, aquestes xifres tan elevades són aquelles les quals estan dintre del perímetre de l'Agència, és a dir, que nosaltres directament gestionem. Però és que paral·lelament nosaltres com a agència i en el nostre perímetre de protecció rebem moltíssims intents d'atacs. Estem parlant de milions i milions d'atacs. I ara concretarem aquests milions d'atacs. I és que 5.000 milions d'atacs en el 2023 es van rebre dintre del perímetre de protecció, i 6.900 milions d'atacs es van rebre en el 2024. Aleshores, aquests són intents.

En aquest sentit, els sistemes de protecció van funcionar i, per tant, vam poder bloquejar tots aquests intents i només ens vam quedar amb una xifra residual del que això després va esdevenir un incident de ciberseguretat. Ja us aviso, a vostès, que d'alguna manera en el proper any, quan hagi de presentar les memòries o quan vostès ho considerin, que la xifra en el 2025 és més elevada. És a dir, això, la

quantitat de ciberatacs, que també és una tendència global, no és només una tendència dintre de l'àmbit de l'Administració pública de la Generalitat, va in crescendo i cada any superem, i són xifres històriques les que ens estem trobant.

Així mateix, durant el 2023-2024, en podem destacar una tipologia d'atacs, que són els de la denegació de servei. Per què? Perquè aquests tipus d'atacs el que busquen és deixar inoperativa una organització. Aquí a Catalunya en vam rebre, en el 2023, fins a trenta-sis atacs de denegació de servei. Això busquen fer inoperativa directament una organització enviant peticions massives en els sistemes d'informació de les organitzacions. En canvi, la bona notícia és que en el 2024, de trenta-sis atacs de denegació de servei, es van passar a trenta-tres atacs de denegació de servei. Per tant, sí que es va reduir.

En tot aquest còmput de xifres, ens quedem amb un concepte, i és que, malgrat que la tendència en ciberatacs continua a l'alça, i ho veurem a les properes memòries, la detecció i l'estabilització dels bloquejos van ser cada vegada més robusta, fet que ens reafirma la importància i la utilitat dels sistemes de prevenció de l'Agència de Ciberseguretat.

Un cop parlat dels incidents, ara entraré a la part d'àmbits d'actuació de la pròpia agència. I és que, com ja he posat de relleu, alguns dels sectors, com el sanitari, van ser els principals víctimes d'incidents de seguretat digital en el 2023. A nivell mediàtic, ja ho he mencionat, està destacat l'incident de l'Hospital Clínic, i com a conseqüència va quedar clar que la ciberseguretat havia de situar-se al centre dels nostres esforços. En aquest sentit, el Govern i l'Agència van aprovar dotar-se dels recursos necessaris per accelerar i impulsar més accions en tres eixos estratègics. El sector sanitari, el món local i l'àmbit universitari, incloent els centres de recerca i educatius.

Si al 2023, els he comentat que el sector sanitari va ser la principal víctima de ciberincidents, l'any següent, en canvi, l'activitat delictiva a la xarxa amb més impacte va ser el sector universitari. O sigui, 2023, el sector sanitari; 2024, el sector universitari amb 1.790 incidents, mentre que l'àmbit hospitalari i la Generalitat van patir 676 i 643 incidents, respectivament. Pel que fa en concret a l'àmbit de la Generalitat, comentar que el 2024 va haver-hi un canvi de tendència, amb un

desplaçament de l'activitat ciberdelictiva cap al robatori de credencials, sobrepassant inclús les fronteres de l'àmbit sanitari.

Ara m'endinsaré en el que és, si em permeten, en el que és els projectes més destacats del període que avui presento. I en aquest sentit, mencionar que, sens dubte, aquests projectes, un d'ells va ser el desplegament del model de protecció en ciberseguretat als seixanta-vuit hospitals del Siscat. Va ser un esforç de país que va permetre establir un marc homogeni de prevenció, de protecció i de resposta en un dels àmbits més crítics fins aleshores, que és el de salut. Paral·lelament, es van començar a treballar una sèrie de proves pilots, per exemple, a les universitats, en el model integral de ciberseguretat pels àmbits, que buscava d'alguna manera normalitzar i automatitzar el desplegament del model que els estic mencionant.

També es van començar a definir algunes iniciatives sectorials, com l'ISAC Salut, que permetien i que busquen potenciar la col·laboració i la coordinació en un àmbit tan sensible com el sanitari. I, a més a més, en aquest 2023 se'ns van assignar uns fons europeus, uns importants fons europeus, dintre del programa de RETECH, i que està en el marc del Pla de Recuperació, Transformació i Resiliència, i durant aquells anys es va començar a fer és definir els àmbits d'actuació a què es destinarien aquells fons europeus. I aquí m'agrada recalcar que actualment, des del 2025, hem aterrat tots aquests àmbits d'actuació, tenim fins a vint-i-set iniciatives, de fet, és la major inversió i execució en projectes de ciberseguretat que mai s'ha fet en aquest país, i que, per tant, està centrat bàsicament en protegir el que més importa.

D'una banda, tots els serveis essencials més crítics, des de la part d'Administració, però també a l'àmbit de salut. No només això, també incideix en la part de talent, que crec que també és una cosa i un repte que tenim al davant. També posa una mirada en les futures amenaces emergents, perquè ens hem de preparar pel que ve, per exemple, amb el tema de la computació quàntica, i dona suport a les pimes, especialment dintre del sector TIC, per ser més competitives, especialment oferint-los serveis d'adequació i de certificació a l'Esquema Nacional de Ciberseguretat.

I tornem al 2024. Si el 2023 he explicat aquests projectes destacables, el 2024 es va impulsar el primer programa de *bug bounty* governamental, una iniciativa que va

permetre detectar vulnerabilitats de forma proactiva a través del que se'n diu *hacking* ètic. A més, cal destacar la creació d'un pavelló de l'Agència al Barcelona Cybersecurity Congress, que va acollir setze empreses i entitats catalanes, acció que va esdevenir una palanca per accelerar la innovació, el talent, l'activitat econòmica, i que també va contribuir a la política d'internacionalització del sector de la ciberseguretat de Catalunya.

És pertinent assenyalar que des de l'Agència de Ciberseguretat de Catalunya s'impulsa anualment aquest congrés, de manera conjunta amb Fira Barcelona, per situar Catalunya com a pol d'atracció i de talent en l'àmbit de la ciberseguretat, i que enguany celebrarem el mes de novembre, coincidint amb l'Smart City Expo World Congress.

Per últim, arran de l'aprovació del nou Esquema Nacional de Seguretat de l'any 2022, durant el 2023 l'Agència va ser reconeguda com a òrgan d'auditoria tècnica per part del Centro Criptológico Nacional, i aquest reconeixement habilita l'Agència per realitzar auditories de conformitat amb l'Esquema Nacional de Seguretat a l'Administració pública, al sector públic i a la resta d'entitats incloses dintre el seu àmbit competencial, així com per emetre els corresponents certificats de conformitat.

Per tal de vetllar per aquest impuls de l'Esquema Nacional de Seguretat, l'Agència va reforçar el seu model de seguretat incorporant com a última milla l'auditoria de certificació. I durant el 2024 també aquest rol de l'Agència que es va consolidar amb el reconeixement definitiu després de superar el procés d'auditoria corresponent, que va confirmar que l'Agència complia amb tots els requeriments i requisits establerts.

Ara passem a la banda d'innovació i tecnologia, i és que, pel que fa a innovació i tecnologia, l'any 2023 va representar un període de fonamentació i alineament metodològic a l'Agència. Es va consolidar la unitat de ciència i analítica de dades creada per gestionar tot el cicle de vida de les dades de ciberseguretat i explotables. Aquesta unitat té la funció de responsabilitzar-se del tractament integral de les dades, és a dir, fent-ne recuperació, emmagatzematge, processament, integració i transformació i anàlisis. Així mateix, en aquest context, es van començar a treballar

en casos d'ús d'intel·ligència artificial i *machine learning* amb l'objectiu de millorar les capacitats analítiques i operatives de l'Agència.

Pel que fa al 2024 vam promoure una sèrie de projectes d'innovació, fins a tretze iniciatives, de les quals algunes es van treballar, es volien treballar amb empreses privades, d'altres amb entitats públiques, d'altres a través de consorci, mentre que la resta eren de caràcter intern. Aquí, destacar-ne, el projecte europeu SAFE, centrat a desenvolupar solucions europees basades en intel·ligència artificial per a xocs, per tal de reforçar la detecció i resposta de les ciberamenaces. Com a fita, aleshores, l'Agència va poder consolidar la seva participació a través d'un consorci publicoprivat europeu, amb la finalitat de reforçar el seu laboratori d'innovació i de dades.

(Pausa.) Disculpin. A nivell de formació, donat que el nostre sector està en constant evolució, i tal com he pogut anar desglossant al llarg d'aquesta compareixença, i també ho vaig exposar durant la meva presentació com a directora l'any passat, el talent i la formació de nous professionals i dels propis empleats de la Generalitat és i continua sent un objectiu cabdal. L'any 2023 vam formar un total de 5.467 empleats públics i 6.459 professionals sanitaris amb cursos bàsics de ciberseguretat, mentre que el volum del 2024, a nivell de participació, va superar àmpliament el de l'exercici anterior.

Durant aquest període, l'Agència va dinamitzar diverses formacions, algunes orientades, com he esmentat, a la formació bàsica, però també en formació especialitzada, i també formacions orientades als alts càrrecs i personal directiu de la Generalitat. En el marc del sistema sanitari integral vam formar 15.828 professionals i en l'àmbit educatiu els docents van tenir l'accés a l'itinerari de ciberseguretat i al curs complet de ciberseguretat a les aules. I amb el centre, per exemple, un cas molt concret, amb el Centre de Recursos Pedagògics de Badalona, es va desenvolupar un contingut específic pels caps d'estudi de centres d'educació primària.

L'interès de la ciutadania per entendre i aprendre sobre aspectes relacionats amb la ciberseguretat també es va evidenciar amb el nombre de visites a la web d'Internet Segura, que en va rebre només en un any 337.435. I és que el 2024 la mateixa web de l'Agència va incrementar un vint per cent les visites i les seves visualitzacions

registrades, reflectint un interès creixent i consolidant la projecció pública de les accions de formació i conscienciació desenvolupades al llarg de l'any.

Per últim, l'any 2024 també va destacar de l'enfocament de l'Agència en el pla estratègic per dones en ciberseguretat, elaborant l'informe *Dones i ciberseguretat a Catalunya* En aquest document es va destacar que el percentatge de dones en posicions directives era del 24,7 per cent, i era proporcional, per tant, a la presència de dones en el sector, 24,6 per cent. Com entendreu i entendran, doncs encara estem lluny de la paritat.

En aquesta línia es van impulsar accions de generació de coneixement i disseminació d'informació sectorial en perspectiva de gènere, com l'establiment d'aliances estratègiques amb actors claus de l'ecosistema, trobades per explorar col·laboracions per apropar el talent femení als espais de debat, la participació per desena vegada als Premis Dona TIC i el foment de les vocacions entre les més joves participant al Saló de l'Ensenyament i fomentant visites a la pròpia Agència amb alumnes, institucions, a màsters, etcètera.

Ara entraré en l'àmbit del pressupost. En l'àmbit econòmic, l'Agència va implementar un pressupost de 30,2 milions d'euros l'any 2023 i es va consolidar l'aposta estratègica per la captació de fons europeus en l'àmbit de la ciberseguretat. Si bé aquests fons no van repercutir directament en l'exercici 2023, sí que, com he comentat abans, se'ns va adjudicar durant aquell any el projecte de RETECH per un import de 20 milions d'euros, que enguany estem executant, dels quals 5 milions corresponen al cofinançament, i també el projecte de Corporate Digital Responsibility per un import de dos-cents mil euros i quaranta mil dels quals també corresponen al cofinançament.

L'exercici 2023 també va reflectir la consolidació i l'increment d'actuacions per desenvolupar activitat específica en diversos àmbits. Destaquen l'àmbit de salut, amb 5,7 milions d'euros, el d'universitats, amb sis-cents mil euros i el de la Secretaria de Telecomunicacions i Transformació Digital, amb 4,5 milions d'euros. Durant el 2024 es va aprovar per acord de govern el contracte programa de ciberseguretat per un període de quatre anys, del 2024 al 2027, amb un pressupost de 67 milions d'euros a raó de 16,8 milions d'euros anuals. I es va consolidar l'instrument previst

en el contracte programa que va permetre gestionar sol·licituds d'actuació per 5 milions d'euros. Finalment cal destacar l'assignació de projectes específics en l'àmbit de salut, com he comentat, a raó de 6,2 milions d'euros.

El balanç pressupostari del 2024 va permetre consolidar l'activitat de l'Agència, i tot i que no va haver-hi un increment significatiu respecte l'any anterior, va haver-hi un increment en l'augment de la despesa corrent de fins a 35,7 milions d'euros, que va fer possible enfortir la capacitat operativa experta en ciberseguretat afrontant, com he explicat, els reptes creixents i establint un model de ciberseguretat que va fer possible l'estabilitat de les accions. Per tant, la solidesa i l'evolució dels serveis van permetre un nivell de resposta especialitzada i adaptada a sectors com el de la salut i les universitats.

Per anar finalitzant, no podem obviar que en els exercicis 2023-2024 i gràcies a l'esforç de tot l'equip de l'Agència es van aconseguir fites rellevants. Com ja he destacat, l'Agència va ser reconeguda com a òrgan d'auditoria tècnica, fet que va suposar poder fer les auditories de certificació, de conformitat amb l'Esquema Nacional de Ciberseguretat i consolidar les primeres auditories de certificació a l'Administració local.

Del 2024, també cal remarcar que va ser l'any que va dotar l'Agència de capacitat i de consolidació de processos per poder desenvolupar la seva activitat com a òrgan auditor i que es va treballar en l'actualització de la metodologia del marc de ciberseguretat per a la protecció de dades, el conegut com a MCPD. Val a dir que també es va avançar amb determinació implementant el model de protecció sanitària als seixanta-vuit hospitals del Siscat, i que vam ser premiats amb el Digital Skills Awards 2024 pel nostre programa d'Internet segura.

Per acabar, vull agrair el temps que la cambra m'ha cedit avui, així com l'atenció que tots vostès han prestat en aquesta presentació de les memòries 2023-2024. És pertinent assenyalar que ja estem treballant amb la memòria 2025 i que és la primera memòria que s'elabora íntegrament sota la meva direcció i que, si tot evoluciona segons el previst, remetrem al Parlament de Catalunya de cara al mes de març.

Per descomptat, resto a la seva plena disposició per fer la compareixença de la nova memòria de 2025 dins del termini que sigui més òptim per vostès.

Moltíssimes gràcies.

La vicepresidenta

Moltíssimes gràcies, directora. Ara és el torn dels grups i per començar aquest torn té la paraula el Grup de Junts, la diputada Anna Navarro.

Anna Navarro i Descals

Molt bé, moltes gràcies i que bé que tornis a estar aquí i per tota la feina que esteu fent. Des de Junts per Catalunya entenem molt bé la necessitat de la vostra agència. Has explicat moltíssimes coses. A mi m'agradaria parlar, et diré els títols i després endinsar una mica en tot això. Jo he vist els números de l'any 2025 i l'escalada no és el doble, és molt més exponencial. Crec que parlarem d'algun programa de transparència del ciutadà, hem vist la Hisenda, la Borsa d'Habitatge, Logaritme, Endesa. Algun programa de transparència, perquè si jo soc un ciutadà puc entendre què ha passat amb Hisenda si tenen les meves dades?

El segon tema que m'agradaria parlar són els pressupostos perquè el salt és tan bèstia, és tan significant que podríem parlar de la capacitat o de l'ambició de país ara que de moment no tenim pressupostos? També ens agradaria molt entendre la coordinació amb Europa, quina arquitectura està proposant Europa i si nosaltres la seguim o no i si hi ha gaps en això.

Molt important la protecció del món local. Estava mirant, hi havia uns anuncis de diaris que el noranta-nou per cent dels municipis ni tenen la coordinació amb un SOC I, evidentment, l'escalada dels *deepfakes* i, evidentment que estem parlant de Catalunya, però com has començat, que tota la desinformació a la IA ve de tots els sistemes. Si poguéssim entendre una mica la coordinació, perquè està tan fragmentat, ve de tants llocs diferents...

Una altra pregunta seria la coordinació amb l'ATC, perquè tenim les escalades d'amenaces per exemple a Hisenda, però com que nosaltres ara estem parlant de Catalunya, si l'Agència de Seguretat de Catalunya té algun programa de cooperació amb l'ATC.

Llavors, la capacitat real davant de l'escalada d'amenaces. L'increment de cada any és que ja no és el doble ni el triple, és molt i molt gran. Llavors, les polítiques actuals,

el vostre equip, la capacitat d'agafar gent..., jo em recordo que vam coincidir, que em vàreu convidar en un acte que estaves buscant noies, no?, que has parlat que hi havia com uns cinc mil, que esteu entrenant molta gent. Quina és la capacitat actual de l'Agència i si esteu agafant més gent al ritme de l'escalada, crec que seria molt important entendre els recursos humans i aquesta capacitat operativa.

Llavors, com us organitzeu?, depèn del que recomana la Unió Europea i del que està passant en el món? Seria tot això, si poguéssim parlar una mica de tot això.

Gràcies.

La vicepresidenta

Moltíssimes gràcies. Ara és el torn del Grup d'Esquerra Republicana. Té la paraula la diputada Marta Vilalta.

Marta Vilalta i Torres

Sí, moltíssimes gràcies i moltes gràcies també a la directora de l'Agència de Ciberseguretat de Catalunya, la senyora Caballero per tota la feina que ens ha exposat dels anys 23 i 24, però també de tota l'activitat que sabem que fan al dia a dia. Per això, algunes de les preguntes no seran només de mirada enrere, que està bé saber tot el que es va fer el 23-24, el que es va fer també el 25 i s'està preparant i el que s'està treballant ara, sinó també com afrontem els reptes i de mirada de futur.

Sense cap mena de dubte –i crec que això és un consens majoritari–, la ciberseguretat i com les administracions públiques hi poden fer front és un dels temes clau avui dia, en la nostra època. A escala global parlaves dels reptes a nivell de geopolítica, de la intel·ligència artificial, que són globals arreu del món però, per tant, també ens afecten a Catalunya. I en tenim notícies cada dia, ahir una atac a Barcelona, a l'Ajuntament de Barcelona en l'àmbit de la borsa d'habitatge, la setmana passada doncs també semblava una atac al Ministeri d'Hisenda. En fi, parlaves de fa dos anys o tres a l'Hospital Clínic, i així podríem parlar d'Acció l'any passat, etcètera, és a dir, amb aquestes dades que fan esfereir, aquests milers de milions d'intents d'atacs als que heu de fer front.

Per tant, és un gran repte i que ens afecta de ple també a Catalunya, no estem immunitzats a aquest fenomen. I davant d'això nosaltres sempre hem considerat

l'Agència de Ciberseguretat com una estructura d'Estat i per això els hi tornem a demanar ja ho vam fer la primera vegada que va comparèixer en aquesta comissió, la màxima ambició en aquest àmbit, que creiem que així ho estan treballant també seguint el relleu de les etapes anteriors en el marc de l'Agència, també feien referència, de fet, aquestes memòries fan referència als equips anteriors, però aquesta continuïtat també la volem posar en relleu i encomanar aquesta ambició amb la qual s'ha de seguir treballant en aquest àmbit.

Llavors, li voldríem fer unes quantes preguntes, com dèiem, no tant amb la mirada posada en els anys anteriors sinó també en els reptes actuals, vinculades a les funcions i a les necessitats de l'Agència. El món local, en parlaven també ara. Sobretot, aquells municipis rurals amb poca població que, d'acord que no tenen un impacte molt gran amb la quantitat de població que hi viu, però sí que poden ser vulnerables. De fet, fins i tot més vulnerables perquè no tenen les eines.

Llavors hem vist que en aquest últim any han treballat amb certificació de seguretat digital gratuïta per ajuntaments, també amb el consorci Localret, però ens agradaria si pogués aprofundir com s'està treballant per protegir també el món local i per dins d'aquest ecosistema, dins d'aquest perímetre, com treballar la seguretat. També que ens fes una valoració de les campanyes de sensibilització que han fet, de fet les hem vist als mitjans de comunicació aquest últim any especialment, com hi ha hagut –creiem–, o com a mínim aquesta és la percepció, un increment en campanyes de sensibilització, quin ha estat el retorn, l'impacte, quina valoració en fan.

I sobre la manca de talent, que ara també sortia en la conversa anterior, com ho estan treballant? Ens parlava en la primera compareixença de la ciberacadèmia, de possibles treballs amb universitats, amb centres de formació professional, amb aquest talent també femení que sempre fa falta, si ens pogués aprofundir també una mica com està el fet de poder tenir tot el talent, no només la formació necessària de base als treballadors públics, sinó el talent necessari per fer front a totes les amenaces.

I també li voldríem fer una pregunta sobre si ens fan falta a Catalunya canvis legislatius, sabem que hi ha regulacions europees, de fet modificacions que s'estan fent ara, sabem que a l'Estat espanyol s'està pendent de la transposició justament

de les directives europees, però a Catalunya –i sabem que tot això és global–, però si a Catalunya necessitem o no des del seu punt de vista alguna regulació específica en matèria de ciberseguretat i o en matèria d'intel·ligència artificial, que està molt vinculat, que és una font d'oportunitat sense dubte, però d'amenaça també. I en aquest sentit saber si des del seu punt de vista ens faria falta una regulació, una normativa específica en aquest àmbit.

I, per acabar, voldria comentar-li dos temes que no han sortit o..., un segur que no ha sortit, i és que en l'àmbit de la ciberseguretat ham de fer referència obligatòria al fet que en l'última dècada o en els últims anys un dels principals riscos a nivell de ciberseguretat a la Generalitat de Catalunya ha estat també el ciberespionatge a personalitats, sobretot del món independentista, catalanes, per part de l'Estat espanyol a través dels programes com Pegasus o com Candiru. Ja ens va explicar en la seva primera compareixença que això no són ben bé les seves funcions, però sí que són unes amenaces vinculades en aquest cas a la seguretat personal i d'una sèrie de persones.

El seu predecessor, el director anterior va comparèixer a la comissió d'investigació d'aquest Parlament sobre els afectats per l'espionatge de Pegasus i ens va explicar que des del 2022, justament quan es va començar a detectar això es van adquirir capacitats pròpies de detecció de programari espia, que es van implantar capacitats de monitoratge i protecció contínua als usuaris més crítics, sobretot alts càrrecs, de fet es feia un programa de prevenció que afectava més de la meitat dels alts càrrecs de la Generalitat. Bé, la pregunta és si s'ha donat continuïtat a aquests serveis de monitoratge, de prevenció o de seguiment, per tant si s'ha donat continuïtat a aquest programa i activitats o, si per una altra banda això ja no es fa, atès que ara consideren que ja no hi ha un risc perquè ara l'independentisme ja no està al Govern de la Generalitat de Catalunya.

I finalment, una última referència també amb aquesta mirada de futur immediat, i tenint en compte, com li deia, que l'agència de ciberseguretat és el referent i ha de ser el referent en l'àmbit de la ciberseguretat al nostre país i en les administracions públiques del nostre país. Aquí hi ha dos objectius que per Esquerra Republicana creiem que són cabdals, temes que s'estan treballant a nivell de país. El traspàs de

Rodalies, d'una banda, de l'empresa Renfe cap a la Generalitat, la nova operadora i el traspàs també de la gestió de l'IRPF cap a l'Agència Tributària de Catalunya. Dos àmbits on la ciberseguretat és un element cabdal i ha de ser cabdal i pot ser crític, si no es treballa bé.

I en aquest sentit sí que ens agradaria saber com l'Agència de Ciberseguretat de Catalunya estava col·laborant amb la resta de departaments o si s'han fet accions justament per a dimensionar-se o per a poder treballar aquests reptes, aquests traspassos i, per tant, com estar més preparats perquè quan tinguem el traspàs integral de les infraestructures al nostre país o, en tot cas, del servei de ferrocarril i també de tot el que és l'Agència Tributària de Catalunya amb tot el que ha de ser la gestió i la decisió sobre els nostres tributs i impostos, com s'està treballant i preparant perquè hi hagi la seguretat en aquests àmbits.

I amb aquest últim segon que em queda, el moment que va caure el sistema operatiu de Rodalies la setmana passada es va dir que potser era un ciberatac, després van dir que no, que havia sigut un error del software, però sí que voldríem saber si en aquell moment van demanar el seu servei, si van estar en contacte i, per tant, si també van estar treballant davant..., en el que es creia en un primer moment que havia pogut ser un ciberatac.

Gràcies per la feina. Li he fet moltes preguntes però, en tot cas, ens importa molt el tema i creiem que és molt important seguir enfortint l'Agència de Ciberseguretat de Catalunya i, per tant, ens posem a disposició també per seguir treballant.

Gràcies.

La vicepresidenta

Moltes gràcies. La següent intervenció és la del Grup Popular i té la paraula el senyor Escribano.

Cristian Escribano Ramírez

Gràcies, presidenta. Gràcies per la intervenció que ha fet, senyora Caballero, perquè sumat a la lectura de la memòria, la veritat és que és molt revelador. Igual com ha fet la senyora Vilalta, jo li faré unes quantes preguntes durant la meva intervenció que també entendré perfectament que no es puguin respondre totes en aquesta

compareixença, però que també serviran com a reflexió futura del que al nostre parer ha de ser també la feina de l'Agència. I és que, si alguna cosa tenim clara, és que la ciberseguretat és seguretat pública i que, quan falla, falla el nostre sistema públic. I la memòria recull els incidents freqüents, els més freqüents són fuites de credencials i instruccions amb comptes no privilegiats. És a dir, planerament el que vol dir és que el risc normalment entra per la porta del davant.

Identitats digitals febles, higiene bàsica insuficient i una cultura de la seguretat que encara no està prou interioritzada en tota l'Administració i el sector públic. Les dades sobre credencials, compromeses i instruccions bàsiques apunten a un element clau i és que el factor humà continua sent el primer factor de risc, però també ha de ser el primer mur de contenció. Aquí l'agència, des del nostre partit, té una oportunitat d'impacte positiu molt clara i és liderar una veritable cultura de la ciberseguretat a tot el sector públic, no només mitjançant protocols o normatives, sinó amb formació pràctica, simulacions, acompanyaments i també responsabilització progressiva als sectors públics.

Aquí, com també han fet referència altres companys, la implicació del món local també és molt clau i sí que és veritat que en els últims anys s'està incidint molt. Jo, des de la meva perspectiva de regidor, que també a Mataró, per exemple, tenim un telèfon, no és el mateix mesures de seguretat quan ens el van donar que ara. S'han anat implementant algunes que realment et dificulten l'entrada, però que l'impacte és molt positiu per quants atacs tenen també els ens locals.

Un altre element que també desprèn la lectura de les memòries és l'evolució cap a un model proactiu. Passar de gestionar incidents a anticipar riscos hauria de ser l'objectiu estratègic. Això implica avançar a la intel·ligència de les ciberamenaces en anàlisi predictiva i en prioritzar el risc com un element clau. El fet que l'agència assumeixi rols com l'òrgan d'auditoria tècnica, evidentment ajuda a fer aquest salt, sempre que també vagi acompanyat de criteris homogenis i exigents.

És per tot això que nosaltres –ara li faig les dues primeres preguntes–, i és, tenen dades sobre el temps mitjà de detecció i de resposta? I també especialment, quin és el nivell de maduresa per àmbits crítics com la salut, el món local i les universitats?

Per altra banda, la ciberseguretat pública ja no només va de delinqüència digital, sinó que va d'una guerra híbrida d'espionatge, de sabotatge i també, com vostè ha dit, de pressió geopolítica. Els informes europeus assenyalen activitat a Europa d'actors vinculats a Rússia, però també a la Xina en campanyes de ciberespionatge.

I l'EEAS ha documentat també infraestructures i operatives d'ingerència informativa, principalment russes, però també xineses per manipular l'espai informatiu europeu. La ciberseguretat no entén de compartiments administratius, per això és rellevant que l'Agència reforci i sistematitzi la coordinació amb altres nivells del Govern, especialment amb organismes estatals competents i amb els mecanismes europeus de resposta i alerta.

Això, que té conseqüències directes per Catalunya, com vostè ha explicat, també ens fan dirigir-li un parell de preguntes. Tenen una línia específica de detecció i atribució d'amenaces d'actors estatals? I també, com coordinen això amb els organismes competents estatals i europeus, perquè també s'ha expressat aquí, la coordinació és clau.

És evident també que el context internacional obliga a totes les administracions a pensar la tecnologia en clau geopolítica i que l'Agència contribueixi a orientar aquestes decisions, aportant criteri tècnic i visió estratègica, és una aportació de gran valor pel conjunt del Govern i pel sector públic. També hem de parlar –i per nosaltres és important–, de la cadena de subministrament tecnològic. La Comissió Europea ha estat explícita i, en el marc del Toolbox de 5G considera Huawei representa riscos materialment més alts que altres proveïdors i ha defensat restriccions i exclusions, són justificades i alineades amb la seguretat europea. I recentment la Comissió ha tornat a moure fitxa amb propostes per reforçar i fer més vinculants els *de-riskings* de proveïdors d'alt risc en infraestructures crítiques.

Per això, aquí la pregunta és molt específica i és sobre..., també creiem que ha de tenir aquí l'Agència una feina proactiva i és, està recomanant l'Agència aplicar una política de compra pública segura, amb criteris de risc geopolític, auditories i plans de substitució? Perquè aquí també és on l'Agència podria recomanar al Govern sobre totes aquestes directives o recomanacions europees, per facilitar també que

dins del sector públic totes aquelles eines que es faciliten als treballadors tinguin aquest plus de seguretat d'inici.

És a dir, no esperar que puguin venir atacs de fora, sinó que l'atac ja estigui pràcticament instal·lat d'un inici i tenir un menor risc. I finalment, cal dir que a Catalunya i des de la seva agència tenim l'oportunitat de liderar molt bones pràctiques en ciberseguretat pública dins de l'àmbit autonòmic però també dins de l'àmbit europeu, sempre que prioritzem la transparència en indicadors, l'avaluació de l'impacte real, una compra pública responsable i un enfocament clar als serveis essencials. Les memòries apunten molt bé les eines i els camins, o sigui, jo no tinc cap advertiment a fer-li a l'informe.

També vostè ens ha avançat que l'informe que ens presentarà del 2025, tots aquests indicadors dels que hem parlat, augmenten i això no és atribuïble en cap cas a l'Agència perquè, en un context mundial on totes les amenaces de la ciberseguretat augmenten, també la inversió que fem amb l'Agència, hem de pensar si és prou adequada, però invertir en ciberseguretat al final és invertir en el nostre sector públic. Així que moltes gràcies per la seva compareixença.

Repeteixo, entenc que la magnitud de les preguntes que li he formulat el meu grup i a altres grups fan difícil que ens les pugui respondre, però jo crec que la seva és una feina prou important com perquè, bé, jo estaré encantat de tornar a aquesta comissió quan vostè torni.

Gràcies.

La vicepresidenta

Moltíssimes gràcies. És el torn del Grup de Comuns, perquè VOX no hi és, per tant, té la paraula la diputada Núria Lozano.

Núria Lozano Montoya

Gràcies, vicepresidenta. I gràcies a la senyora Caballero per la seva compareixença. Mentre que la memòria del 2023 presentava una institució que consolidava la seva posició com a peça clau, en canvi, el 2024 s'obre de manera clara una etapa de maduració de planificació a mig termini, marcada per noves iniciatives, també per la consolidació dels eixos i del marc estratègic que s'havia posat en marxa l'any

anterior. Per tant se'ns presenta no ja com un escut reactiu, que és una mica el punt de partida, sinó com a impulsora d'una governança digital segura i col·laborativa, aprofundint en aquestes línies de treball.

I en aquest sentit és cert que es consolida com a autoritat en ciberseguretat, que audita, que certifica aquest compliment de les normes de seguretat, tant a la Generalitat com als seus ens vinculats. Ens ha semblat molt interessant tot el relacionat amb la innovació en seguretat pública, molt particularment el programa de *bug bounty*, perquè a més a més de ser una iniciativa pionera a l'Estat espanyol implica també un reforç de la transparència i un exercici de col·laboració amb el sector i amb experts de caràcter internacional, que ens sembla molt interessant en aquest camp.

Com ens ha semblat igualment interessant l'impuls que s'ha fet a la conscienciació i formació ciutadana, tant en formació i divulgació. Segurament els usuaris del transport públic i les usuàries tenim clars aquests cartells que hem anat veient en alguns espais de transport públic, que segurament per alguna gent era el primer cop que algú s'adreçava directament a elles per parlar d'aquestes qüestions, malgrat que és un lloc on tothom va amb el mòbil a la mà, i permeti'm el símil, però ens semblava un espai molt adient per fer aquesta tasca de sensibilització, donat l'ús intensiu d'aquesta tecnologia al mateix.

En qualsevol cas i partint també d'un altre element que ens sembla important, farem també alguna referència més en clau de futur, algunes preguntes amb llavor de resposta, d'altres que no, i alguna reflexió. Però sí que ens ha semblat molt interessant el fet que el nou contracte programa permet una planificació de caràcter plurianual, que garanteix una estabilitat pressupostària que fa possible que es pugui desenvolupar la tasca amb una altra perspectiva, que permet tenir una mirada una mica més llarga.

Deia que voldríem aprofitar també aquesta compareixença per destacar alguns punts clau, per allò que se'n diu progressar adequadament en la matèria, respecte als quals voldríem conèixer el seu parer. Per Comuns la ciberseguretat és una qüestió de servei públic i de drets de ciutadania. És a dir no parlem només d'una qüestió tècnica, encara que ho sigui, sinó d'un bé comú i d'un deure dels poders

públics envers la gent, perquè cap Administració ni cap persona quedi desprotegida davant de les amenaces digitals. I, per tant, ho entenem com a part del contracte social digital.

Igual que garantim seguretat física hem de garantir seguretat en línia sense que hi hagi fractures, ni territorials, ni tampoc socioeconòmiques. Per això proposem estudiar la creació d'una oficina de ciberseguretat pel ciutadà on qualsevol entitat, sigui una entitat social, sigui una pime, sigui una persona física, s'hi pugui adreçar per aquelles necessitats que tingui. O bé perquè ha patit un incident, o perquè necessita consells de prevenció, o perquè vol accedir a formació i a capacitació en la matèria. Si s'han plantejat una mesura d'aquest tipus.

Com considerem que protegir els serveis públics i la democràcia en l'era de l'IA és absolutament clau, s'ha fet referència abans als cada cop més creïbles atacs de *phishing*, també a les *deepfakes* que circulen. I sí que tenim un element de preocupació, perquè més enllà de normalitzar-les com a vector d'atac, que això és una realitat, ja, parlem d'un risc per la democràcia i pel sector públic i ens hem d'avançar a les amenaces. És fàcil imaginar atacs de desinformació massiva o suplantacions d'identitat per minar la confiança ciutadana en les institucions.

I, per tant, ens plantejàvem què proposeu per reforçar la recerca i protocols respecte a aquestes qüestions, també respecte a la desinformació digital, que és un autèntic problema ja a data d'avui, i també per desplegar les previsions del futur Reglament d'Intel·ligència Artificial europeu, que exigirà controls de ciberseguretat obligatoris pels sistemes d'alt risc, en quins termes consideren que s'hauria de produir.

Després pel que fa a la governança digital i la sobirania tecnològica des d'una òptica de país, doncs defensem també aquesta sobirania popular a l'àmbit digital i això passa per una governança democràtica de la tecnologia, amb un òrgan de coordinació interdepartamental que vetlli pel compliment de la seguretat a tota la Generalitat i al seu sector públic de manera transversal, integrant la ciberseguretat en cada nova política pública de caràcter digital. Al respecte, quines previsions tenen?

I una qüestió que sí que li volem dedicar una atenció especial, que és la perspectiva feminista i social, tant pel que fa al talent com a l'educació i als drets digitals. Pensem

que és imprescindible incorporar de manera transversal la perspectiva de gènere i d'inclusió social en l'agenda de la ciberseguretat i és preocupant que no només no avancem cap a la paritat, sinó que fins i tot el 2024 el component de gènere sigui un dos per cent inferior al del 2023. Un senyal d'un problema que és cert, que és no només de l'Agència, és en general el sector tecnològic, però clar, cal establir objectius de paritat en formacions i contractacions, també promoure referents femenins per incentivar aquesta aportació d'un talent que ens estem perdent i que dona una mirada diferent respecte aquestes qüestions.

També pel que fa a l'atenció a la violència digital de gènere. Pensem que necessitem protocols especialitzats, probablement en col·laboració amb l'Institut Català de les Dones i amb entitats especialitzades. Quina actuació tenen prevista al respecte?

Des d'una perspectiva d'horitzó ecosocial i sostenibilitat tecnològica, nosaltres volem parlar també de sostenibilitat social i cal garantir a la ciutadania els drets digitals assegurats, privacitat, protecció de dades, accés equitatiu a la ciberseguretat. I, en aquest sentit si s'han plantejat impulsar una Carta Catalana de Drets Digitals, que pugui reforçar i desplegar aquests principis a casa nostra i reconegui explícitament el dret a la ciberseguretat com a part del dret a la seguretat i a la intimitat –i vaig acabant, vicepresidenta–, des d'un punt de vista també de sostenibilitat tecnològica i mediambiental, perquè cal posar l'accent en un aspecte emergent, en la relació entre tecnologia, seguretat i sostenibilitat ambiental. Cal millorar l'eficiència energètica dels sistemes, hi ha un ús molt intensiu d'energia, fomentar l'ús de renovables també als centres de dades públiques.

Bé, a tall de conclusió, vivim temps de canvis cap a un món diferent al que havíem conegut i la ciberseguretat és imprescindible per la prosperitat i estabilitat del nostre país, però ha de ser per tothom, per institucions, per empresa i per ciutadania treballant conjuntament. Celebrem els avenços assolits, però pensem que cal patir perquè es mantingui el rumb i s'accelerin les accions i des d'aquesta perspectiva demanem al Govern reforçar el suport polític i material a l'Agència de Ciberseguretat, consolidant-la com una eina pública al servei del bé comú, que és un país cibersegur, lliure, igualitari i sostenible.

Moltes gràcies.

La vicepresidenta

Gràcies, diputada. Donat que el diputat de la CUP ha hagut de marxar a una altra comissió i la diputada d'Aliança avui no ha assistit a aquesta convocatòria, té la paraula per concloure el torn d'intervencions la senyora Ivana Martínez, del Grup Socialistes i Units per Avançar.

Ivana Martínez Valverde

Doncs, gràcies. Primer, donar-li les gràcies per la seva presentació i donar la benvinguda també a la companya que l'acompanya de l'equip. No sé si li donarà temps, òbviament, a totes les preguntes, esperem que..., sinó la podríem convidar a venir un altre dia o fins i tot per escrit, no ho sé si això és possible, però crec que em quedaran preguntes molt interessants i..., perquè al final, també escoltant la resta de grups, crec que és de les poques compareixences on tothom està d'acord en la necessitat i en la importància d'aquesta agència, no? Cosa que hem de tenir molt clar, perquè al final tots i totes coneixem alguna persona, alguna entitat, alguna administració que ha patit un intent d'atac o un atac i, bé, aquí es veu, amb els números que vostè ha donat d'atacs i que cada vegada estan augmentant més.

Desgraciadament crec que no ha sigut tampoc una sorpresa, sí el número, però no el fet que hagin augmentat perquè, com deia, tothom al final ha patit d'alguna manera o una altra un ciberatac i creiem, això reforça, creiem, aquesta necessitat que aquesta agència cada vegada tingui més força, tant a nivell de pressupostos com a nivell de personal, crec que no hi ha ningú d'aquesta sala que pugui dir el contrari i així s'ha vist en les intervencions amb anterioritat meves.

També jo vull destacar, sobretot, una de les coses que vostè ha dit, que és el tema de la formació. Creiem que la formació, tal com vostè ha dit, és súper positiu que cada vegada es demani més, hi hagi més importància, fins i tot li deia al meu company, potser ens hauríem de plantejar com a Parlament fer algun curs de ciberseguretat, perquè és veritat que és el dia a dia que ens trobem i moltes vegades, nosaltres mateixos que potser hem de fer alguna llei a posteriori, com deia la companya Vilalta, no tenim aquesta informació per poder lluitar contra o amb la ciberseguretat. I jo crec que potser com a Parlament ens hauríem de plantejar que

aquesta formació també ens arribi a nosaltres, perquè al final, després venim, donem la nostra opinió però no tenim totes les dades i tota la informació.

Tema de gènere. Jo crec que hem de fer una reflexió social en general. Tenim un problema amb el tema de gènere, i només cal veure les aules. Jo no parlo de les aules de la formació que vostè dona, sinó les aules dels cicles formatius a les universitats on el gran percentatge, jo crec que podríem parlar d'un vuitanta per cent són homes. Jo conec un cas on només hi ha una nena al cicle formatiu de tota una aula. Bé, n'hi havia dos i una ho va deixar. És a dir, tenim un problema com a societat, perquè al final és un tema latent. Crec que referents com vostè –i així li dic, senyora Caballero–, és molt important perquè les nenes del país han de tenir referents femenins que vegin que podem estar davant d'un espai que no és només d'homes, sinó crec que és molt important que hi hagi referents com vostè, així que també la felicito per la part que li toca.

Però sí que és veritat que hem de fer una reflexió com a societat i nosaltres com a polítics també hauríem de fer alguna cosa i pensar què estem fent malament perquè no arribi l'interès d'una cosa que, com he dit al principi, que ens toca a tots i a totes. I, ostres, alguna cosa estem fent malament. Jo aquesta seran únicament les meves reflexions. Ara li faré les preguntes. Vostè ha parlat dels fons europeus. M'agradaria si ens pogués explicar una miqueta més aquests projectes i centrar-se una miqueta més en aquest tema tan important. Després, bé, el tema de formació com m'havia apuntat però ja l'hi he dit.

I també voldria saber una opinió, perquè vostès són un mecanisme al final de control de la ciberseguretat, i aquests últims dies hem vist l'anunci que ha fet el president del Govern Pedro Sánchez sobre la prohibició de les xarxes socials als menors de setze anys, que al final és una manera també de protegir d'aquests ciberatacs, d'aquestes substitucions, aquests perfils, aquest ús de la intel·ligència artificial per modificar fotografies de nenes, etcètera. I llavors, vostè com veu aquest anunci de la prohibició de les xarxes socials? I bé, una mica que ens doni el seu parer.

I una altra vegada gràcies per venir i molt interessant.

Gràcies.

La vicepresidenta

Moltíssimes gràcies, diputada. Bé, ara té una feina, directora *(La vicepresidenta riu.),* perquè se li han fet moltíssimes preguntes. Li dedicarem un torn de quinze minuts, si li sembla bé i, a veure com ho fa...

Laura Caballero Nadales (directora de l'Agència de Ciberseguretat de Catalunya)

Moltíssimes gràcies, primer de tot. Preguntes súper interessants de tots vostès. Com tinc pocs minuts i hi ha preguntes molt interessants, aniré directament al gra. Han parlat vostès de la ciberseguretat com un servei públic. No puc estar més d'acord amb vostès. És a dir, la ciberseguretat ha d'estar al servei de la ciutadania, de les empreses, i també de l'Administració pública. I aquesta és una miqueta la meva aposta, també com a directora, que això ha de ser un servei públic. I en aquesta línia feia referència la diputada d'Esquerra.

És cert, hem aparegut a les campanyes, als mitjans de comunicació precisament en aquesta línia, de dir, escolta, això no és només de protegir les grans empreses, això no és només de protegir l'Administració, que també, sinó això també va que els nostres pares, els nostres fills, estan exposats. I ja no és una cosa trivial. No, és que això va també de perdre els diners, del risc de perdre els diners, de perdre la reputació, de posar en risc els seus drets fonamentals.

Per tant, estem incidint molt en els medis, ens hauran vist a TV3, a les falques radiofòniques, també. Per donar algunes dades, vam treure al canal de WhatsApp i d'avisos de ciberseguretat una cosa tan senzilla com és un canal de WhatsApp, on cada dia pràcticament estem traslladant les estafes que estan corrent per internet, especialment a Catalunya, amb l'objectiu que els nostres ciutadans i ciutadanes tinguin de primera mà el que està corrent perquè estiguin previngudes i previnguts. I ja tenim més de disset mil subscriptors al canal. O sigui, ha sigut un èxit que, sincerament, ni ens ho esperàvem.

Per tant, aquest interès creixent s'ha posat a manifest i jo no només –i aquí potser estic avançant coses, però jo no només vull quedar la part de conscienciació i la formació, que crec que és importantíssima, sinó que hem de donar eines a la ciutadania perquè estiguin empoderats i tinguin l'autonomia per discernir i saber poder distingir entre si una cosa que els arriba és bona o si és dolenta. Aleshores,

estem treballant en aquesta autonomia també de la ciutadania, perquè a vegades conscienciar no és suficient.

I per què ho dic? Perquè amb el tema dels *deepfakes*, que també s'ha esmentat, això es posarà cada cop més complicat. I llavors, conscienciar és importantíssim, però també és molt important que qui toca i les plataformes, per exemple, de comunicacions, les plataformes de les xarxes socials, han de fer mesures per poder diferenciar què és allò que està generat per IA i què no. Que jo, quan em truquin, pugui saber si aquesta trucada està generada per una IA i no. Hi ha mecanismes tècnics que això permeten.

Llavors, hem d'advocar perquè també sigui una corresponsabilitat, que no només quedi de la part de la ciutadania, en aquesta conscienciació, que sí. En aquest sentit, farem iniciatives, estem posant-nos en contacte amb aquest tipus de plataformes. Volem establir relacions per advocar i forçar que aquestes coses també passin aquí, en totes aquestes plataformes.

I parlàvem que sigui un servei públic. Sí, un servei públic, per als ciutadans i ciutadanes però també pel món local, efectivament. El món local és una de les principals víctimes, per exemple, dels atacs de ransomware, perquè molt bé apuntaven que, al final, són aquelles entitats que potser tenen menys recursos i, per tant, estan menys preparades.

Què estem fent aquí? A banda que promocionem qualsevol iniciativa a nivell de conscienciació i jo estic voltant bastant, m'haureu vist en molts llocs i tinc molta presència, perquè quan se'n parla un es consciencia. A nivell de fons europeus RETECH i també per contestar a la pregunta de la diputada del PSC, hem engegat un projecte amb Localret, efectivament, que a banda de donar suport a la certificació de l'Esquema Nacional de Seguretat, que això és importantíssim, perquè al final demostra la diligència dels ajuntaments per dir, escolta, estic fent les coses bé i ho vull demostrar i per això em certifico, estem desplegant les primeres fases del nostre model de protecció.

I això què implica? Nosaltres tenim un model de protecció que es basa –ara no em posaré a..., abaixaré tècnicament, però en diferents fases. I les primeres fases són les de diagnòstic i les de pla d'acció. I això és important, perquè el primer que has

de fer quan arribes a una entitat és saber com està. Com està i quines accions has d'emprendre per tal de resoldre totes aquelles vulnerabilitats que pugui tindre aquesta entitat. Això amb els fons de RETECH, una de les iniciatives més cabdals d'aquests fons RETECH és poder donar aquest diagnòstic tècnic i de consultoria i després un pla d'acció als ajuntaments. Llavors, els ajuntaments tindran a disposició aquests fons per tal de desplegar les fases 1 i fase 2 que comentava. Per tant, món local també és importantíssim. Al final, és el que està al territori i ens hem de –en aquesta línia del servei públic–, ens hem d'enfocar en això.

Com veieu, es parlava d'ambició. Jo ambició la tinc tota. El que sí que és cert –i aquesta ambició també és una ambició, a banda que com a directora em surt–, és una ambició que ve forçada també, és que no ens podem quedar quiets. Com ens quedem quiets realment estem parlant d'integritat democràtica, de resiliència del país. Per tant, sí o sí, ha d'haver-hi ambició. Sinó, sí que tindrem problemes. En aquest sentit, que sapigueu que estem treballant molt fort per executar durant aquest any els fons RETECH, que serà quelcom molt diferencial i és una inversió històrica pel país a nivell de ciberseguretat.

I estic d'acord amb vostès i això també ho hem així sol·licitat a nivell de pressupostos, que això estigui alineat amb la capacitat de recursos i la capacitat operativa de la pròpia agència. És a dir, estem parlant de números històrics i, per tant, això d'acompanyar també d'una capacitat de recursos que estigui alineat amb el que comentem.

Què més? A nivell de talent. És cert que podem parlar de xifres històriques, però si no tenim talent que pugui proveir aquests serveis doncs tindrem les eines però no tindrem ningú que les pugui manegar. Aleshores, el talent en ciber, en general, és un repte molt important. Per què? Perquè és un talent escàs i és un talent que, al final, competeix a nivell mundial amb la resta d'empreses que estan instaurades. És cert que, això ens ho comenten els nostres proveïdors, hi ha una molt alta competència perquè això és l'oferta i la demanda, és així, si hi ha pocs professionals estan molt demandats i això és un problema que s'ha d'enfocar.

Com estem enfocant des de l'Agència aquesta manca de talent? Doncs, per exemple, s'ha esmenat el tema de la ciberacadèmia. La ciberacadèmia no vol

substituir ni les universitats, ni els centres formatius. La ciberacadèmia busca més crear un interès en professionals que potser no venen del món de la ciberseguretat, però que podrien ser perfectament perfils que puguin ser adequats per fer un canvi en el món de la ciberseguretat. Hi ha molta gent de la ciberseguretat que no venen estrictament, perquè a la ciberseguretat abans no hi havia una carrera, ara hi ha una o dos. Jo sí que soc enginyera, però hi ha molta gent que ve d'altres àmbits i d'altres *backgrounds* que també són perfectament vàlids dintre del món de la ciberseguretat.

A vegades pensem que la ciberseguretat és només un tema tècnic, s'ha comentat, no és només un tema tècnic. Per mi la ciberseguretat és 360. És a dir, des de la conscienciació, des de la part normativa, des de la part tècnica, agafant des de la part de gestió de riscos i aquí hi caben molts perfils. És a dir, no només la part tècnica. Per tant, la ciberacadèmia ha de servir com aquella entrada per generar l'interès, això estarà en el juny del 2000, bé, d'aquest any, estarà llançada la ciberacadèmia, però també anem de la mà de les universitats. Cada cop que ens criden, cada cop que, ei, aneu a fer una xerrada als col·legis, aneu a fer una xerrada als instituts, és a dir, nosaltres estem en plena disposició perquè som conscients que o generem aquest interès o sí que és cert que tindrem un problema de talent.

I està molt relacionat també amb el tema del talent femení. És a dir, malauradament, jo quan vaig començar la meva carrera d'enginyeria doncs les xifres no han variat gaire, llavors hem de fer alguna cosa en aquest sentit, i una de les coses que jo em dec com a directora i que tinc molt ficada al cap és que, per aconseguir que les dones també sentin que la ciberseguretat també és cosa d'elles, és generar referents. Llavors aquí sí que intentem amb el tema de DonaTIC, DonaCiber, amb aquests premis, amb totes aquelles iniciatives que també tenim un informe de DonaCiber que també surto a explicar aquestes dades que creïn de dir, escolta, això també és cosa vostra.

Per tant, aquí entomo també aquesta responsabilitat i amb tota la humilitat del món d'actuar com a referent i tant de bo hi hagi més dones que agafin aquest camí perquè realment és el futur, i sinó, estarem traient de l'equació a la dona d'una de les professions del futur. Per tant això com a societat jo crec que no ens ho podem permetre.

S'ha parlat de models legislatius, de normes legislatives. Jo crec que, més enllà de generar una nova legislació i sota el meu parer, el que és important és que realment es prenguin seriosament les legislacions i que d'alguna manera aquestes legislacions estiguin alineades, perquè sinó, serà impossible abordar totes les legislacions que estiguin apareixent. En aquest sentit nosaltres com a òrgan d'auditoria tècnica som, fem capacitats per certificar l'Esquema Nacional de Seguretat, és la regulació que aplica a nivell de ciberseguretat a nivell d'Estat i, al final, creiem que és perfectament vàlid com a legislació.

Aquí el que hem de fer és advocar i aconseguir que, efectivament, les empreses donar-los suport, acompanyament perquè realment es muntin en aquest carro de la certificació, perquè és una manera molt sana i molt bona de saber on estàs i què has de fer per poder arribar on hauries d'estar amb els requeriments de seguretat que s'estableixen segons les regulacions.

A nivell de coordinació dic que estem coordinats també amb les diferents autoritats, agències, organismes de ciberseguretat. A nivell d'Espanya, per exemple, amb el Centro Criptológico Nacional, és a dir, en aquest sentit hi ha una col·laboració absoluta. Amb l'Incibe, que és la part més de ciutadania i de la part d'empreses privades igualment, és a dir, que intentem sumar esforços i és que no només també amb Espanya, sinó també a nivell europeu tenim, per exemple, estem participant a l'EXO que és una associació de diferents empreses de ciberseguretat a nivell europeu, tenim relacions amb diferents països per intercanviar idees i punts de col·laboració, perquè al final això, si ho fem sols no arribarem enlloc.

O sigui, això de la ciberseguretat, dels números que estem parlant, o col·laborem, o sinó el mateix, seran estèrils els esforços que fem, perquè els ciberdelinqüents no tenen fronteres, per tant, en aquest sentit ens hem de posar tots d'acord i col·laborar. Falten recursos i per tant com més siguem i més alineats estiguem doncs millor en aquest sentit.

Hem parlat de la IA amb el tema del servei de la ciutadania, el tema dels *deepfakes,* del món local. Estic repassant una miqueta, eh? En aquest sentit, amb les noves..., amb el fet de traspassar les competències cap al tema de Rodalies o el tema de l'Agència Tributària, comentar que per exemple nosaltres ja amb les entitats ja tenim

un model de col·laboració. Per exemple, amb Ferrocarrils tenen el seu equip de seguretat i estem súper alineats amb els serveis que els hi prestem i també l'alineament amb qualsevol cosa que pugui passar. Nosaltres com a Agència, si passés qualsevol cosa al país estaríem a disposició per ajudar en el que fes falta i així és com actuem, hem actuat i actuarem. Per tant com a rol de Catalònia-Cert és la nostra responsabilitat que qualsevol cosa que passi estarem allà donant suport.

Una de les coses que molt bé comentava, el tema de la identitat digital com a repte. És cert, és que molts cops els vectors d'entrada a vegades ens podem pensar que són tècnicament unes «virgueries», sí que n'hi ha, d'aquestes, però en general el vector d'entrada és el factor humà i aquí ho enllacem amb el tema de la conscienciació. Aquí estem fent molts esforços també a nivell de Generalitat, per exemple, que també hi havia casos de suplantació, de reforçar totes les mesures de seguretat per assegurar que això no passi. Això està passant, és veritat, però tots els temes de les mesures, el doble factor d'autenticació, tot això que estem veient que les aplicacions també a nivell d'Administració pública però també a nivell, a títol individual s'està aplicant, és quelcom molt bàsic, però molt important per evitar aquestes fuites de dades i, sobretot, aquests riscos relacionats amb la identitat digital.

I en aquesta línia, és molt important i torno a la part de proactivitat, és a dir, per descomptat estaré, per descomptat estarem si passa alguna cosa a nivell de país donant suport, però és molt important seguir amb aquest model proactiu. I, com a part de l'estratègia és això, com a part de l'estratègia en aquest mandat sota la meva direcció és seguir amplificant el nostre model, amplificant el nostre model en l'àmbit salut. De fet, si comentàvem que el 2023-2024 efectivament vam començar a protegir els hospitals, ara amb els fons RETECH comencem a ampliar no només els hospitals, sinó els centres sociosanitaris, els centres d'atenció primària, els centres de salut mental. Per tant, tot l'àmbit de salut que, a més, és un àmbit supercrític, estem fent esforços per no només quedar-nos a la part d'hospitals, sinó ampliar i cobrir amb la nostra protecció, amb el paraigües de protecció tot aquest àmbit de salut.

I és important dir que tot això, a nivell més proactiu ens estem preparant nosaltres també mateixos amb la IA. La IA hem dit que no només té coses o té riscos negatius associats, sinó que té unes parts molt positives. Per exemple, estem aplicant la IA per millorar les nostres operacions, estàvem parlant de milers de milions d'atacs, doncs hi ha moltes coses que amb agents d'IA podem eficientar i dedicar-nos a allò que és important.

Hi ha alguns atacs que segueixen una sèrie de patrons i que, per tant, amb agents d'IA som capaços d'integrar-ho a les nostres operacions, reduir la necessitat de dedicar-hi esforços de persones per tasques repetitives. En aquest sentit la IA ens permet ser molt més eficients i això actualment estem implementant un sistema d'IA integrada en el centre d'operacions de la ciberseguretat precisament per això. No només això, les pròpies eines de ciberseguretat estan incorporant IA per tenir moltes més capacitats i nosaltres ens estem aprofitant de tot plegat.

S'ha parlat del tema del ciberespionatge. Reiteraré el que vaig comentar en el seu moment. Nosaltres independentment..., o sigui, no etiquetem la tipologia, ens centrem en protegir els actius de l'Administració pública i aquests actius també estan relacionats amb els dispositius dels propis alts càrrecs. Aleshores, qualsevol cosa i en resposta al que comentava, efectivament, estem tenint continuïtat en la protecció dels alts càrrecs i, per tant, aquestes revisions i aquests sistemes de protecció avançada es segueixen produint. Independentment de la motivació, nosaltres el que ens centrem és en protegir els dispositius i els actius de la Generalitat i això ho fem i ho seguirem fent en aquest sentit. *(Pausa.)*

No sé si m'he saltat alguna pregunta si... *(Veus de fons.)* Sí? Ai, doncs perdoneu. Estava buscant, però jo crec que en general..., si no, doncs, a la plena disposició per respondre a través de Relacions Institucionals qualsevol pregunta que se'n derivi. Entenc que és un tema que, a més, és nou, que tothom d'alguna manera estem aprenent fent camí, així que a plena disposició de vostès per poder respondre-les.

Gràcies.

La vicepresidenta

Moltíssimes gràcies, directora per la seva feina al capdavant de l'Agència i també per la compareixença d'avui. Com veu, desperta moltes inquietuds i moltes preguntes, per tant sempre serà benvinguda en aquesta comissió.

Aturem un segon. És veritat que hi ha una..., el següent punt de l'ordre del dia, però ara en parlem, aturem un segon per acomiadar la directora.

(Pausa llarga.)

Diputats i diputades, un segon només.

Proposta de resolució per a la creació d'un fons de sobirania tecnològica (posposició)

250-00850/15

Ara hi ha un altre punt de l'ordre del dia, que és veritat que per correu s'ha retirat, que és una proposta de resolució del Grup de Comuns, però li volia donar la paraula a la diputada per si vol comentar alguna cosa i si no, evidentment, no cal.

Núria Lozano Montoya

A veure, el diputat titular de la comissió plantejava la posposició i entenc que no hi ha cap inconvenient al respecte, per tant, simplement reiterar aquesta petició.

La vicepresidenta

Posposar..., perfecte. Només perquè quedés en acta que era una proposta de resolució.

Per tant, ara sí, acabem la sessió. I s'aixeca, per descomptat.

Quedin-se els portaveus un segon, també, per parlar de la següent convocatòria.

Gràcies.

La sessió s'aixeca a...