Estratègia Balear de Ciberseguretat

Centre Balear de Ciberseguretat

Financiado por la Unión Europea
NextGenerationEU

Gobierno de España
Ministerio para la Transformación Digital y de la Función Pública
Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_
Instituto Nacional de Ciberseguridad

Vicepresidència Primera i Conselleria d'Economia, Hisenda i Innovació
Direcció General d'Innovació i Transformació Digital

ÍNDEX

00 **Resum executiu** 4

01 **Context global de la ciberseguretat** 8

02 **Diagnòstic balear: situació actual** 14

03 **Missió, visió, valors i eixos estratègics** 20

04 **Objectius estratègics** 28

05 **Línies d'actuació** 48

06 **Evolució progressiva de capacitats** 64

07 **Seguiment, mesura i avaluació** 66

A1 **Memòria econòmica de l'Estratègia** 74

00 Resum executiu

L'acceleració de la digitalització i el creixement constant de les ciberamenaces han transformat profundament l'entorn en què operen la ciutadania, les empreses i les administracions públiques de les Illes Balears. L'expansió de serveis digitals, l'augment de la interconnectivitat i l'adopció de tecnologies emergents han generat oportunitats de desenvolupament econòmic i social, però també una major exposició a riscos, tal com reflecteixen les dades de ciberdelinqüència, que es van multiplicar durant els últims anys.

Per a l'elaboració d'aquesta Estratègia s'han tingut en compte els marcs de referència vigents en els tres nivells que condicionen la política de ciberseguretat a les Illes Balears. A nivell europeu, la Directiva NIS2, el Cybersecurity Act i les infraestructures comunes impulsades per la UE (EU-SOC Network, Joint Cyber Unit, ENISA), que eleven el nivell d'exigència i reforcen la cooperació. A nivell nacional, l'Estratègia Nacional de Ciberseguretat, l'Esquema Nacional de Seguretat i l'actuació del CCN-CERT i l'INCIBE, que fixen el sòl de compliment i els mecanismes de coordinació. I a nivell balear, Pacte Social i Polític per la Sostenibilitat Econòmica, Social i Ambiental de les Illes Balears, del qual aquesta Estratègia és peça operativa, contribuint als seus eixos d'economia resilient i societat cohesionada i als seus objectius de governança i adaptació als reptes globals.

Durant els darrers anys, el Govern ha impulsat iniciatives clau que constitueixen la base d'aquesta Estratègia: la Política de Seguretat de l'IBSALUT, que va permetre consolidar capacitats avançades en el sector sanitari; la presentació el 2022 de la primera Estratègia Balear de Ciberseguretat; l'aprovació el 2025 dels estatuts d'IB Digital com a organisme autònom encarregat de concentrar els recursos tecnològics del Govern; la creació de la Càtedra de Ciberseguretat amb la UIB; i l'aprofitament de fons europeus que han permès finançar serveis especialitzats, infraestructures, formació i projectes de recerca.

20,5M€

El conjunt d'actuacions contemplades en l'Estratègia s'articula sobre una inversió total estimada de 20,5 milions d'euros, concebuda de forma progressiva i alineada amb els diferents horitzons temporals d'execució i amb el model de governança proposat

Sobre aquesta base, l'Estratègia Balear de Ciberseguretat, amb un horitzó de vigència de quatre anys (2027–2030), es concep com l'instrument que permetrà fer un salt qualitatiu cap a un model territorial modern i resilient. El conjunt d'actuacions contemplades en l'Estratègia s'articula sobre una **inversió total estimada de 20,5 milions d'euros**, concebuda de forma progressiva i alineada amb els diferents horitzons temporals d'execució i amb el model de governança proposat.

El seu propòsit és reforçar la seguretat de l'espai digital balear mitjançant un enfocament centrat en la coordinació institucional, la protecció del teixit productiu, la capacitació de la ciutadania i l'impuls del coneixement i la innovació. La seva visió projecta unes Illes Balears referents en ciberresiliència, amb una Administració robusta i homogènia en les seves mesures de seguretat, un ecosistema empresarial competitiu i protegit, una societat formada i conscient del risc digital, i un teixit de recerca —UIB, Fundació Bit, DIHBAITUR— capaç de generar talent i solucions avançades.

Per materialitzar aquesta visió, es defineixen **els valors** amb què l'Estratègia articularà els **tres eixos estratègics:**

Administració digital ciberresilient i de referència

Governança robusta, resiliència dels serveis públics, col·laboració institucional i posicionament en l'ecosistema nacional de ciberseguretat.

Ecosistema ciber- balear: empresa, innovació i talent

Desenvolupament d'una indústria balear de ciberseguretat, impuls de la recerca i la innovació, i generació, atracció i retenció de talent especialitzat.

Societat balear cibersegura

Maduresa i resiliència del teixit empresarial davant de ciberamenaces, i cultura de ciberseguretat en la ciutadania.

9 Objectius
13 Línies d'actuació

L'Estratègia defineix nou objectius estratègics i tretze línies d'actuació que permeten el desplegament coherent.

A partir d'aquests eixos, l'Estratègia defineix **nou objectius estratègics** i un conjunt de línies d'actuació que permeten el seu desplegament coherent, incloent-hi l'operació del Centre Balear de Ciberseguretat, la prestació de serveis regionals, el suport al teixit productiu, l'impuls de la formació i la innovació, i la construcció de capacitats avançades de vigilància i anàlisi

Amb aquesta Estratègia, el Govern de les Illes Balears expressa la seva voluntat ferma de situar l'arxipèlag entre les comunitats autònomes de referència en matèria de ciberseguretat. Aquesta ambició es tradueix en tres compromisos concrets: assolir un nivell de maduresa homogeni i verificable en la ciberseguretat de tota l'Administració balear; consolidar un ecosistema propi de coneixement, innovació i talent capaç de generar valor econòmic i social; i garantir que la ciutadania i les empreses del territori disposin dels recursos, la formació i l'acompanyament necessaris per desenvolupar-se amb confiança en l'entorn digital. L'Estratègia permetrà reforçar la confiança de la ciutadania, millorar la competitivitat de les empreses i assegurar la prestació contínua i segura dels serveis públics, consolidant el territori com una comunitat preparada per als desafiaments del futur digital.

01 Context global de la ciberseguretat

La ciberdelinqüència s'ha consolidat com un dels riscos més rellevants per a l'estabilitat econòmica i social a escala mundial. El *ransomware*, els atacs a cadenes de subministrament, l'explotació de vulnerabilitats en serveis essencials i les campanyes de frau massiu no són ja fenòmens excepcionals, sinó una constant que afecta per igual la ciutadania, empreses i administracions públiques. L'expansió de dispositius connectats, la migració accelerada al núvol i l'adopció de tecnologies com la intel·ligència artificial han multiplicat la superfície d'exposició, configurant un escenari en el qual la capacitat de protecció, detecció i resposta resulta determinant per a la confiança digital de qualsevol territori.

La Unió Europea ha respost a aquest desafiament amb un marc regulatori i operatiu cada vegada més exigent. La Directiva NIS2 ha reforçat substancialment els requisits de governança i gestió del risc per als serveis essencials i importants, ampliant el perímetre d'entitats obligades a tota la Unió, mentre que el Reglament DORA ha imposat estàndards específics de resiliència operativa al sector financer i la Cybersecurity Act ha establert un esquema europeu de certificació de productes i serveis.

En paral·lel, l'Estratègia Europea de Ciberseguretat per a la Dècada Digital ha articulat un paraigua comú de capacitats a través d'instruments com l'European Cybersecurity Competence Centre (ECCC) i la Network of National Coordination Centres (NCCs), infraestructures compartides com l'EU-SOC Network, i mecanismes avançats de coordinació operativa com la Joint Cyber Unit (JCU) i la CSIRTs Network.

El conjunt d'aquest edifici normatiu i institucional configura el marc sobre el qual els Estats membres —i les seves regions— han de continuar construint i evolucionant les seves capacitats de ciberseguretat.

En l'àmbit nacional, Espanya disposa d'un ecosistema de ciberseguretat madur i en evolució contínua. L'Estratègia Nacional de Ciberseguretat de 2019, aprovada pel Consell de Seguretat Nacional, estableix els principis i prioritats per garantir un ús segur i fiable del ciberespai, recolzant-se en l'Esquema Nacional de Seguretat (ENS), actualitzat mitjançant el Reial decret 311/2022, que defineix els requisits de seguretat aplicables al sector públic. Sobre aquesta base, el CCN-CERT i l'INCIBE operen com a pilars de la resposta operativa i del suport tant al sector públic com al teixit productiu i la ciutadania, mentre que la transposició de la Directiva NIS2, actualment en fase d'Avantprojecte de Llei, suposarà un nou impuls regulatori que reforçarà la supervisió i la gestió del risc en els sectors essencials.

Aquest entorn, complementat amb les inversions del Pla de Recuperació, Transformació i Resiliència, reforça la capacitat de l'Estat per articular una defensa cohesionada, facilita la coordinació amb les comunitats autònomes i estableix les bases per al desenvolupament de capacitats avançades de prevenció, detecció i resposta a tot el territori.

En aquest context global, europeu i nacional, les Illes Balears afronten oportunitats i reptes específics derivats de la seva estructura econòmica, la

seva condició insular i la seva elevada dependència tecnològica. La digitalització del territori, impulsada per un sector serveis que representa més d'un terç del PIB, un teixit productiu marcat per milers de pimes i micropimes i una ciutadania altament connectada, ha generat avenços significatius en qualitat de vida i competitivitat, però també ha incrementat de forma notable l'exposició a riscos digitals, tal com reflecteixen les dades de ciberdelinqüència registrades a l'arxipèlag durant els darrers anys.

Per reforçar les seves capacitats, el Govern de les Illes Balears ha impulsat durant aquest període un conjunt d'iniciatives que constitueixen la base sobre la qual es construeix aquesta Estratègia. Entre elles destaca la creació d'una unitat de recerca en ciberseguretat en col·laboració amb la Universitat de les Illes Balears (UIB), considerada el germen del Centre Balear de Ciberseguretat, així com la consolidació d'un organisme de referència en ciberseguretat sanitària en l'àmbit de l'IBSalut, que ha permès desenvolupar capacitats avançades per a la protecció de serveis crítics. Més recentment, l'aprovació el 2025 dels estatuts de l'Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions (IB Digital) com a organisme autònom ha reforçat el model de governança en concentrar els recursos tecnològics del Govern, a la qual cosa se suma la creació de la Càtedra de Ciberseguretat amb la UIB i l'aprofitament de fons europeus (especialment Next Generation EU) que han permès finançar infraestructures, serveis especialitzats, formació i projectes de recerca orientats a augmentar la resiliència de l'ecosistema públic i privat de l'arxipèlag.

1.1

Marc jurídic i normatiu de referència

L'Estratègia Balear de Ciberseguretat s'emmarca en un conjunt articulat de normes i instruments regulatoris europeus, nacionals i autonòmics que defineixen les obligacions, els estàndards i els marcs de cooperació aplicables en matèria de ciberseguretat. El seu coneixement resulta essencial per comprendre el context d'exigència en què opera la Comunitat Autònoma i per garantir que les actuacions previstes en aquesta Estratègia s'alineen plenament amb l'ordenament jurídic vigent.

Marc Europeu

La Unió Europea ha consolidat durant els darrers anys un edifici regulatori ambiciós que estableix obligacions directes i indirectes per a les administracions públiques, els operadors de serveis essencials i el teixit empresarial dels Estats membres:

- La **Directiva (UE) 2022/2555 (NIS2)**, que substitueix la Directiva NIS original, reforça substancialment els requisits de governança, gestió del risc i notificació d'incidents per a un perímetre ampliat d'entitats essencials i importants, establint un marc de supervisió més exigent i harmonitzat a tota la Unió. La seva transposició a l'ordenament espanyol, actualment en fase d'Avantprojecte de Llei, condicionarà de forma significativa l'evolució de les obligacions en matèria de ciberseguretat en els propers anys.
- La **Directiva (UE) 2022/2557 (CER — Critical Entities Resilience)** complementa la NIS2 des de la perspectiva de la resiliència física i operativa de les entitats crítiques. Mentre que la NIS2 se centra en la seguretat de les xarxes i sistemes d'informació, la Directiva CER estableix obligacions perquè els Estats membres identifiquin entitats crítiques en sectors essencials i garanteixin la seva resiliència davant amenaces de tota naturalesa —incloses les cibernètiques, les físiques, les naturals i les provocades per l'home—. La seva rellevància per a les Illes Balears rau en l'estreta interrelació entre la protecció digital i la continuïtat operativa d'infraestructures essencials en un territori insular, on la interrupció de serveis crítics té un impacte amplificat sobre la població i l'activitat econòmica.

- El **Reglament (UE) 2022/2554 (DORA)**, sobre resiliència operativa digital del sector financer, imposa requisits específics de gestió de riscos TIC, proves de resiliència i supervisió de proveïdors tecnològics crítics. Tot i que el seu abast directe se centra en entitats financeres, el seu enfocament i exigències influeixen en l'evolució dels estàndards de resiliència aplicables al conjunt del sector públic i privat.
- El **Reglament (UE) 2019/881 (Cybersecurity Act)** estableix un marc permanent per a l'Agència de la Unió Europea per a la Ciberseguretat (ENISA) i crea un esquema europeu de certificació de productes, serveis i processos de ciberseguretat, orientat a reforçar la confiança en les solucions digitals que operen en el mercat interior.
- El **Reglament General de Protecció de Dades (RGPD) — Reglament (UE) 2016/679** constitueix el pilar fonamental de la protecció de dades personals a la Unió Europea, imposant obligacions de seguretat del tractament, notificació de bretxes i avaluació d'impacte que s'integren directament en el marc de ciberseguretat de qualsevol organització pública o privada.
- El **programa Digital Europe (DIGITAL)** i els instruments financers associats proporcionen el marc de finançament europeu per al desenvolupament de capacitats en ciberseguretat, intel·ligència artificial, supercomputació i competències digitals avançades, constituint una font clau de recursos per a les iniciatives previstes en aquesta Estratègia.

Marc nacional

Espanya ha desenvolupat un ecosistema normatiu i institucional robust que estableix les bases sobre les quals les comunitats autònomes han d'articular les seves capacitats de ciberseguretat:

- La **Llei 36/2015, del 28 de setembre, de Seguretat Nacional** configura el marc general del Sistema de Seguretat Nacional i estableix els principis de contribució de recursos de les administracions públiques, incloses les comunitats autònomes, a la seguretat de l'Estat, incorporant expressament la ciberseguretat com a àmbit d'interès.
- La **Llei 8/2011, del 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques (LPIC)**, i la seva normativa de desenvolupament —principalment el **Reial decret 704/2011** que aprova el Reglament de protecció de les infraestructures crítiques—, configuren el sistema nacional de protecció d'infraestructures crítiques. Aquesta llei estableix el catàleg d'infraestructures estratègiques, defineix les responsabilitats dels operadors crítics i crea les estructures de coordinació (Centre Nacional de Protecció d'Infraestructures Crítiques — CNPIC, actualment integrat a l'Oficina de Coordinació de Ciberseguretat). La LPIC resulta particularment rellevant per a les Illes Balears per la dependència de l'arxipèlag d'infraestructures essencials de connectivitat, energia, transport i telecomunicacions la protecció integral de les quals exigeix una coordinació estreta entre les dimensions física i digital de la seguretat. La futura transposició de la Directiva CER a l'ordenament espanyol actualitzarà i ampliarà aquest marc, reforçant les obligacions de resiliència de les entitats crítiques.
- El **Reial decret llei 12/2018, del 7 de setembre**, transposa la primera Directiva NIS a l'ordenament espanyol, establint un marc de seguretat per a les xarxes i sistemes d'informació dels operadors de serveis essencials i els proveïdors de serveis digitals, i definint les autoritats competents i els CSIRT de referència a nivell nacional.
- **L'Estratègia Nacional de Ciberseguretat 2019**, aprovada pel Consell de Seguretat Nacional, estableix els principis, objectius i línies d'acció que guien la política de ciberseguretat de l'Estat, definint el Consell Nacional de Ciberseguretat com a òrgan de suport al Consell de Seguretat Nacional i articulant la cooperació amb les comunitats autònomes.
- **L'Esquema Nacional de Seguretat (ENS) — Reial Decret 311/2022, del 3 de maig**, que actualitza el

RD 3/2010, defineix els principis bàsics i requisits mínims de seguretat que han d'aplicar totes les administracions públiques espanyoles per a la protecció de la informació i els serveis electrònics. L'ENS, complementat per les guies CCN-STIC, constitueix l'estàndard de referència obligatori per al sector públic balear i l'eix sobre el qual s'articulen les mesures de protecció de l'Administració autonòmica.

- La **Llei Orgànica 3/2018, del 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD)** adapta el RGPD a l'ordenament espanyol, estableix garanties complementàries i regula drets digitals de la ciutadania, reforçant les obligacions de seguretat que les administracions i empreses han d'aplicar en el tractament de dades personals.
- **L'Estratègia de Ciberseguretat del Sistema Nacional de Salut 2025-2028**, impulsada pel Ministeri de Sanitat i aprovada en el si del Consell Interterritorial del Sistema Nacional de Salut (CISNS), estableix el marc comú d'actuació en matèria de ciberseguretat per al conjunt del SNS, definint els principis, objectius i línies estratègiques dirigits a protegir la informació sanitària, garantir la continuïtat assistencial i reforçar la resiliència del sector davant incidents cibernètics. Reconeixent la sanitat com a sector d'alta criticitat en línia amb la Directiva NIS2, articula la cooperació entre el Ministeri, els serveis de salut autonòmics i els CERT de referència, i constitueix la referència sectorial sobre la qual es projecten les mesures aplicables a l'àmbit sanitari balear, en particular al Servei de Salut de les Illes Balears (IBSALUT).
- La **transposició de la Directiva NIS2**, actualment en fase d'Avantprojecte de Llei, suposarà una ampliació significativa de les obligacions en matèria de governança de la ciberseguretat, gestió del risc, notificació d'incidents i supervisió, afectant tant operadors de serveis essencials com un nombre considerablement major d'entitats públiques i privades. Aquesta Estratègia es concep amb vocació d'anticipar i facilitar l'adaptació de l'ecosistema balear a les noves exigències que derivaran d'aquesta transposició.

02

Diagnòstic balear: situació actual

Les Illes Balears, en el seu compromís per consolidar un entorn digital segur per a la ciutadania, les empreses i l'administració pública, s'enfronten a un context marcat per una creixent digitalització dels serveis i per un ecosistema tecnològic en ràpida evolució. En aquest escenari, la ciberseguretat s'ha convertit en un element essencial per garantir la continuïtat, la qualitat i la confiança en els sistemes digitals que sustenten l'activitat econòmica, social i administrativa de l'arxipèlag, tal com ja recollia l'estratègia balear prèvia.

2.1

Context balear d'amenaces i exposició

Alineat amb altres comunitats autònomes que han desenvolupat enfocaments, les Illes Balears han avançat en els darrers anys en iniciatives de reforç institucional, capacitats tècniques i col·laboració amb agents clau de l'ecosistema regional.

Aquest diagnòstic sintetitza la situació actual de la ciberseguretat a la regió, identificant les principals tendències d'amenaces, el grau d'exposició del territori i l'estat de maduresa de l'administració i de l'ecosistema regional. El seu propòsit és oferir una visió clara i equilibrada del punt de partida, com a base per orientar les línies estratègiques que es desenvoluparan a continuació, alineat amb la realitat balear i amb les necessitats presents i futures del territori.

La creixent digitalització dels serveis públics, les empreses i la ciutadania a les Illes Balears ha vingut acompanyada d'un augment sostingut dels incidents reportats i del volum d'activitat delictiva en l'entorn digital. A data d'elaboració d'aquest document, les dades disponibles evidencien un creixement sostingut de la cibercriminalitat que afecta de forma directa el territori balear. Segons l'Informe sobre la Cibercriminalitat a Espanya 2024 del Ministeri de l'Interior, els fets coneguts van assolir els 464.801 el 2024, representant el 18,9 % del total d'infraccions penals —pràcticament el doble que el 2019 (9,9 %)—, amb el frau informàtic com a tipologia àmpliament dominant (88,8 %). En paral·lel, els incidents de nivell alt o superior en operadors de serveis essencials gairebé es van duplicar en un sol any, passant de 81 el 2023 a 160 el 2024. Les Illes Balears, amb una economia altament digitalitzada i dependent del sector serveis, no són alienes a aquesta realitat, cosa que reforça la urgència de les mesures contemplades en aquesta Estratègia.

Aquest creixement respon a la confluència de diversos factors estructurals:

- L'adopció accelerada de serveis digitals per part de ciutadania, empreses i administració ha ampliat significativament la superfície d'exposició.
- La interconnexió creixent entre sistemes públics i privats ha multiplicat els vectors d'atac disponibles.
- L'obsolescència tecnològica i el deute tècnic acumulat en part de les infraestructures del sector públic i del teixit empresarial, on conviuen sistemes heretats amb arquitectures modernes, generant entorns heterogenis difícils de protegir de forma homogènia.
- La major capacitat de detecció i denúncia per part de ciutadania i organitzacions.

Tots aquests factors completen un escenari en el qual el volum d'incidents registrats reflecteix tant l'augment real de l'amenaça com una major maduresa en la seva identificació.

Més enllà d'aquests factors compartits amb la resta de l'Estat, les Illes Balears presenten particularitats que configuren un perfil de risc propi:

- La condició insular de l'arxipèlag implica una dependència crítica de les infraestructures de connectivitat i comunicacions que enllacen les quatre illes principals, la interrupció de les quals tindria un impacte amplificat respecte a territoris peninsulars.

- El pes del sector turístic, que representa més d'un terç del PIB regional, genera una superfície d'atac que fluctua amb l'estacionalitat: durant els mesos de més afluència, el volum de transaccions digitals, dispositius connectats i dades personals en circulació es multiplica, exposant al territori a pics de risc que requereixen capacitats de resposta escalables.

- L'existència d'un teixit productiu dominat per pimes i micropimes amb recursos limitats per invertir en ciberseguretat, que operen en sectors (hostaleria, comerç, logística, serveis) on la dependència digital és alta i la maduresa en protecció freqüentment baixa.

En aquest context, el territori es veu afectat tant per campanyes d'abast estatal (incloent-hi atacs de *ransomware* dirigits a organismes públics i empreses, campanyes de *phishing* cada vegada més sofisticades i explotació de vulnerabilitats en serveis exposats) com per riscos associats a l'adopció accelerada de tecnologies emergents el desplegament de les quals no sempre va acompanyat de les mesures de seguretat adequades.

El panorama resultant és el d'un entorn dinàmic i en evolució, amb reptes assumibles però que exigeixen reforçar de forma decidida les capacitats de prevenció, detecció i resposta, la cultura de seguretat en tots els nivells i la coordinació institucional entre els actors del territori, en línia amb el que ja anticipava la primera Estratègia Balear de Ciberseguretat i el plantejament del Centre Balear de Ciberseguretat..

2.2

Estat actual i evolució de la ciberseguretat en l'ecosistema balear

L'ecosistema balear de ciberseguretat ha experimentat en els últims anys un avenç progressiu que abasta l'administració pública, el teixit empresarial i la ciutadania, tot i que amb graus de maduresa desiguals. Les Illes Balears parteixen avui d'un conjunt de fortaleses que permeten abordar el desenvolupament d'aquesta Estratègia des d'una base sòlida, però també de mancances que cal identificar amb claredat per orientar adequadament les prioritats d'actuació.

En l'àmbit de l'Administració pública, l'evolució de les capacitats ha estat gradual i sostinguda, amb fites institucionals que han anat consolidant una base cada vegada més robusta. El primer pas rellevant es va produir el 2018, amb l'aprovació del Decret 2/2018, que va establir la Política de Seguretat de la Informació de l'IBSALUT, alineada amb l'ENS i orientada a definir responsabilitats, objectius i una estructura organitzativa específica per a la protecció dels sistemes sanitaris. Aquest marc formal va ser el punt de partida per al desenvolupament de capacitats avançades, com el SOC 24x7 i l'alt nivell de compliment ENS assolit pel sector sanitari, que constitueix avui una de les referències més madures de l'ecosistema públic balear.

Posteriorment, el 2022, la presentació de la primera Estratègia Balear de Ciberseguretat va marcar un salt qualitatiu en plantejar la creació del Centre Balear de Ciberseguretat, la contractació d'un SOC regional —actualment en fase d'implementació—, la definició de polítiques comunes i la coordinació activa amb el CCN i INCIBE.

En l'àmbit sanitari, el Pla Estratègic de Salut Digital 20252029 va reforçar encara més la centralitat de la ciberseguretat dins de la transformació digital assistencial, articulant projectes vinculats a la governança de la dada, la interoperabilitat, la intel·ligència artificial i la teleassistència.

La creació el novembre de 2025 de la Càtedra de Ciberseguretat amb la UIB, concebuda per impulsar la formació especialitzada, la recerca aplicada i la transferència de coneixement, i l'aprovació el desembre de 2025 dels estatuts de l'Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions (IB Digital) com a organisme autònom amb el mandat de concentrar els recursos tecnològics del Govern, han completat un cicle institucional que situa l'Administració balear en una posició de partida significativament més sòlida que la de tot just uns anys enrere.

No obstant això, la maduresa en ciberseguretat dins del mateix sector públic presenta diferències rellevants. Mentre que l'àmbit sanitari i els serveis centrals del Govern han assolit nivells de protecció significatius, els consells insulars i bona part dels ajuntaments de l'arxipèlag disposen de capacitats tècniques i recursos humans considerablement més limitats, la qual cosa genera una protecció heterogènia al territori i reforça la necessitat d'un model de serveis compartits que garanteixi un nivell de seguretat homogeni en tota l'Administració pública local, afavorint un ús més eficient dels recursos públics i una major sostenibilitat del model de prestació de serveis digitals en el temps.

A l'àmbit empresarial, el panorama reflecteix la realitat d'un territori el teixit productiu del qual està dominat per pimes i micropimes que operen en sectors d'alta exposició digital amb nivells de maduresa en ciberseguretat generalment baixos. La majoria d'aquestes empreses no tenen personal especialitzat, polítiques formalitzades de seguretat i capacitat per invertir de forma significativa en protecció digital. Les iniciatives de conscienciació i suport impulsades des d'INCIBE i des del mateix ecosistema balear (a través de la Fundació Bit, les cambres de comerç i les associacions empresarials) han contribuït a elevar la sensibilització, però la bretxa entre el nivell d'amenaça al qual s'enfronta el teixit productiu i la seva capacitat real de resposta continua sent considerable, especialment en les empreses de menor grandària. L'estacionalitat turística agreuja aquesta situació, en generar pics d'activitat digital durant els quals moltes empreses operen amb personal temporal i sistemes no sempre adequadament protegits.

En l'àmbit de la ciutadania, la societat balear presenta un perfil altament digitalitzat, amb taxes elevades d'ús de serveis en línia, administració electrònica, comerç digital i xarxes socials. No obstant això, aquesta elevada connectivitat no sempre va acompanyada d'hàbits de seguretat digital adequats. Les estafes online, el phishing i la suplantació d'identitat afecten de forma creixent la ciutadania, amb especial incidència en col·lectius més vulnerables com la gent gran, els joves i els usuaris amb baixa alfabetització digital. Les accions de sensibilització desenvolupades fins ara han assegut una primera base, però la cultura de ciberseguretat en la ciutadania balear es troba encara en una fase incipient que requereix un esforç sostingut, continuat i adaptat als diferents perfils de la població.

En conjunt, l'ecosistema balear de ciberseguretat es troba en un moment d'inflexió: l'Administració ha fet passos institucionals rellevants que proporcionen una base organitzativa sòlida, però tant el teixit empresarial com la ciutadania necessiten un impuls decidit per elevar el seu nivell de protecció i conscienciació. Aquesta Estratègia parteix precisament d'aquesta diagnosi per articular actuacions que cobreixin els tres àmbits de forma equilibrada i coordinada.

2.3

Capacitats sòlides, resposta fragmentada: el repte balear

L'estat actual de la ciberseguretat a les Illes Balears reflecteix un recorregut sòlid però desigual. L'última dècada ha consolidat capacitats reals que situen la comunitat autònoma en una posició de partida favorable. Tanmateix, aquestes capacitats s'han desenvolupat de forma fragmentada, amb nivells de maduresa heterogenis entre administracions, dependències funcionals dispars i un teixit empresarial —majoritàriament pime i altament exposat al sector turístic— amb un grau de protecció molt desigual.

D'aquest diagnòstic es desprèn la necessitat de transitar d'un model de capacitats fragmentades a un model de resiliència coordinada: articular, escalar i projectar el ja construït sota una governança única, amb una visió territorial comuna i una capacitat de protecció, detecció i resposta homogènia per a Govern, consells, ajuntaments, empreses i ciutadania. L'experiència acumulada confirma a més que l'eficàcia d'aquest tipus d'instruments no depèn tant de l'amplitud del seu catàleg com de la seva capacitat d'execució real i de la seva adaptació al context territorial.

Per tot això es fa necessària una Estratègia Balear de Ciberseguretat pròpia, amb un enfocament diferencial basat en l'especialització sectorial, la proximitat al territori, els serveis compartits i la prioritat a l'execució sobre la teoria, capaç de donar resposta efectiva a les particularitats i a les necessitats reals de l'arxipèlag.

03

Missió, visió, valors i eixos estratègics

3.1

Missió

L'Estratègia Balear de Ciberseguretat, té com a propòsit reforçar la resiliència digital del territori mitjançant un model de governança sòlid i coordinat que garanteixi la protecció dels serveis públics, elevi la maduresa del teixit empresarial davant de les ciberamenaces i impulsi una cultura de seguretat digital en el conjunt de la ciutadania.

Per a això, l'Estratègia s'orienta a la provisió de capacitats i serveis de ciberseguretat concrets, a l'acompanyament operatiu de les administracions, les empreses (especialment pimes i micropimes) i la ciutadania, i a la generació d'un impacte real i mesurable en la capacitat de prevenció, detecció, resposta i recuperació del territori davant d'incidents de ciberseguretat.

El seu objectiu és consolidar capacitats avançades de prevenció, detecció i resposta, promoure la recerca, la innovació i el talent en ciberseguretat, i donar suport especialment a les pimes i als col·lectius més vulnerables, alineant-se amb els marcs nacionals i europeus per construir un entorn digital segur, confiable i sostenible a les Illes Balears.

3.2

Visió

Convertir les Illes Balears en un territori referent en ciberresiliència, en el qual una Administració pública protegida per un model robust i homogeni de seguretat digital garanteixi serveis confiables i alineats amb els estàndards nacionals i europeus; un teixit empresarial preparat i competitiu operi en un entorn digital segur, amb capacitat per prevenir, resistir i recuperar-se dels ciberincidents; i una ciutadania formada i conscient dels riscos digitals es desenvolupa amb confiança en l'espai digital.

Aquesta visió se sustenta en un ecosistema de coneixement i innovació —articulat al voltant de la UIB, la Fundació Bit, DIHBAITUR i altres agents del territori— capaç de generar talent, recerca i solucions avançades, i en un model de coordinació integral que consolidi les Illes Balears com un territori digital segur, innovador i preparat per als desafiaments del futur. La singularitat de l'arxipèlag balear —amb una economia en la qual cobra gran rellevància el turisme, una administració distribuïda per illes i un teixit productiu compost majoritàriament per pimes— posiciona les Illes Balears com un laboratori natural de ciberresiliència en entorns insulars i turístics, capaç de generar solucions, models i bones pràctiques transferibles a altres territoris amb característiques similars.

En aquest sentit, l'Estratègia Balear de Ciberseguretat es configura com l'instrument director que permetrà articular, de forma ordenada i sostinguda, les capacitats, recursos i actuacions necessàries per fer efectiva aquesta visió. A través dels seus eixos estratègics, objectius i línies d'actuació, l'Estratègia estableix el marc de referència per reforçar la governança de la ciberseguretat en l'Administració, impulsar el desenvolupament d'un ecosistema empresarial i innovador propi, i construir una cultura de seguretat digital estesa al conjunt de la societat balear. La seva vocació és servir de full de ruta compartit entre institucions, empreses, agents de coneixement i ciutadania, assegurant que la ciberseguretat s'integri com un element estructural de la transformació digital del territori i no com una resposta puntual a incidents o amenaces.

TERRITORI DIGITAL SEGUR

3.3

Valors

La ciberseguretat no és responsabilitat exclusiva d'un únic actor. En un territori insular, altament digitalitzat i interconnectat com les Illes Balears, la protecció de l'espai digital requereix la implicació activa i coordinada de tots els col·lectius: administracions públiques, empreses, agents de coneixement i ciutadania. Tots formen part d'un ecosistema digital compartit en el qual la seguretat és una responsabilitat col·lectiva.

Sobre aquesta premissa, es defineixen els principis rectors que han de guiar el desenvolupament, l'execució i l'evolució d'aquesta Estratègia. Aquests principis es formulen en coherència amb el marc de sostenibilitat institucional promogut pel Govern a través del Pacte Social i Polític per a la Sostenibilitat Econòmica, Social i Ambiental de les Illes Balears, incorporant la resiliència, l'eficiència en l'ús dels recursos públics i la governança col·laborativa com a fonaments del desplegament de la ciberseguretat al territori. En coherència amb aquest enfocament, l'Estratègia s'articula al voltant dels principis següents:

Corresponsabilitat i col·laboració

La ciberseguretat efectiva només és possible mitjançant la col·laboració entre tots els actors del territori. L'Estratègia promou models de cooperació entre administracions públiques, empreses, universitats i organismes de referència nacionals i internacionals, amb l'objectiu de construir capacitats compartides que cap actor pot desenvolupar de forma aïllada. En un arxipèlag on la condició insular amplifica la interdependència entre sistemes i organitzacions, la cooperació no és una opció sinó una necessitat estructural.

Transversalitat de la ciberseguretat

La ciberseguretat s'ha d'integrar com un element estructural de la transformació digital, no com una capa afegida a posteriori. Aquest principi exigeix que la seguretat s'incorpori des del disseny en tots els serveis digitals, polítiques públiques i processos d'innovació, garantint la confidencialitat, integritat i disponibilitat de la informació i anticipant els riscos derivats de tecnologies emergents com la intel·ligència artificial, la computació al núvol o l'Internet de les Coses.

Orientació a resultats i pragmatisme

L'Estratègia es guia per un enfocament pragmàtic i orientat a resultats, prioritzant aquelles actuacions que generin un impacte real i verificable en la millora de la ciberseguretat del territori. Aquest principi impulsa l'adopció de solucions simples, eficaces i properes a la realitat de les administracions, les empreses i la ciutadania, afavorint la utilitat pràctica, l'execució progressiva i l'obtenció de beneficis tangibles davant de plantejaments excessivament complexos o merament teòrics.

Resiliència i continuïtat

L'objectiu no és només prevenir els ciberincidents, sinó garantir la capacitat de detectar-los amb rapidesa, respondre de forma eficaç i recuperar l'operativitat en el menor temps possible. Aquest principi orienta l'Estratègia envers el reforç de la continuïtat dels serveis públics essencials, la protecció de les infraestructures crítiques i la millora contínua de les capacitats de resposta a tot el territori, amb especial atenció a la dependència de les infraestructures de connectivitat que enllacen les quatre illes. L'Estratègia incorpora, a més, mecanismes de seguiment, avaluació i revisió periòdica que garanteixin la seva vigència i permetin incorporar lliçons apreses, ajustar prioritats i respondre a canvis en l'entorn d'amenaces, l'evolució tecnològica i el marc regulatori de forma àgil.

Serveis públics segurs i de confiança

L'Administració balear ha de garantir que els serveis digitals que presta a la ciutadania i a les empreses són segurs, fiables i conformes amb els estàndards nacionals i europeus. Aquest principi impulsa l'evolució cap a una Administració que no només protegeix els seus sistemes, sinó que genera confiança activa en l'ús dels serveis públics digitals, alineant-se amb els requisits de l'ENS, la NIS2 i les guies CCN-STIC.

Protecció de la ciutadania i atenció a col·lectius vulnerables

L'Estratègia situa les persones al centre de la ciberseguretat. Això implica promoure una cultura de seguretat digital accessible per a tots els perfils de la societat balear, amb especial atenció als col·lectius més exposats —persones grans, joves i usuaris amb baixa alfabetització digital—, garantint que ningú quedi al marge de la protecció en l'entorn digital.

Proporcionalitat, adaptació al territori i impuls del coneixement

Les mesures de ciberseguretat han de ser proporcionades al nivell de risc, a la capacitat de cada actor i a les particularitats del teixit socioeconòmic balear. En un territori on les pimes i micropimes representen la immensa majoria del teixit productiu i on les administracions locals disposen de recursos limitats, l'Estratègia aposta per un model d'actuació gradual, accessible i escalable que permeti a cada organització avançar des del seu nivell de partida. Perquè aquest model sigui sostenible, resulta imprescindible comptar amb un ecosistema capaç de generar coneixement propi, formar professionals especialitzats i desenvolupar solucions avançades adaptades al territori, impulsant la col·laboració amb la UIB, la Fundació Bit, DIHBAITUR i altres agents d'innovació per convertir la ciberseguretat en un vector de desenvolupament econòmic i tecnològic de l'arxipèlag.

3.4

Eixos

Prenent com a punt de partida la missió, la visió i els principis rectors definits en els apartats anteriors, l'Estratègia Balear de Ciberseguretat estableix una sèrie d'objectius estratègics orientats a fer efectiva la seva implantació. Aquests objectius s'estructuren en tres eixos complementaris que, de forma conjunta, permeten abordar les necessitats específiques dels diferents col·lectius i àmbits d'actuació de les Illes Balears:

- Administració Digital ciberresilient i de referència.
- Ecosistema ciber-balear: empresa, innovació i talent.
- Societat balear cibersegura.

EIX 1

Administració Digital ciberreselient i de referencia

OBJECTIU 1

MARC DE GOVERNANÇA EN L'ADMINISTRACIÓ

Línia d'Actuació 1
Evolució del model governança de la ciberseguretat en l' Administració

OBJECTIU 2

RESILIENCIA EN SERVEIS PÚBLICS

Línia d'Actuació 2
Reforçar capacitats de prevenció, detecció i resposta

Línia d'Actuació 3
Protecció 'infraestructures i serveis

Línia d'Actuació 4
Adaptació a riscos emergents i noves tecnologies

OBJECTIU 3

COL-LABORACIÓ INSTITUCIONAL

Línia d'Actuació 5
Marcs de cooperació institucional

OBJECTIU 4

POSICIONAMENT ILLES BALEARS

Línia d'Actuació 6
Participació en xarxes, forums i espais de col laboració

EIX 2

EcoCiber balear: empresa, innovació i talent

OBJECTIU 5

INDÚSTRIA BALEAR DE CIBERSEGURETAT

Línia d'Actuació 7
Plans de desenvolupament d'indústria ciberseguretat

Línia d'Actuació 8
Dinamització empresarial i cooperació públic-privada

OBJECTIU 6

RECERCA I INNOVACIÓ EN CIBERSEGURETAT

Línia d'Actuació 9
Impuls de programes R+D+| en col-laboració amb centres de referència

OBJECTIU 7

ATRAURE, GENERAR I RETENIR CIBERTALENT

Línia d'Actuació 10
Elaboració de plans formatius per a la generació de talent

Línia d'Actuació 11
Impuls d'iniciatives d'atracció i retenció de talent

EIX 3

Societat balear cibersegura

OBJECTIU 8

CIBERRESILIENCIA TEIXIT EMPRESARIAL

Línia d'Actuació 12
Programes per a la millora de les capacitats en ciberseguretat en el teixit empresarial

OBJECTIU 9

CULTURA SOLIDA EN CIBERSEGURETAT

Línia d'Actuació 13
Promoció de la conscienciació i bones práctiques de ciberseguretat a la ciutadania balear

EIX 1

Administració Digital ciberresilient i de referència

Aquest eix orienta els esforços cap a la consolidació d'una Administració balear més segura, cohesionada i preparada davant de ciberamenaces, posicionant el sector públic autonòmic com a referent en protecció digital dins del panorama nacional.

Es fonamenta en la creació d'un marc robust de governança, liderat pel Centre Balear de Ciberseguretat i concebut explícitament com un habilitador de l'acció perquè estableixi criteris homogenis, rols clars i mecanismes de coordinació entre tots els nivells de l'Administració —Govern, Consells Insulars, ajuntaments i FFCSE—, amb l'objectiu de facilitar la presa de decisions, prioritzar actuacions i accelerar la implantació efectiva de mesures de protecció, afavorint un ús més eficient i sostenible dels recursos públics i no com un fi en si mateix.

Així mateix, impulsa la resiliència dels serveis públics, reforçant la capacitat d'anticipació, detecció, resposta i recuperació davant incidents, recolzant-se en capacitats centralitzades com el monitoratge continu, l'alerta primerenca, el suport operatiu i la planificació de la continuïtat. Aquest eix integra també la capacitat d'anticipació davant de riscos emergents i tecnologies disruptives, assegurant que l'Administració no només reaccioni davant d'amenaces conegudes, sinó que identifiqui tendències incipients i adapti les seves polítiques i controls de forma proactiva.

L'eix abasta igualment la col·laboració institucional com a palanca estratègica, consolidant la presència de les Illes Balears en xarxes, fòrums i espais de cooperació nacionals i internacionals que reforcin el seu posicionament i permetin l'intercanvi de coneixement, intel·ligència d'amenaces i bones pràctiques. El seu abast s'estén al conjunt de l'Administració autonòmica — Conselleries, ens instrumentals del sector públic (organismes autònoms, empreses públiques, fundacions i consorcis), Consells Insulars i ajuntaments—, prestant especial atenció a aquells àmbits i entitats amb menors recursos i capacitats pròpies, tots ells considerats agents essencials per al desplegament i implementació efectiva d'aquesta Estratègia.

Aquest eix reconeix la necessitat de reforçar el posicionament de la Comunitat Autònoma en l'ecosistema nacional de ciberseguretat, impulsant programes que facilitin l'accés de les empreses balears a ajudes, incentius i mecanismes de suport a la inversió en solucions i serveis de ciberseguretat, així com l'extensió de serveis compartits de ciberseguretat a Consells Insulars i ajuntaments, per tal de garantir un nivell de protecció homogeni i sostenible a tot el territori.

La seva finalitat és garantir una Administració sòlida, coordinada i de referència, capaç d'operar de manera segura i confiable, alineada amb els estàndards nacionals i europeus (ENS, CCN-STIC, NIS2) i preparada per afrontar els desafiaments d'un entorn digital en constant evolució.

EIX 2

Ecosistema ciber-balear: empresa, innovació i talent

Aquest eix s'adreça a impulsar la creació i consolidació d'un ecosistema propi de ciberseguretat a les Illes Balears, capaç de generar activitat econòmica, coneixement avançat i professionals especialitzats que reforcin la posició competitiva del territori.

Parteix de la convicció que la ciberseguretat no és únicament una necessitat defensiva, sinó també una oportunitat de desenvolupament econòmic i tecnològic. El creixement sostingut de la demanda de solucions i serveis de ciberseguretat, unit a l'elevada exposició digital de l'arxipèlag —amb un sector turístic que representa més d'un terç del PIB i un teixit productiu compost majoritàriament per pimes—, configura un entorn propici per al sorgiment d'empreses especialitzades, l'atracció d'inversió i l'especialització sectorial de l'ecosistema ciber-balear en aquells àmbits on el territori presenta majors fortaleses i necessitats específiques, afavorint un model de creixement basat en el coneixement i sostenible en el temps.

En aquest sentit, el sector turístic s'identifica de forma explícita com a focus prioritari d'especialització, juntament amb altres àmbits estratègics vinculats a la realitat insular, com la logística portuària i marítima, el sector nàutic, la salut i els serveis intensius en digitalització. L'Estratègia contempla el desenvolupament progressiu de subprogrames sectorials de ciberseguretat, orientats a abordar els riscos específics d'aquests àmbits i a afavorir la generació de solucions adaptades, escalables i amb potencial de transferència a altres territoris amb característiques similars.

L'eix s'articula al voltant de tres dimensions complementàries. En primer lloc, el desenvolupament d'una indústria balear de ciberseguretat, impulsant la creació, consolidació i creixement d'empreses proveïdores de solucions i serveis, i afavorint l'articulació d'un ecosistema competitiu, innovador i connectat amb altres pols de referència nacionals i internacionals mitjançant iniciatives de dinamització empresarial i cooperació públic-privada. En segon lloc, el foment de la recerca i la innovació, promovent programes d'R+D+I i transferència de coneixement en col·laboració amb la UIB, la Fundació Bit, DIHBAI-TUR i altres agents del sistema d'innovació balear, amb una orientació prioritària cap a l'aplicació pràctica, la resolució de reptes reals del teixit productiu i la generació d'impacte econòmic. En tercer lloc, la generació, atracció i fidelització de talent especialitzat, mitjançant el desplegament de programes formatius, el desenvolupament de competències avançades i la posada en marxa d'iniciatives que promoguin itineraris professionals, pràctiques, borses d'ocupació i col·laboració universitat-empresa, integrant la ciberseguretat en els itineraris formatius i en la formació contínua del territori.

L'Estratègia reconeix de forma explícita les dificultats estructurals per a la captació de professorat especialitzat i la necessitat d'articular solucions específiques i realistes que permetin reforçar l'oferta formativa en ciberseguretat, especialment en l'àmbit de la Formació Professional. En aquest context, la Formació Professional Dual s'identifica com un instrument particularment rellevant per al desenvolupament del talent en ciberseguretat, en articular un model d'alternança entre el centre educatiu i l'empresa en el qual l'alumne adquireix competències pràctiques reals en un entorn productiu, amb la participació de l'empresa com a agent formador. La promoció de cicles d'FP Dual vinculats a la ciberseguretat —en coordinació amb centres educatius, empreses del sector i l'Administració— permetrà generar un espai de desenvolupament de professionals amb competències actualitzades i directament aplicables, accelerar la seva inserció laboral i, alhora, reforçar les capacitats de les pròpies empreses participants, que es beneficien del talent format a mida de les seves necessitats. El desenvolupament del talent es concep, així, com un procés progressiu i escalable, alineat amb la capacitat real del territori i amb les necessitats del mercat laboral, garantint la consolidació de capacitats pròpies que reforcin la sostenibilitat de l'ecosistema digital balear.

L'experiència d'altres regions mostra que la consolidació d'un sector de ciberseguretat insular i local -

amb capacitats empresarials, talent qualificat i pols d'innovació— contribueix no només a reforçar la seguretat del territori, sinó també a dinamitzar l'economia mitjançant un mercat en creixement, serveis d'alt valor afegit i empreses capaces de competir a escala nacional i internacional. Seguint aquesta línia, l'eix aspira a posicionar les Illes Balears com un territori que connecta educació, administracions, empreses tecnològiques i ecosistema d'innovació en un circuit continu de coneixement, talent i solucions, projectant l'arxipèlag com a referent en àmbits com la recerca aplicada, la innovació en sectors estratègics i la col·laboració pública-privada en matèria de ciberseguretat, des d'un enfocament realista, progressiu i orientat a l'escalabilitat de l'ecosistema.

Aquest eix reconeix, a més, que la condició insular i turística del territori no és només un repte, sinó un avantatge competitiu diferencial que permet posicionar les Illes Balears com a referent en el desenvolupament de solucions de ciberseguretat aplicades a entorns insulars, turístics i d'alta estacionalitat, reforçant l'especialització sectorial com a element distintiu i estratègic de l'ecosistema ciber-balear.

EIX 3

Societat balear cibersegura

Aquest eix s'orienta a enfortir la protecció i la maduresa digital del teixit empresarial i de la ciutadania, dos pilars essencials per a la resiliència social i econòmica de l'arxipèlag. El seu objectiu és reduir l'exposició al risc, promoure la prevenció i conscienciació davant les ciberamenaces, i reforçar la capacitat de resposta i recuperació davant incidents, consolidant un ús segur, responsable i sostenible de les tecnologies digitals a tot el territori.

A l'àmbit empresarial, l'eix posa el focus en pimes i micropimes —predominants en sectors d'alta exposició digital com turisme, comerç, logística i serveis— que presenten vulnerabilitats significatives davant ciberatacs capaços de comprometre la seva continuïtat operativa i la seva competitivitat. Per revertir aquesta situació, s'impulsa un model de suport progressiu, realista i accessible, basat en sensibilització, diagnòstics lleugers, guies sectorials i acompanyament tècnic especialitzat, tant en fase preventiva com després de l'ocurrència d'incidents. Aquestes actuacions s'articularan des del Centre Balear de Ciberseguretat, en coordinació amb associacions empresarials, cambres de comerç i agents econòmics del territori, per tal d'elevar la maduresa del teixit productiu, facilitar una gestió més eficaç dels incidents de ciberseguretat i reduir de forma sostinguda la seva superfície d'exposició. De forma complementària, l'eix promou una ciutadania balear més preparada i conscient, dotant-la de coneixements, hàbits segurs i recursos pràctics que permetin afrontar amenaces creixents com fraus digitals, suplantacions d'identitat i estafes en línia. Les accions se centraran en programes continuats de sensibilització i formació, amb especial atenció a col·lectius de major vulnerabilitat —persones grans, joves i usuaris amb baixa alfabetització digital—, garantint un enfocament inclusiu que eviti bretxes de protecció i reforci la confiança de la ciutadania en l'entorn digital.

En aquest marc, s'integrarà un punt d'entrada clar i accessible als serveis d'orientació i suport en ciberseguretat, que permeti a les persones afectades rebre informació fiable, pautes d'actuació inicial i derivació als recursos disponibles.

Aquest eix es recolza de manera estructural en la coordinació efectiva amb les Forces i Cossos de Seguretat de l'Estat, reconeixent el seu paper essencial en la investigació i persecució del cibercrim i promovent una col·laboració fluida que faciliti la correcta gestió d'incidents, la preservació d'evidències i l'adequada atenció a les víctimes, sense duplicar les funcions que corresponen als organismes estatals competents.

L'experiència d'altres comunitats autònomes confirma que la conscienciació social i la preparació empresarial són elements essencials per a la resiliència col·lectiva quan es complementen amb capacitats d'acompanyament i resposta. En un territori amb una elevada dependència de serveis digitals i una marcada estacionalitat turística —factors que amplifiquen la superfície d'atac—, aquest eix resulta determinant per reforçar la confiança digital, garantir un ús segur de les tecnologies i consolidar un ecosistema balear més robust davant les ciberamenaces.

04

Objectius estratègics

Els objectius de l'Estratègia Balear de Ciberseguretat constitueixen la concreció operativa del propòsit, la visió i els tres eixos estratègics prèviament definits. La seva formulació permet orientar de manera clara i coherent les capacitats que les Illes Balears han de desenvolupar per enfortir la protecció del territori insular davant d'amenaces cada vegada més sofisticades, garantint un marc d'actuació coordinat, eficient i alineat amb les directrius estatals i europees.

En aquest context, els objectius es presenten com els pilars fonamentals que guiaran la creació i desplegament d'estructures com el Centre Balear de Ciberseguretat, així com l'articulació de polítiques, mecanismes de coordinació i serveis essencials que permetin complir adequadament amb les responsabilitats en matèria de ciberseguretat.

Així mateix, els objectius d'aquesta Estratègia s'alineen de forma directa amb els del Pacte Social i Polític per la Sostenibilitat Econòmica, Social i Ambiental de les Illes Balears, tant en la seva dimensió estratègica com de desenvolupament.

En particular, l'Estratègia contribueix a l'articulació d'un ecosistema d'innovació i clústers tecnològics, a la promoció d'una transformació digital segura, a la reducció de la bretxa digital des del vessant de la ciberseguretat, a la millora integral de la ciberseguretat i la protecció de dades —objectiu per al qual aquesta Estratègia constitueix l'instrument principal de resposta— , i a l'increment de la inversió en R+D en ciberseguretat. De la mateixa manera, apuntala els objectius de desenvolupament del Pacte relatius a la millora de les infraestructures TIC, la formació en tecnologies emergents, l'establiment d'una estratègia regional de digitalització segura, la innovació tecnològica aplicada al turisme regeneratiu i la protecció dels sistemes de monitoratge ambiental basats en tecnologies digitals.

D'aquesta manera, la ciberseguretat es configura com un habilitador transversal del conjunt de l'agenda d'innovació i digitalització del territori.

EIX 1

Administració Digital ciberresilient i de referència

Objectiu 1

Establir un marc robust i efectiu de governança de la ciberseguretat

DESCRIPCIÓ

L'Administració balear necessita un model de governança que unifiqui criteris, responsabilitats i mecanismes de coordinació en matèria de ciberseguretat. La creació del Centre Balear de Ciberseguretat, contemplada dins la visió institucional, i la recent constitució de l'Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions (IB Digital) com a organisme autònom, ofereixen l'oportunitat d'estructurar un sistema coherent en el qual els diferents actors públics treballin sota una direcció estratègica comuna.

Un marc de governança efectiu permetrà alinear polítiques, optimitzar recursos, millorar la coordinació entre els organismes de la Comunitat Autònoma i assegurar una presa de decisions més informada i consistent. Les experiències d'altres regions demostren que l'existència d'un model clar de governança (amb òrgans definits, funcions assignades i periodicitat establerta) impulsa la supervisió, la cooperació interadministrativa i la capacitat per implantar mesures de seguretat de forma homogènia, afavorint un ús eficient i sostenible dels recursos públics.

Aquest objectiu inclou, a més, la definició de marcs estables de coordinació i cooperació entre les institucions públiques de les Illes Balears i els organismes nacionals i internacionals competents, assegurant que la interlocució amb el CCN, INCIBE i les estructures europees de ciberseguretat es realitzi de forma planificada, contínua i alineada amb els objectius estratègics del territori.

RESULTATS ESPERATS

01 **Un model de governança formalitzat i aprovat que estableixi de manera clara els òrgans responsables, les seves funcions i la forma en què es coordinen entre si i amb el Centre Balear de Ciberseguretat.**

02 **Marc normatiu i procedimental homogeni, assegurant que totes les entitats del sector públic autonòmic apliquen criteris comuns de seguretat, conformes amb l'ENS, la NIS2 i les guies CCN-STIC.**

03 **Òrgans de coordinació plenament operatius entre el Govern, els consells insulars, els ajuntaments, FFCCSE i els organismes públics, permetent una supervisió contínua i una resposta coordinada davant incidents.**

04 **Capacitat reforçada de supervisió i control, que inclogui mètriques estratègiques, gestió integral del risc, seguiment de compliment regulatori i avaluació periòdica de maduresa.**

05 **Major eficiència institucional, reduint duplicitats, optimitzant recursos i facilitant l'adopció de serveis compartits i capacitats centralitzades de seguretat.**

06 **Marcs estables de cooperació amb organismes nacionals i internacionals, garantint una interlocució fluida, planificada i orientada a resultats.**

OBJECTIU 2

Incrementar la resiliència dels serveis públics davant de ciberincidents

DESCRIPCIÓ

Reforçar la resiliència dels serveis públics balears implica millorar la capacitat operativa real de l'Administració per anticipar, detectar, gestionar i recuperar-se de ciberincidents que puguin afectar la prestació de serveis essencials a la ciutadania. La posada en marxa de capacitats i serveis compartits de ciberseguretat, com les funcions de monitoratge i resposta del Centre Balear de Ciberseguretat, permetrà elevar la protecció institucional i oferir un suport més consistent a totes les entitats públiques de l'arxipèlag.

Un model de resiliència sòlid combina procediments unificats, vigilància contínua, capacitat de resposta coordinada i disponibilitat de plans de continuïtat que redueixin l'impacte dels incidents. La integració d'aquests elements, des d'un enfocament eminentment operatiu, permetrà a l'Administració balear prestar serveis més segurs, reduir els temps de resposta i minimitzar interrupcions en escenaris de risc elevat.

Aquest objectiu incorpora així mateix una dimensió anticipatòria: l'evolució constant del panorama de ciberamenaces, unida al ràpid avanç de tecnologies disruptives com la intel·ligència artificial, la computació al núvol, l'IoT o l'automatització, exigeix que l'Administració balear desenvolupi una capacitat anticipatòria sòlida i permanent, que li permeti no només reaccionar davant d'amenaces conegudes, sinó també identificar tendències incipients, avaluar impactes potencials i adaptar les seves polítiques i controls abans que els riscos es materialitzin. Aquest enfocament d'anticipació s'integra plenament en la tasca del Centre Balear de Ciberseguretat, que actuarà com a node de coneixement avançat, integrant intel·ligència d'amenaces, tendències tecnològiques i senyals primerencs rellevants per al territori.

Finalment, aquest objectiu integra l'extensió de serveis compartits de ciberseguretat a consells insulars i ajuntaments, reconeixent que la protecció homogènia de tot el sector públic territorial requereix un model de prestació compartida que optimitzi recursos i garanteixi un nivell de protecció consistent en les quatre illes, assegurant la sostenibilitat del model de prestació dels serveis públics digitals en el temps

RESULTATS ESPERATS

01 **Capacitat de gestió d'incidents reforçada i coherent, amb procediments comuns i una resposta més àgil i coordinada en tot el sector públic autonòmic.**

02 **Serveis i funcions compartides de detecció i resposta plenament operatives, proporcionant suport transversal i elevant la capacitat de protecció del conjunt de l'Administració.**

03 **Serveis públics essencials més protegits, sustentats en mecanismes de continuïtat i recuperació provats i actualitzats i exercitats de forma periòdica.**

04 **Major capacitat d'identificació prematura de riscos emergents, mitjançant vigilància tecnològica contínua, anàlisi de tendències i participació en xarxes d'intercanvi d'informació especialitzades.**

05 **Adaptació àgil de polítiques, controls i capacitats, permetent ajustar les mesures de protecció sense esperar a l'aparició d'incidents significatius.**

06 **Integració de capacitats avançades al Centre Balear de Ciberseguretat, que actuï com a observatori regional i plataforma operativa connectant intel·ligència d'amenaces, evolució tecnològica i anàlisi d'impacte.**

07 **Esquema de serveis compartits formalitzat, que faciliti als consells insulars i als ajuntaments accedir a serveis de ciberseguretat de manera coordinada i amb un nivell de qualitat homogeni.**

08 **Millora real del nivell de protecció en entitats amb menys recursos, gràcies a suport tècnic especialitzat, serveis compartits operatius, accés a alertes i acompanyament efectiu en la gestió de la ciberseguretat.**

OBJECTIU 3

Impulsar la col·laboració institucional per millorar les capacitats de ciberseguretat

DESCRIPCIÓ

La ciberseguretat és, per la seva pròpia naturalesa, una funció que transcendeix les fronteres de qualsevol organització individual. En un territori insular com les Illes Balears, on les infraestructures digitals connecten administracions, empreses i ciutadania en un ecosistema altament interdependent, la col·laboració institucional resulta essencial per construir capacitats que cap actor pot desenvolupar de forma aïllada.

Aquest objectiu persegueix consolidar la presència institucional de les Illes Balears en els principals espais de cooperació en matèria de ciberseguretat, tant a nivell nacional com internacional. Es tracta de garantir una participació i sostinguda en xarxes, fòrums i grups de treball que permetin l'intercanvi de coneixement, intel·ligència d'amenaces, alertes, bones pràctiques i recursos tècnics, reforçant simultàniament el posicionament de l'arxipèlag com a territori de referència.

L'experiència d'altres comunitats autònomes confirma que la participació en estructures cooperatives (com la xarxa nacional de SOCs, els grups de treball del CCN, les iniciatives d'INCIBE o les xarxes europees de CSIRTs) genera beneficis directes: millora la capacitat de detecció i resposta, accelera l'accés a recursos especialitzats, permet l'homologació de procediments i eleva la visibilitat institucional. Per a les Illes Balears, aquesta dimensió col·laborativa adquireix una rellevància singular atesa la seva condició insular, que converteix la connectivitat i la cooperació en actius estratègics de primer ordre.

RESULTATS ESPERATS

01 **Participació i estable de les Illes Balears en xarxes nacionals i internacionals de ciberseguretat, amb presència consolidada en els fòrums i grups de treball de major rellevància estratègica.**

02 **Canals formals de coordinació amb organismes nacionals especialitzats (CCN, INCIBE) i internacionals (ENISA, xarxes europees de CSIRTs), que garanteixin un flux continu d'informació, alertes i recursos tècnics.**

03 **Integració del Centre Balear de Ciberseguretat a la xarxa nacional de SOCs i en les iniciatives de compartició d'intel·ligència d'amenaces, elevant les capacitats operatives del territori.**

04 **Acords de col·laboració públic-privada que permetin compartir informació rellevant, capacitats tècniques i experiència especialitzada en matèria de ciberseguretat.**

05 **Major visibilitat i reconeixement institucional de les Illes Balears com a comunitat autònoma compromesa i activa en l'àmbit de la ciberseguretat.**

06 **Reforç de la cooperació interadministrativa amb consells insulars i ajuntaments, establint mecanismes continus de comunicació, suport tècnic i coordinació operativa.**

OBJECTIU 4

Reforçar el posicionament de les Illes Balears en l'ecosistema nacional de ciberseguretat

DESCRIPCIÓ

Més enllà de la protecció interna dels seus sistemes i serveis, les Illes Balears han de projectar el seu compromís amb la ciberseguretat com un element diferenciador que reforci la seva posició en l'ecosistema nacional. Això implica no només desenvolupar capacitats pròpies, sinó també facilitar que les empreses del territori accedeixin als instruments de suport disponibles per millorar la seva seguretat digital, i posicionar la Comunitat Autònoma com un interlocutor rellevant en les polítiques nacionals de ciberseguretat.

Aquest objectiu es materialitza mitjançant el desenvolupament de programes que impulsin i facilitin la inversió en ciberseguretat per part del teixit empresarial balear, facilitant l'accés a ajudes, incentius i mecanismes de suport procedents tant de la pròpia Comunitat Autònoma com de fons estatals i europeus. En un arxipèlag on les pimes i micropimes representen la immensa majoria del teixit productiu, la capacitat de canalitzar recursos financers cap a la millora de la seguretat digital constitueix un element clau de competitivitat i resiliència territorial.

Així mateix, el posicionament en l'ecosistema nacional requereix que la Comunitat Autònoma sigui capaç d'articular la seva oferta de capacitats, demostrar el seu compromís institucional i participar activament en les decisions estratègiques que s'adoptin a nivell estatal en matèria de ciberseguretat, establint les Illes Balears com un territori de referència i un soci fiable en la construcció d'una Espanya digitalment segura.

RESULTATS ESPERATS

01 **Programes operatius d'impuls i finançament de la ciberseguretat a les empreses balears, amb mecanismes clars d'accés a ajuts, incentius i suport a la inversió.**

02 **Major capacitat de captació de fons estatals i europeus destinats a ciberseguretat, optimitzant la participació en convocatòries i programes competitius.**

03 **Increment significatiu de la inversió en ciberseguretat per part de les pimes i micropimes balears, elevant el nivell de protecció del teixit productiu.**

04 **Posicionament reconegut de les Illes Balears com a comunitat autònoma activa i compromesa en l'ecosistema nacional de ciberseguretat.**

05 **Articulació d'una interlocució estable i propositiva amb els organismes nacionals competents, contribuint a les polítiques i decisions estratègiques de l'Estat en aquesta matèria.**

EJE 2

EcoCiber balear: empresa, innovació i talent

OBJECTIU 5

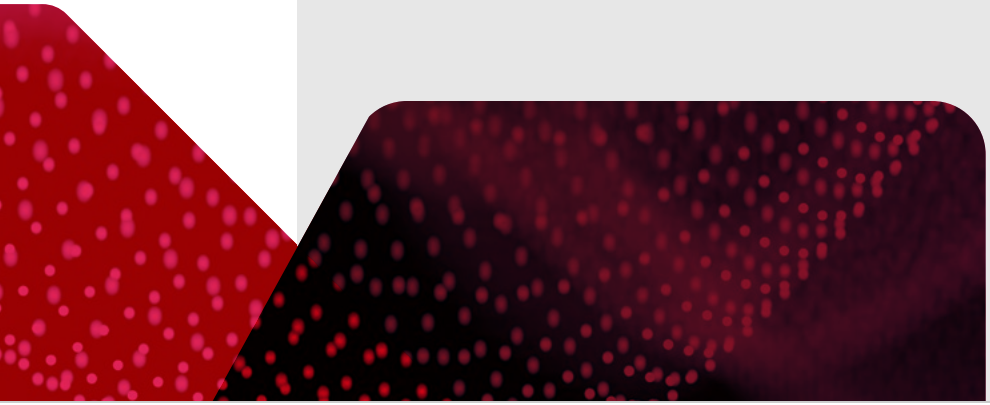
Potenciar el desenvolupament d'una indústria de ciberseguretat a les Illes Balears

DESCRIPCIÓ

El desenvolupament d'un sector industrial de ciberseguretat propi constitueix una oportunitat estratègica per a les Illes Balears. El creixement sostingut de la demanda de solucions i serveis de protecció digital, impulsat tant per l'enduriment regulatori europeu (NIS2, DORA, Cybersecurity Act) com per la creixent sofisticació de les amenaces, configura un mercat en expansió que l'arxipèlag pot aprofitar per diversificar la seva base econòmica i generar activitat d'alt valor afegit.

Aquest objectiu persegueix impulsar la creació, consolidació i creixement d'empreses proveïdores de solucions i serveis de ciberseguretat a les Illes Balears, afavorint l'articulació d'un ecosistema empresarial competitiu, innovador i connectat amb altres pols de referència nacionals i internacionals. El seu abast abasta des del suport a l'emprenedoria tecnològica i la maduració de startups, fins a la dinamització d'empreses ja existents i l'atracció de companyies especialitzades que considerin l'arxipèlag com a seu d'operacions o centre de desenvolupament.

La condició insular i turística del territori, lluny de suposar únicament un repte, ofereix un entorn diferenciat per al desenvolupament de solucions de ciberseguretat en àmbits amb alta demanda i escassa oferta especialitzada: protecció del sector hoteler i de serveis turístics, seguretat en entorns Smart, protecció d'infraestructures distribuïdes entre illes o ciberseguretat aplicada a la logística i el transport interinsular. Aquests nínxols converteixen l'arxipèlag en un laboratori natural de ciberresiliència insular i turística, amb capacitat per desenvolupar solucions exportables i posicionar les Illes Balears com a referent davant territoris amb problemàtiques similars en l'àmbit nacional, europeu i mediterrani.



L'experiència d'altres regions confirma que la consolidació d'un sector local de ciberseguretat requereix combinar instruments de política industrial —plans sectorials, mecanismes de compra pública innovadora, projectes tractors— amb iniciatives de dinamització empresarial i cooperació públic-privada que vertebren l'oferta, connectin els actors de l'ecosistema i facilitin l'accés a mercats i finançament.

RESULTATS ESPERATS

01 **Consolidació d'un teixit empresarial especialitzat en ciberseguretat, amb empreses locals capaces d'oferir serveis i solucions competitives en el mercat nacional i internacional.**

02 **Desenvolupament d'una oferta diferenciada de ciberseguretat en sectors estratègics de l'arxipèlag (turisme, serveis, logística, salut), aprofitant les particularitats del territori com a avantatge competitiu.**

03 **Increment d'iniciatives d'emprenedoria i innovació empresarial en ciberseguretat, impulsades per programes de suport, espais de prova i acompanyament en la maduració de solucions.**

04 **Major capacitat d'atracció d'inversió i d'empreses especialitzades, posicionant les Illes Balears com un territori atractiu per a l'activitat empresarial en ciberseguretat.**

05 **Dinamització de la cooperació publicoprivada com a motor de l'ecosistema, amb mecanismes estables de diálogo, projectes conjunts i compra pública que actúe com a tractora de la indústria local.**

06 **Projecció de les Illes Balears com a pol de referència en ciberseguretat aplicada a entorns turístics, insulars i de serveis, generant visibilitat i reconeixement en xarxes nacionals i europees.**

OBJECTIU 6

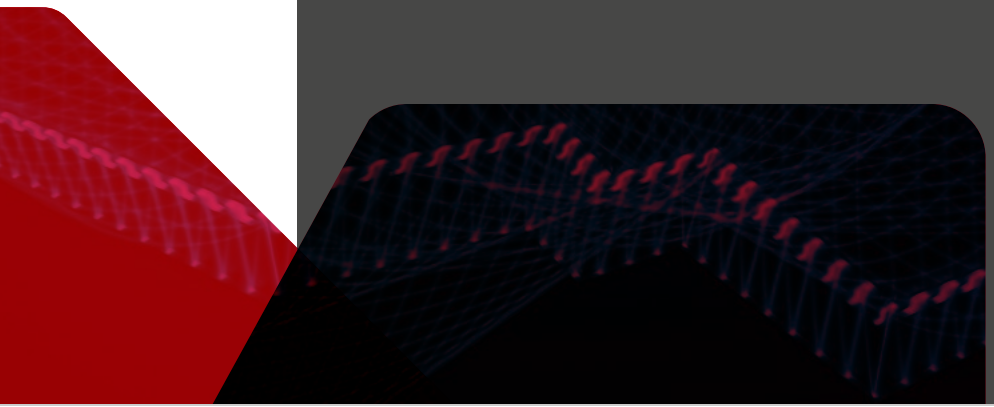
Fomentar la recerca i innovació en ciberseguretat

DESCRIPCIÓ

La consolidació d'un ecosistema de recerca i innovació en ciberseguretat és clau per enfortir la posició de les Illes Balears com un territori competitiu, segur i capaç d'anticipar desafiaments tecnològics. L'impuls a la col·laboració amb la Universitat de les Illes Balears, la Càtedra de Ciberseguretat, la Fundació Bit i DIHBAITUR permet aprofitar capacitats existents i orientar-les cap a la creació de coneixement, el desenvolupament de solucions avançades i la transferència efectiva de resultats al sector públic i al teixit productiu.

El creixement de la ciberdelinqüència i la dependència digital de l'economia balear fan imprescindible comptar amb capacitats d'R+D+I que permetin generar respostes pròpies, adaptar solucions a les particularitats de l'arxipèlag i anticipar escenaris de risc que les mesures convencionals no poden abordar. Les experiències d'altres regions confirmen que la combinació de programes de recerca aplicada, projectes pilot i col·laboració públic-privada accelera la maduresa del sector i genera oportunitats econòmiques directament vinculades a la ciberseguretat.

Aquest objectiu busca situar les Illes Balears en aquesta senda, fomentant un entorn que connecti universitat, administració, empreses tecnològiques, Digital Innovation Hubs i centres d'innovació, generant un circuit continu de coneixement i solucions que reforcin la seguretat del territori.



RESULTATS ESPERATS

01 **Aliances consolidades amb la UIB, la Fundació Bit, DIHBAITUR i els agents del sistema d'R+D+I balear, permetent la creació de projectes de recerca aplicada orientats a resoldre reptes reals del sector públic i privat.**

02 **Major producció de coneixement aplicable, mitjançant projectes de recerca, pilots tecnològics i validació de solucions de seguretat en entorns reals.**

03 **Increment de la participació d'institucions i empreses balears en convocatòries i projectes nacionals i europeus d'R+D+I en ciberseguretat.**

04 **Programes efectius de transferència tecnològica que facilitin que els resultats de recerca esdevinguin solucions aplicables en administracions públiques i empreses.**

05 **Reforç de les capacitats del Centre Balear de Ciberseguretat, en integrar coneixement, recerca i innovació en el seu funcionament i en l'evolució dels seus serveis.**

OBJECTIU 7

Atraure, generar i retenir talent especialitzat en ciberseguretat al territori balear

DESCRIPCIÓ

L'enfortiment del talent especialitzat en ciberseguretat és un element clau per consolidar un ecosistema innovador i competitiu a les Illes Balears. Tal com recull la planificació estratègica balear, la col·laboració amb la Universitat de les Illes Balears (UIB), la creació d'una càtedra de ciberseguretat i entitats d'innovació constitueixen pilars essencials per avançar en aquesta línia. Aquest objectiu s'orienta a impulsar iniciatives que permetin desenvolupar capacitats avançades, atreure perfils especialitzats i afavorir que els professionals formats a les illes puguin desenvolupar la seva carrera al territori.

L'enfocament es basa en actuacions coordinades entre l'administració, l'àmbit acadèmic i l'ecosistema innovador, on la formació contínua, l'especialització tècnica, la transferència de coneixement i el desenvolupament de programes de capacitació es consideren elements estructurals per a l'impuls del talent en ciberseguretat. Així mateix, la promoció de programes formatius específics, itineraris d'especialització i mecanismes que facilitin la connexió entre estudiants, investigadors i empreses resulta fonamental per consolidar un flux estable de talent que doni suport al creixement del sector.

El Centre Balear de Ciberseguretat actua com a agent articulador per facilitar aquesta col·laboració, promoure iniciatives de formació avançada, impulsar projectes conjunts amb la UIB, la Fundació Bit i els hubs d'innovació, i contribuir a la generació de noves oportunitats professionals, en línia amb les actuacions recollides en els acords institucionals vigents.

RESULTATS ESPERATS

01 **Increment de l'oferta formativa especialitzada en ciberseguretat al territori balear, mitjançant la col·laboració amb la UIB i entitats d'innovació, incloent programes d'especialització i activitats formatives avançades.**

02 **Major incorporació de talent jove i especialitzat, gràcies a programes de pràctiques, estades, beques i oportunitats de col·laboració universitat-empreses alineades amb les accions previstes en l'estratègia balear.**

03 **Retenció de professionals qualificats, mitjançant itineraris professionals, participació en projectes estratègics i oportunitats de desenvolupament vinculades a l'ecosistema regional de ciberseguretat.**

04 **Impuls d'iniciatives de transferència de coneixement, connectant recerca aplicada, innovació i necessitats reals d'administracions i empreses.**

05 **Enfortiment de la col·laboració entre administració, universitat i sector privat, consolidant un entorn que faciliti la generació contínua de talent i la creació de perfils especialitzats en ciberseguretat.**

EJE 3

Societat balear cibersegura

OBJECTIU 8

Reforçar la ciberresiliència del teixit empresarial balear

DESCRIPCIÓ

El teixit empresarial balear, integrat majoritàriament per pimes i micropimes i representat de forma rellevant en activitats com el turisme, el comerç, la logística i els serveis, constitueix un component essencial de l'economia de l'arxipèlag. En coherència amb l'Estratègia Balear de Ciberseguretat, que identifica explícitament la necessitat de donar suport a empreses i entitats públiques mitjançant capacitats centralitzades i serveis d'acompanyament tècnic articulats des del Centre Balear de Ciberseguretat, aquest objectiu s'orienta a elevar de manera gradual i sostenible la preparació del teixit productiu davant de riscos digitals, contribuint a l'estabilitat i continuïtat de l'activitat econòmica del territori.

L'enfocament es basa en un model de suport progressiu, accessible i adaptat a la realitat operativa de les pimes. Aquest model inclou activitats de sensibilització, difusió de recomanacions pràctiques, diagnòstics d'abast limitat, orientació tècnica i col·laboració amb agents de l'ecosistema regional —universitats i entitats d'innovació—. L'objectiu és facilitar que cada empresa pugui adoptar mesures de millora proporcionades a la seva mida, recursos i necessitats concretes, permetent evolucionar cap a nivells de maduresa superiors a mesura que avanci la consolidació de capacitats en el territori.

Així mateix, l'enfortiment de la col·laboració públic-privada contribueix a crear un entorn estable que promogui la confiança, l'intercanvi d'informació útil i l'adopció de bones pràctiques entre empreses, associacions sectorials i administracions.

RESULTATS ESPERATS

01 **Millora progressiva de la preparació de les empreses mitjançant l'accés a recursos, orientacions i recomanacions pràctiques proporcionades a diferents nivells de maduresa (sensibilització, guies, diagnòstics de base, accions formatives).**

02 **Consolidació d'un servei de suport especialitzat coordinat des del Centre Balear de Ciberseguretat, que faciliti acompanyament gradual a pimes i micropimes.**

03 **Increment de la cultura de ciberseguretat en l'àmbit empresarial, promogut mitjançant accions de difusió i col·laboració amb la UIB, la Fundació Bit i els hubs d'innovació, segons pràctiques ja esmentades en iniciatives de referència autonòmica.**

04 **Increment de la capacitat de prevenció i resposta del teixit productiu, gràcies a la implantació progressiva de mesures bàsiques de protecció i a la millora de l'accés a orientació tècnica qualificada.**

05 **Reforç de la col·laboració públic-privada, facilitant l'intercanvi estructurat d'informació, el desenvolupament d'iniciatives conjuntes i la creació d'un entorn de confiança que permeti abordar necessitats comunes del teixit empresarial.**

OBJECTIU 9

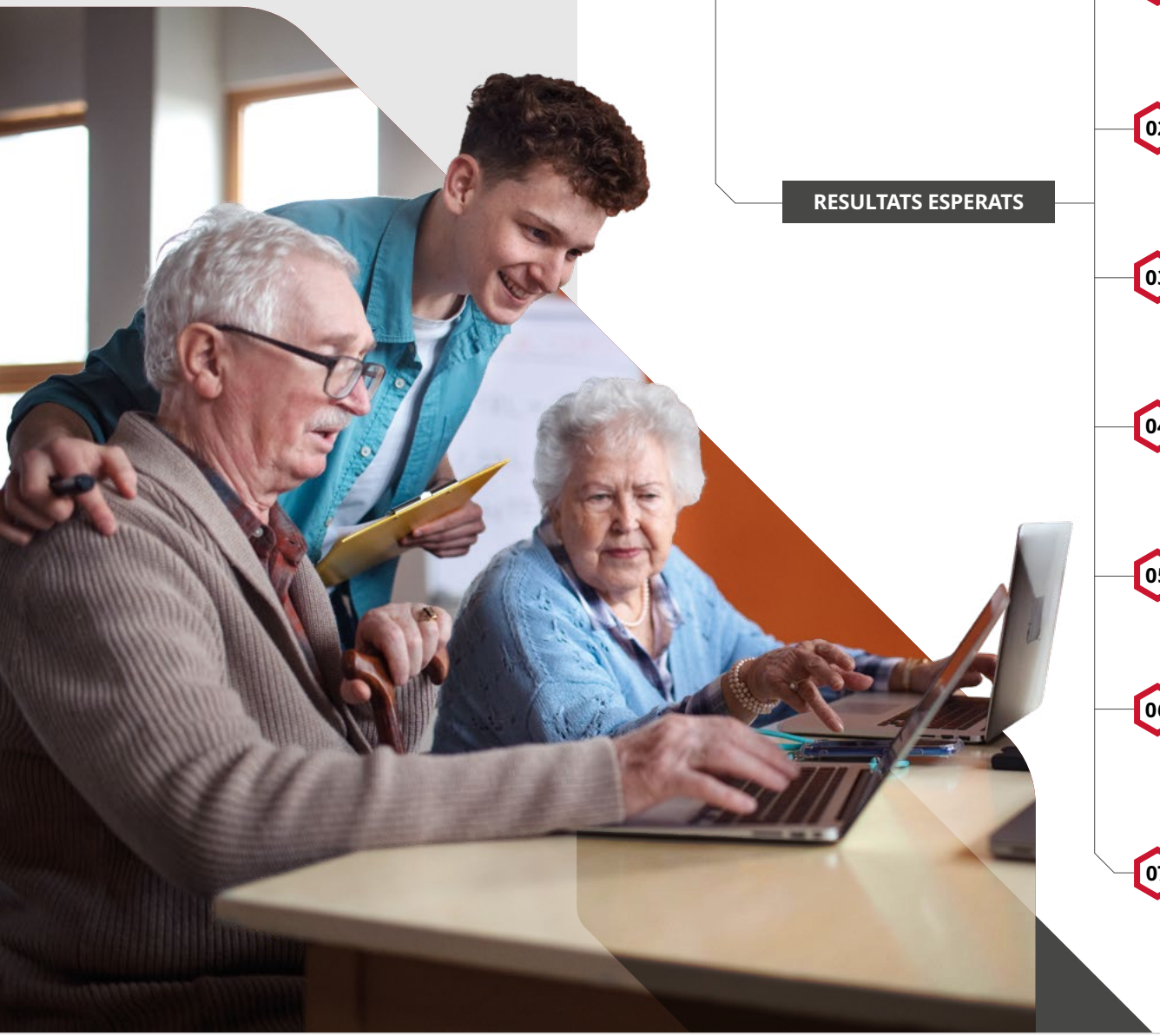
Desenvolupar una cultura sòlida de ciberseguretat a la ciutadania

DESCRIPCIÓ

Desenvolupar una cultura sòlida de ciberseguretat en la ciutadania balear requereix impulsar actuacions continuades que fomentin hàbits segurs, habilitats digitals crítiques i una major conscienciació davant de riscos creixents com fraus en línia, suplantacions d'identitat o estafes digitals. Aquest objectiu incorpora, a més, la necessitat d'oferir orientació i suport a les persones afectades després de l'ocurrència d'incidents de ciberseguretat, reconeixent que la resposta adequada posterior a l'incident és un element clau per reduir impactes, evitar recurrències i reforçar la confiança digital. L'experiència d'altres regions confirma que les societats digitalment madures són més resilients quan combinen prevenció, conscienciació i capacitats d'acompanyament accessibles per a totes les edats i perfils.

Aquest objectiu també abasta el reforç de les competències dels empleats públics, que constitueixen la primera línia de defensa en la protecció dels serveis públics. La professionalització, la formació contínua i la reducció de pràctiques de risc en l'Administració resulten essencials per garantir la seguretat dels sistemes, alineant-se amb les orientacions europees i nacionals per enfortir la protecció integral de dades i serveis públics.

L'Estratègia Balear ja reconeix la importància d'implicar agents educatius i d'innovació —com la UIB, la Fundació Bit i els hubs tecnològics— per impulsar programes de sensibilització, capacitació i orientació post-incident, adaptats a col·lectius diversos i articulats de manera accessible per a la ciutadania. Consolidar aquesta cultura permetrà no només reduir l'exposició al risc, sinó també millorar la capacitat de reacció i de recuperació de les persones afectades, elevant de forma sostinguda la confiança digital en la ciutadania i en el sector públic, com a element clau per a la cohesió social i la sostenibilitat de l'ecosistema digital balear.



RESULTATS ESPERATS

01 **Increment del nivell de conscienciació ciutadana davant fraus digitals, suplantacions d'identitat i altres amenaces comunes, gràcies a campanyes accessibles i continuades.**

02 **Major capacitació digital de la població, especialment en col·lectius vulnerables (persones grans, joves i usuaris amb baixa alfabetització digital), mitjançant programes formatius adaptats.**

03 **Reforç de les competències en ciberseguretat de l'ocupació pública, integrant itineraris formatius obligatoris i formació contínua orientada a reduir pràctiques de risc.**

04 **Increment de la participació social en la ciberseguretat, fomentant la denúncia d'incidents, l'adopció d'hàbits segurs i la corresponsabilitat en la protecció digital.**

05 **Disponibilitat de mecanismes d'orientació i assistència a víctimes de ciberincidents, que facilitin pautes clares d'actuació postincident i l'accés als recursos de suport existents.**

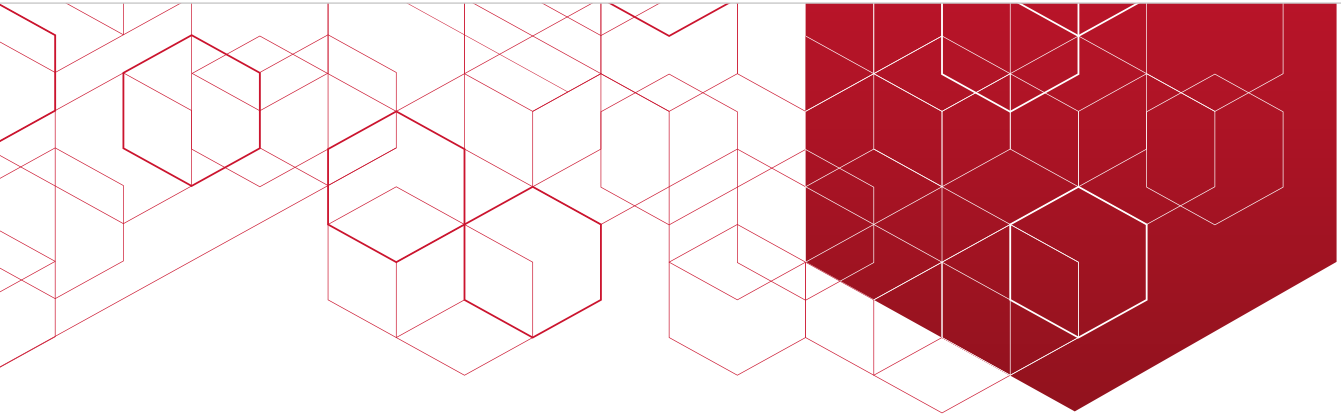
06 **Coordinació estable amb centres educatius, universitats i agents d'innovació, ga-rantint la integració de la ciberseguretat i de l'orientació post-incident en programes educatius, campanyes institucionals i activitats divulgatives.**

07 **Millora del nivell general de confiança digital en la societat balear, reduint l'exposició a amenaces i augmentant la resiliència de l'ecosistema social i administratiu.**

05

Línies d'actuació

Les línies d'actuació constitueixen el marc operatiu que permetrà transformar els objectius estratègics en avenços tangibles per a l'Administració balear, les empreses i la ciutadania. A través d'elles s'organitzen les activitats clau que s'han de posar en marxa per reforçar la protecció digital del territori, millorar la capacitat de resposta davant d'amenaces i desplegar els serveis i estructures previstos en l'Estratègia, contribuint a una execució eficaç, coherent i sostenible de les polítiques públiques en matèria de ciberseguretat.



En aquest marc, les línies d'actuació compleixen funcions diferenciades i complementàries. D'una banda, s'identifiquen línies de caràcter habilitador, orientades a crear les condicions necessàries per a una execució eficaç de l'Estratègia —com el reforç de la governança, les capacitats tècniques, la coordinació interadministrativa i les infraestructures de suport—. De l'altra, s'inclouen línies amb impacte directe immediat, enfocades a generar beneficis tangibles des de fases primerenques del desplegament, mitjançant serveis operatius, suport directe als diferents actors del territori i actuacions visibles per a empreses, administracions i ciutadania, contribuint a una execució eficaç, coherent i sostenible de les polítiques públiques en matèria de ciberseguretat.

El seu disseny permet articular les accions de manera estructurada, facilitant que cada àmbit disposi d'un conjunt coherent d'iniciatives que guiïn el seu desenvolupament, i permeten coordinar esforços entre administracions, entitats locals, empreses, universitats i agents tecnològics, garantint que l'Estratègia avanci de forma conjunta i convergent. Aquest enfocament, alineat amb les millors pràctiques, impulsa una execució ordenada i eficaç basada en la corresponsabilitat, la cooperació i l'optimització de capacitats compartides, en la qual les línies d'actuació funcionen com a nexe entre els desafiaments identificats i les mesures necessàries per superar-los.

Convé assenyalar que el nivell de detall i la naturalesa de les línies d'actuació varien de forma deliberada en funció de l'eix al qual es vinculen, reflectint el diferent grau de responsabilitat directa i capacitat d'intervenció que l'Administració autonòmica té sobre cada àmbit. A l'Eix 1, les línies són més prescriptives i operatives, atès que actuen sobre recursos, sistemes i estructures que la mateixa CAIB gestiona directament: governança, infraestructures digitals, serveis públics i coordinació interadministrativa. En els Eixos 2 i 3, les línies adopten un enfocament d'impuls, acompanyament i facilitació, perquè el Govern no opera directament sobre el teixit empresarial ni sobre els hàbits de la ciutadania, sinó que actua com a catalitzador mitjançant programes de suport, sensibilització, formació, incentius i cooperació amb agents de l'ecosistema, reforçant la cohesió territorial i la sostenibilitat del model d'intervenció pública.

De la mateixa manera, les activitats incloses en cada línia d'actuació es presenten com un conjunt d'iniciatives rellevants per a la consecució de l'objectiu al qual es vinculen, sense que el seu ordre d'aparició impliqui seqüència temporal ni nivell de prioritat. La priorització, calendarització i assignació de recursos de cada activitat es concretarà en els successius plans d'acció que desenvolupin aquesta Estratègia, atenent criteris d'impacte, viabilitat, disponibilitat de recursos i evolució del context d'amenaces. Aquest enfocament permet mantenir la flexibilitat necessària per adaptar l'execució a les circumstàncies de cada moment sense comprometre la coherència estratègica ni la continuïtat de les actuacions en el temps.

A continuació, es presenten les línies d'actuació proposades per a la consecució dels objectius estratègics i la concreció dels eixos identificats.

LÍNIA 01

Impulsar la evolución y mejora del modelo de gobernanza de la ciberseguridad en la Administración balear, consolidando roles, políticas y mecanismos de coordinación en toda la CAIB

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 1. Establir un marc robust i efectiu de governança de la ciberseguretat

ESTIMACIÓ PRESSUPOSTÀRIA

637.500,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Formalitzar el rol del Centre Balear de Ciberseguretat com a òrgan tècnic de referència per a coordinació, suport i supervisió	■	■														
2 P	Definir l'estructura de governança de la ciberseguretat a la CAIB (òr-gans, funcions, responsabilitats, incloent sector públic instrumental)	■	■	■													
3 P	Constituir el Comitè de Ciberseguretat de la CAIB (composició, funci-ons, periodicitat)			■	■												
4 P	Unificar polítiques, directrius i procediments de ciberseguretat (marc documental comú aplicable a tota l'Administració autonòmica)			■	■	■	■	■									
5 P	Crear un sistema de coordinació interna per a intercanvi estructurat d'informació de seguretat entre responsables TIC, equips operatius i unitats directives				■	■	■	■									
6 P	Definir fluxos d'escalat i presa de decisions per a incidents, crisis i situacions de risc rellevant				■	■	■	■									
7 P	Establir un model comú de gestió del risc de ciberseguretat (criteris estandarditzats d'identificació, avaluació i tractament)					■	■	■	■								
8 P	Establir canals de coordinació amb ens locals i organismes nacionals (consells, ajuntaments, CCN, INCIBE)						■	■	■	■	■						
9 C	Implantar mecanisme periòdic de seguiment i informe (compliment, desviacions, avanç del model de governança)								■	▨	▨	▨	▨	▨	▨	▨	▨

■ Ejecución / implantación ▨ Operación continua / recurrente P Puntual C Continua

LÍNIA 02

Desarrollar y reforzar las capacidades de prevención, detección y respuesta frente a ciberincidentes mediante la operación y mejora continua del Centre Balear de Ciberseguretat

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 2. Incrementar la resiliència de l'Administració balear davant de ciberincidents

ESTIMACIÓ PRESSUPOSTÀRIA

7.500.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Posar en marxa les capacitats operatives del Centre Balear de Ci-berseguretat (vigilància, detecció, anàlisi i resposta davant incidents)	■	■														
2 P	Desenvolupar repositori centralitzat d'alertes, IoCs i amenaces relle-vants accessible per als equips tècnics de la CAIB	■	■														
3 P	Establir servei de suport tècnic immediat per a incidents significatius en conselleries, ens instrumentals, consells insulars i ajuntaments		■	■													
4 P	Implantar procediments unificats de gestió d'incidents (fases, res-ponsables, fluxos de comunicació, temps de resposta, escalats)		■	■	■												
5 C	Realitzar anàlisis periòdiques de vulnerabilitats en sistemes i serveis crítics, amb priorització i remediació			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
6 P	Coordinar la resposta a incidents amb organismes nacionals i inter-nacionals (CCN-CERT, INCIBE-CERT, etc.)			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
7 P	Integrar capacitats de recuperació i continuïtat, assegurant partici-pació del Centre en activació i coordinació després d'incidents greus				■	■	■	■									
8 C	Executar exercicis i simulacres regulars de resposta davant inci-dents (interns i amb entitats externes)					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
9 P	Estendre capacitats del SOC a consells insulars, ajuntaments i ens instrumentals del sector públic balear					■	■	■	■	■	■	■	■				
10 C	Desenvolupar informes operatius periòdics (tendències, patrons d'atac, deficiències i millores)								▨	▨	▨	▨	▨	▨	▨	▨	▨
11 C	Actualitzar de forma contínua eines, processos i capacitats del Cen-tre, incorporant millores tecnològiques i revisions de procediments									▨	▨	▨	▨	▨	▨	▨	▨

■ Ejecución / implantación ▨ Operación continua / recurrente P Puntual C Continua

LÍNIA 03

Desarrollar planes y medidas específicas para la protección de infraestructuras y servicios esenciales siguiendo estándares avanzados de seguridad

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 2. Incrementar la resiliència de l'Administració balear davant de ciberincidents

ESTIMACIÓ PRESSUPOSTÀRIA

1.000.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Identificar i classificar les infraestructures i serveis essencials de l'Administració balear, incloent-hi dependències tècniques, funcionals i operatives																
2 P	Desenvolupar pla sectorial de ciberseguretat turística																
3 P	Realitzar anàlisis de riscos específics per a cada servei essencial (impactes, vulnerabilitats, escenaris d'interrupció)																
4 P	Definir requisits avançats de seguretat aplicables als serveis essen-cials, alineats amb bones pràctiques nacionals i internacionals																
5 P	Dissenyar plans de protecció específics per a cada servei essencial (mesures preventives, controls reforçats, actuacions prioritàries)																
6 C	Coordinar actuacions amb operadors i proveïdors clau per a serveis externalitzats o suportats per tercers																
7 P	Implementar arquitectures de xarxa i comunicacions més robustes (separació i protecció d'entorns crítics)																
8 C	Establir procediments de supervisió contínua (esdeveniments, aler-tes i mètriques integrades al Centre Balear de Ciberseguretat)																
9 P	Definir plans de continuïtat i recuperació específics (RTO/RPO co-herents amb criticitat del servei)																
10 C	Aplicar programes periòdics de revisió i proves de seguretat (test de resistència, revisions de configuració)																
11 C	Realitzar exercicis i simulacres focalitzats en serveis essencials (temps de resposta, coordinació, efectivitat)																
12 C	Actualitzar de forma periòdica els plans i mesures, basant-se en canvis tecnològics, noves amenaces i lliçons apreses																

Ejecución / implantación — Operación continua / recurrente — P Puntual — C Continua

LÍNIA 04

Reforzar la capacidad de anticipación y adaptación de las Illes Balears frente a riesgos emergentes y tecnologías disruptivas

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 2. Incrementar la resiliència de l'Administració balear davant de ciberincidents

ESTIMACIÓ PRESSUPOSTÀRIA

1.000.000,00 € [SENSE IVA]

ACTIVITATS — **PROJECCIÓ TEMPORAL**

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Reforçar el servei d'Observatori de Ciberseguretat del Centre Balear de Ciberseguretat, ampliant fonts, abast analític i periodicitat dels informes	■	■	■	■												
2 P	Enfortir la coordinació amb organismes nacionals i internacionals per assegurar flux continu d'indicadors, alertes, vulnerabilitats i bones pràctiques que alimentin l'Observatori	■	■	■	■												
3 P	Integrar capacitats d'anàlisi avançada (threat intelligence) a l'Obser-vatori: correlació de dades, enriquiment d'indicadors i informes de risc adaptats a Administració, empreses i entitats locals		■	■	■	■	■	■	■	■	■	■	■				
4 P	Crear un programa de vigilància tecnològica continua centrat en tec-nologies disruptives (IA, automatització, noves arquitectures de xar-xa, identitats digitals avançades, IoT)			■	■	■	■	■	■								
5 C	Publicar informes estratègics periòdics que sintetitzin riscos emer-gents, tendències tecnològiques i recomanacions per a la presa de decisions			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
6 C	Desenvolupar un sistema d'alerta primerenca basat en la informació de l'Observatori i en contribucions d'organismes nacionals i interna-cionals				▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
7 P	Posar en marxa el Laboratori de Ciberseguretat, coordinat amb l'Ob-servatori, per validar noves solucions de seguretat i analitzar tècni-ques emergents d'atac					■	■	■	■								
8 C	Realitzar exercicis de prospectiva i anàlisi d'escenaris per identificar amenaces futures, avaluar probabilitat i impacte i definir mesures preventives							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
9 C	Incorporar els resultats de l'Observatori en la planificació de la CAIB (polítiques, arquitectures, prioritats d'inversió i mesures de protecció)									▨	▨	▨	▨	▨	▨	▨	▨

■ Ejecución / implantación ▨ Operación continua / recurrente P Puntual C Continua

LÍNIA 05

Desarrollo de marcos estables de coordinación, cooperación institucional y posicionamiento en materia de ciberseguridad, a nivel territorial, nacional e internacional

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 3. Impulsar la col·laboració institucional per millorar les capacitats de ciberseguretat

ESTIMACIÓ PRESSUPOSTÀRIA

500.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Establir un marc formal de cooperació interadministrativa entre CAIB, consells insulars, ajuntaments, FFCCSE i ens instrumentals, articulat des del Centre Balear de Ciberseguretat																
2 P	Establir canals formals de coordinació amb organismes nacionals especialitzats en ciberseguretat (CCN, INCIBE) per a intercanvi d'in-formació, alertes, guies i recursos tècnics																
3 P	Crear comitès i grups de treball permanents en matèria de ciberse-guretat amb representació tècnica i directiva de totes les administra-cions del territori balear																
4 C	Reforçar la cooperació amb consells insulars, ajuntaments i FFCCSE mitjançant mecanismes continus de comunicació, suport tècnic i coordinació operativa																
5 P	Definir procediments compartits de coordinació davant incidents (flu-xos de comunicació, criteris d'escalat, pautes d'actuació coordinada)																
6 P	Consolidar acords de cooperació amb organismes nacionals (CCN, INCIBE) mitjançant protocols d'intercanvi, coordinació d'alertes, par-ticipació en programes conjunts																
7 P	Formalitzar acords de col·laboració amb altres comunitats autòno-mes que disposin de centres de ciberseguretat o CSIRTs regionals																
8 P	Definir protocols d'interlocució estable amb institucions europees en matèria de ciberseguretat (ENISA, xarxes de CSIRTs, ECCC)																
9 C	Afavorir la participació de les Illes Balears en xarxes i fòrums euro-peus i internacionals, assegurant alineació amb ENS i NIS2																
10 C	Impulsar projectes i actuacions conjuntes entre administracions (exercicis, pilots tecnològics, formació compartida, documentació comuna)																
11 C	Establir un sistema de seguiment i avaluació del model de coopera-ció (indicadors d'activitat, participació, eficàcia, alineació)																

Execució / implantació — Operació contínua / recurrent — P Puntual — C Continuació

LÍNIA 06

Consolidación de la presencia institucional de las Illes Balears mediante la participación en redes, foros y espacios de colaboración que refuercen su posicionamiento como territorio de referencia en materia de ciberseguridad

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 4. Reforçar el posicionament de les Illes Balears en l'ecosistema nacional de ciberseguretat

ESTIMACIÓ PRESSUPOSTÀRIA

250.000,00 € [SENSE IVA]

ACTIVITATS — **PROJECCIÓ TEMPORAL**

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 C	Establir la participació del Centre Balear de Ciberseguretat en xarxes i fòrums nacionals de ciberseguretat (CCN, INCIBE i altres organis-mes de referència)			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
2 P	Crear un programa institucional d'aliances estratègiques amb asso-ciacions sectorials, universitats, agències públiques i entitats tecno-lògiques					■	■	■	■								
3 C	Impulsar la presència de les Illes Balears en esdeveniments, con-gressos i jornades de ciberseguretat mitjançant ponències, interven-cions i presentació de projectes regionals							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
4 C	Representar les Illes Balears en iniciatives i grups de treball estatals i europeus, contribuint a la definició de polítiques, estàndards i línies estratègiques								▨	▨	▨	▨	▨	▨	▨	▨	▨
5 C	Desenvolupar accions de posicionament institucional coordinat (pu-blicacions estratègiques, informes de capacitats regionals, materials divulgatius)									▨	▨	▨	▨	▨	▨	▨	▨
6 C	Afavorir la integració de l'ecosistema balear de ciberseguretat en xarxes col·laboratives, facilitant la participació d'empreses i agents d'innovació en plataformes nacionals i internacionals													▨	▨	▨	▨

■ Execució / implantació ▨ Operació contínua / recurrent P Puntual C Continuació

LÍNIA 07

Establecimiento de planes de desarrollo de una industria y ecosistema especializado en el sector de la ciberseguridad en las Illes Balears, impulsando la creación, consolidación y crecimiento de empresas proveedoras de soluciones y servicios de ciberseguridad

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 5. Potenciar el desenvolupament d'una indústria de ciberseguretat a les Illes Balears

ESTIMACIÓ PRESSUPOSTÀRIA

500.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Elaborar un mapa de l'ecosistema de ciberseguretat de les Illes Ba-lears (empreses especialitzades, proveïdors TIC, startups, clústers, hubs, centres de recerca, associacions)																
2 P	Dissenyar un pla de desenvolupament sectorial de la indústria de ciberseguretat balear (objectius, prioritats, recursos, horitzó tempo-ral)																
3 P	Crear un observatori del ecosistema de ciberseguretat balear, inte-grat en el Centre Balear de Ciberseguretat																
4 P	Impulsar un programa de suport a empreses i startups de cibersegu-retat (mentorització, sandboxes, acompanyament)																
5 P	Dissenyar mecanismes d'innovació oberta o compra pública innova-dora en matèria de ciberseguretat — model GovTechLab —, posici-onant l'Administració balear com a «client tractor».[JA1.1]																
6 C	Establir reconeixements o premis periòdics a iniciatives destacades en ciberseguretat (projectes empresarials, solucions innovadores, bones pràctiques)																
7 C	Impulsar projectes tractors de ciberseguretat en sectors estratègics de l'economia balear (turisme, serveis, logística, salut)																
8 C	Impulsar el posicionament de les Illes Balears com a laboratori de ciberresiliència en entorns insulars i turístics (projectes pilot, publica-cions, fòrums)																

Execució / implantació · Operació contínua / recurrent · P Puntual · C Continuació

LÍNIA 08

Impulso de iniciativas de dinamización empresarial y cooperación público-privada que favorezcan la articulación de un ecosistema balear de ciberseguridad competitivo, innovador y conectado con otros polos de referencia

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 5. Potenciar el desenvolupament d'una indústria de ciberseguretat a les Illes Balears

ESTIMACIÓ PRESSUPOSTÀRIA

250.000,00 € [SENSE IVA]

ACTIVITATS — **PROJECCIÓ TEMPORAL**

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Crear espais de col·laboració estables entre administració, empre-ses tecnològiques i agents d'innovació, coordinats des del Centre Balear de Ciberseguretat	■	■	■	■												
2 C	Impulsar iniciatives de dinamització empresarial (trobades sectorials, taules tècniques, jornades d'innovació, fòrums especialitzats)					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
3 C	Establir acords de col·laboració públic-privada amb empreses espe-cialitzades (projectes pilot, capacitats avançades)								▨	▨	▨	▨	▨	▨	▨	▨	▨
4 C	Fomentar la visibilitat i difusió de les capacitats empresarials del terri-tori (catàlegs sectorials, repositoris de solucions, esdeveniments de presentació)									▨	▨	▨	▨	▨	▨	▨	▨
5 C	Promoure mecanismes de cooperació entre empreses locals i altres pols de referència (missions tecnològiques, xarxes temàtiques, con-nexió amb ecosistemes nacionals i internacionals)											▨	▨	▨	▨	▨	▨
6 C	Impulsar projectes d'emprenedoria i creixement empresarial (star-tups i pimes en innovació, laboratoris, acceleració vinculada al sis-tema balear d'R+D+i)													▨	▨	▨	▨

■ Execució / implantació ▨ Operació contínua / recurrent P Puntual C Continuació

LÍNIA 09

Impulso de programas de investigación, innovación y transferencia de conocimiento en ciberseguridad, en colaboración con universidades y ecosistema de I+D+i balear

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 6. Fomentar la recerca i innovació en ciberseguretat

ESTIMACIÓ PRESSUPOSTÀRIA

3.000.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 C	Organitzar seminaris, jornades tècniques i fòrums de recerca i inno-vació per connectar grups de recerca, empreses i entitats públiques			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
2 C	Impulsar projectes de recerca aplicada en ciberseguretat							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
3 C	Promoure la participació de l'ecosistema balear en programes d'R+D+I								▨	▨	▨	▨	▨	▨	▨	▨	▨
4 P	Crear un programa estructurat de transferència de coneixement									■	■	■					
5 C	Crear repositoris i publicacions tècniques periòdiques (resultats de recerca, estudis sectorials, anàlisi de tendències, experiències pilot)										▨	▨	▨	▨	▨	▨	▨
6 C	Incorporar la recerca i la innovació en l'evolució dels serveis del Centre Balear de Ciberseguretat												▨	▨	▨	▨	▨

■ Execució / implantació ▨ Operació contínua / recurrent P Puntual C Continuació

LÍNIA 10

Elaboración y despliegue de programas formativos y de desarrollo de competencias avanzadas en ciberseguridad para estudiantes y profesionales del ámbito digital, así como para personal empleado público y privado vinculado a funciones de seguridad, integrando la ciberseguridad en los itinerarios formativos y en la formación continua

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 7. Atraure, generar i fidelitzar talent especialitzat en ciberseguretat al territori balear

ESTIMACIÓ PRESSUPOSTÀRIA

1.000.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Dissenyar un marc formatiu integral en ciberseguretat estructurat en nivells (bàsic, intermedi i avançat) alineat amb ENS, NIS2 i guies CCN-STIC	■	■														
2 P	Desplegar programes de formació contínua per al personal empleat públic impartits des del Centre Balear de Ciberseguretat (bones pràctiques, protecció de dades, gestió segura, ús segur de siste-mes)				■	■	■	■	■	■	■	■	■	■	■	■	■
3 P	Coordinar un repositori formatiu centralitzat integrat al Centre (recur-sos educatius, materials didàctics, continguts audiovisuals, guies tècniques)					■	■	■	■								
4 P	Impulsar programes formatius per a joves i futurs professionals (setmanes de la ciberseguretat, xerrades en centres educatius, la-boratoris, activitats STEM)					■	■	■	■	■	■	■	■	■	■	■	■
5 P	Crear un catàleg de cursos avançats i tallers tècnics especialitzats (EDR, SIEM, anàlisi forense, gestió d'incidents, automatització de seguretat)							■	■	■	■						
6 P	Integrar assignatures, mòduls i competències de ciberseguretat en els itineraris formatius oficials de la UIB, centres d'FP i programes especialitzats								■	■	■	■	■				
7 P	Establir programes de certificació i microcredencials en cibersegure-tat reconegudes (auditoria, anàlisi de malware, gestió de riscos)									■	■	■	■				

■ Execució / implantació ▨ Operació contínua / recurrent P Puntual C Continuació

LÍNIA 11

Puesta en marcha de iniciativas para la atracción y fidelización de talento especializado en ciberseguridad en las Illes Balears, promoviendo itinerarios profesionales, prácticas, bolsas de empleo y colaboración universidad-empresa

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 7. Atraure, generar i fidelitzar talent especialitzat en ciberseguretat al territori balear

ESTIMACIÓ PRESSUPOSTÀRIA

1.000.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1	P	Establir programes de pràctiques i estades formatives en empreses															
2	P	Organitzar competicions i activitats de detecció de talent (CTF, hackathons, reptes, laboratoris) per fomentar vocacions primeren-ques i identificar perfils destacats															
3	P	Crear una borsa d'ocupació sectorial en ciberseguretat gestionada pel Centre Balear de Ciberseguretat															
4	P	Impulsar acords universitat-empresa (projectes conjunts, TFG/TFM aplicats a necessitats reals, programes de mentoria)															
5	P	Desenvolupar itineraris professionals especialitzats (rutes de pro-gressió per a perfils tècnics, analistes i gestors amb formació, expe-riència i certificacions)															
6	P	Posar en marxa programes de fidelització del talent format a les illes (oportunitats de desenvolupament professional, participació en pro-jectes estratègics, formació avançada amb la UIB)															

Execució / implantació Operació contínua / recurrent P Puntual C Continuació

LÍNIA 12

Desarrollo de programas para la mejora de las capacidades de ciberseguridad en el tejido empresarial balear, favoreciendo el incremento de su nivel de madurez y resiliencia frente a ciberamenazas

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 8. Reforçar la ciberresiliència del teixit empresarial balear

ESTIMACIÓ PRESSUPOSTÀRIA

2.100.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Desenvolupar eines d'autodiagnòstic de ciberseguretat per a pimes, adaptades a la realitat empresarial balear																
2 C	Promoure cicles d'FP Dual en ciberseguretat mitjançant un model d'alternança centre educatiu-empresa que garanteixi l'adquisició de competències pràctiques aplicables al mercat laboral balear.																
3 P	Establir un servei estable d'acompanyament tècnic des del Centre Balear de Ciberseguretat per assessorar empreses en mesures bà-siques, configuracions i resolució de dubtes																
4 P	Elaborar guies sectorials de seguretat digital (turisme, comerç, logís-tica, serveis) alineades amb ENS, NIS2 i CCN-STIC																
5 P	Posar en marxa un programa d'alertes tècniques dirigit a empreses (vulnerabilitats, configuracions crítiques, mesures recomanades) recolzat en l'Observatori																
6 C	Organitzar tallers i jornades empresarials (protecció d'actius, gestió de riscos, bones pràctiques)																
7 P	Impulsar l'adopció de solucions segures i serveis certificats mitjan-çant criteris objectius que orientin pimes i micropimes																

Execució / implantació · Operació contínua / recurrent · P Puntual · C Continuació

LÍNIA 13

Promoción de la concienciación, sensibilización y buenas prácticas en ciberseguridad en la ciudadanía balear, fomentando un uso seguro y responsable de las TIC

OBJECTIU ESTRATÈGIC IMPACTAT

OBJECTIU 9. Desenvolupar una cultura sòlida de ciberseguretat a la ciutadania

ESTIMACIÓ PRESSUPOSTÀRIA

1.750.000,00 € [SENSE IVA]

ACTIVITATS

PROJECCIÓ TEMPORAL

#	Activitat	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1	P	Elaborar materials divulgatius accessibles (infografies, vídeos breus, guies pràctiques) sobre riscos digitals comuns i hàbits responsables															
2	P	Dissenyar i executar campanyes periòdiques de conscienciació en ciberseguretat adreçades a la ciutadania balear (mitjans digitals, xarxes socials, institucions públiques, suports locals)															
3	P	Crear un portal ciutadà de ciberseguretat integrat al Centre Balear de Ciberseguretat (recursos, alertes, recomanacions, autoavaluacions, guies)															
4	P	Establir un sistema d'avisos i alertes públiques sobre fraus, estafes i riscos emergents mitjançant canals digitals institucionals															
5	P	Habilitar un canal de consulta i orientació bàsica en ciberseguretat per a dubtes habituals (fraus, protecció d'informació personal, ús segur de dispositius)															
6	P	Desenvolupar tallers i sessions d'alfabetització digital segura en col·laboració amb ajuntaments, consells, associacions i entitats edu-catives															
7	P	Establir acords de col·laboració amb entitats educatives, associaci-ons de consumidors, organitzacions socials i mitjans de comunicació per a la difusió coordinada de missatges clau															
8	P	Implementar programes de sensibilització específics per a col·lectius amb major vulnerabilitat digital (persones grans, joves, baixa alfabe-tització digital, noves famílies digitals)															
9	P	Organitzar activitats participatives (reptes, ludificació, campanyes temàtiques, concursos educatius) per fomentar l'aprenentatge actiu															
10	P	Avaluar periòdicament l'impacte de les accions de sensibilització (indicadors de participació, abast, satisfacció, adopció de bones pràctiques) i ajustar les actuacions															

Execució / implantació — Operació contínua / recurrent — P Puntual — C Continuació

06 Evolució progressiva de capacitats

El present full de ruta ordena el desplegament de l'Estratègia Balear de Ciberseguretat, oferint una visió sintètica de la seqüència d'implantació, la priorització de les línies d'actuació i l'evolució progressiva de les capacitats a consolidar al territori.

L'Estratègia agrupa actuacions orientades a reforçar la governança de la ciberseguretat, millorar la prevenció, detecció i resposta davant d'incidents, protegir els serveis essencials, donar suport al teixit empresarial, impulsar el talent i la innovació, i promoure una cultura de ciberseguretat entre la ciutadania.

Per facilitar una execució gradual, flexible i orientada a resultats, el full de ruta s'estructura en tres etapes progressives:

- **Etapa Fundacional:** estableix les bases institucionals, organitzatives, normatives i operatives de l'Estratègia com són la governança única CAIB, marc normatiu comú, plena operació del Centre Balear de Ciberseguretat i compliment ENS/NIS2 en els serveis essencials.
- **Etapa d'Escalat:** estén les capacitats al conjunt del territori, incloent administracions locals, teixit empresarial, sectors estratègics, talent i ciutadania.
- **Etapa de Posicionament:** consolida les Illes Balears com a territori de referència en ciberseguretat, reforçant la seva presència en xarxes nacionals i internacionals, el seu ecosistema innovador i la seva capacitat d'atracció d'inversió i talent.

Aquestes etapes no constitueixen compartiments tancats ni fases estrictament seqüencials. La priorització identifica el focus predominant de cada moment, mantenint la flexibilitat necessària per adaptar l'execució a l'evolució del context tecnològic, pressupostari i d'amenaces.

MADURESA CREIXENT DE LES CAPACITATS

Etapa 1: FUNDACIONAL (Crear les bases comunes)	Etapa 2: ESCALAT (Estendre capacitats al territori)	Etapa 3: POSICIONAMENT (Consolidar lideratge i referència)
Fonaments institucionals, organitzatius, normatius i operatius de l'Estratègia	**Ampliació de capacitats cap a consells, ajuntaments, empreses, talent i ciutadania**	**Projecció de les Illes Balears com a territori de referència en ciberseguretat**
L1 Governança de la ciberseguretat a l'Administració de les Illes Balears	**L2** Extensió de capacitats operatives, exercicis i millora contínua	**L4** Prospectiva, escenaris futurs i adaptació estratègica davant de riscos emergents
L2 Operació inicial del Centre Balear de Ciberseguretat	**L3** Implantació de mesures reforçades en infraestructures i serveis essencials	**L6** Presència institucional a xarxes, fòrums i espais de col·laboració
L3 Identificació i protecció inicial de serveis essencials	**L5** Cooperació interadministrativa consolidada i procediments compartits	**L7** Indústria i ecosistema balear especialitzat en ciberseguretat
L4 Observatori, riscos emergents i vigilància tecnològica	**L8** Dinamització empresarial i cooperació publico-privada	**L8** Ecosistema empresarial connectat amb altres pols de referència
L5 Coordinació institucional inicial amb administracions i organismes de referència	**L10** Formació avançada, repositori formatiu i col·laboració educativa	**L9** Investigació, innovació i transferència de coneixement
L10 Marc formatiu inicial i formació continuada per a personal empleat públic	**L11** Pràctiques, borsa de treball, reptes i acords universitat-empresa	**L11** Atracció i fidelització sostinguda de talent especialitzat
L12 Eines bàsiques i acompanyament inicial al teixit empresarial	**L12** Programas de mejora de la ciberresiliencia empresarial	**L13** Cultura ciutadana madura, avaluada i ajustada de forma contínua
L13 Materials, portal i campanyes ciutadanes de conscienciació	**L13** Tallers, alfabetització digital segura i campanyes per a col·lectius específics	

Nota: les etapes són progressives i solapades. Cada línia d'actuació es pot mantenir activa en més d'una etapa, encara que amb un grau d'intensitat diferent.

07

Seguiment, mesura i avaluació

L'Estratègia Balear de Ciberseguretat, amb un horitzó de vigència de 4 anys (2027–2030), requereix un model de seguiment que permeti avaluar de forma contínua el grau d'avanç de les seves línies d'actuació i el seu impacte real en l'Administració, les empreses i la ciutadania. Aquest model és essencial per garantir l'adequada execució de l'Estratègia, identificar desviacions a temps i orientar les decisions necessàries per assegurar la seva eficàcia al llarg de tot el seu cicle de vigència.

El present apartat estableix les bases del sistema de seguiment, mesura i avaluació que haurà de desenvolupar-se de forma detallada en el pla d'acció que concreti l'execució d'aquesta Estratègia. En aquest sentit, no es pretén definir aquí el catàleg exhaustiu d'indicadors ni els procediments operatius de report, sinó fixar els principis, l'estructura i els criteris que garanteixin un seguiment coherent, rigorós i alineat amb els objectius estratègics.

Per a això, aquest marc s'articula al voltant de tres components:

- **Definició de la governança del seguiment**, articulat en tres nivells complementaris —estratègic, tàctic i operatiu— que determinen la responsabilitat, el seu abast, així com la periodicitat de cadascuna de les actuacions.
- **Identificació dels àmbits de mesura i indicadors**, que agrupen les dimensions clau sobre les quals s'avaluarà el desplegament de l'Estratègia.
- **Definició dels mecanismes de revisió**, que garantirà la seva adaptació contínua als canvis en l'entorn d'amenaces, l'evolució tecnològica i les lliçons apreses durant la seva execució.

La informació generada per aquest sistema s'integrarà en un quadre de comandament accessible per als òrgans de governança, facilitant la presa de decisions basada en evidència i assegurant que l'Estratègia es mantingui viva, rellevant i alineada amb les necessitats reals del territori.

7.1

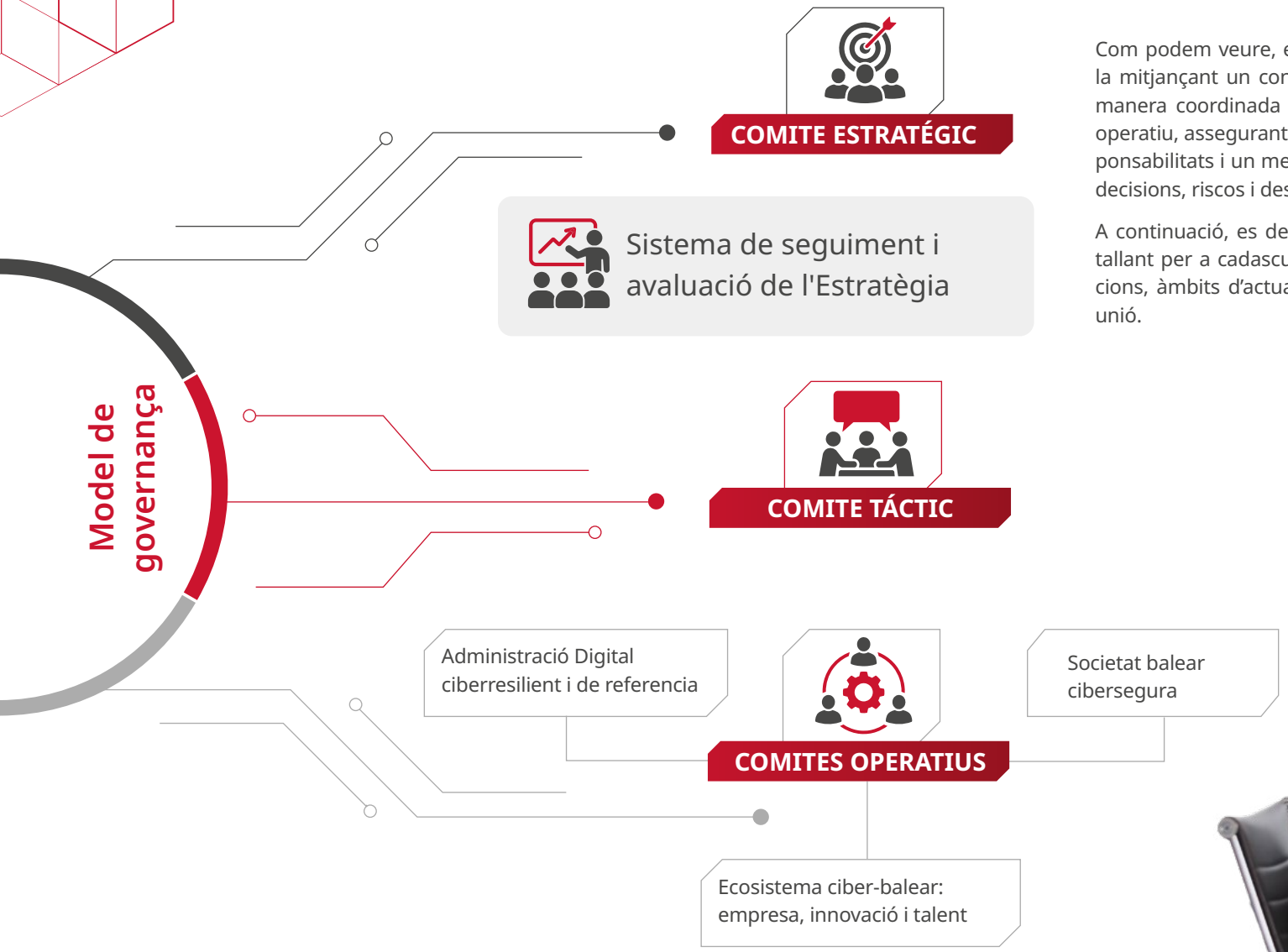
Model de seguiment

El seguiment de l'Estratègia s'articularà mitjançant un model estructurat i sistemàtic, orientat a garantir el control del grau d'avanç, la identificació primerenca de desviacions i la presa de decisions informades per a la seva correcció. Aquest model es recolza en una estructura de tres nivells complementaris, alineats amb el model de governança definit per a l'Estratègia:

- **Nivell estratègic.** Orientat a avaluar l'avenç global de l'Estratègia respecte als seus objectius i eixos, amb una periodicitat anual. Aquesta avaluació serà responsabilitat de l'òrgan de governança de l'Estratègia i es materialitzarà en un informe anual de progrés que sintetitzi els avenços assolits, les desviacions detectades i, si s'escau, les recomanacions d'ajust.
- **Nivell tàctic.** Centrat en el seguiment trimestral del desplegament de les línies d'actuació i de les fites intermèdies associades a cadascuna d'elles. Aquest seguiment serà coordinat pel Centre Balear de Ciberseguretat i permetrà detectar bloquejos, reassignar prioritats i proposar mesures correctores de forma àgil, assegurant la coherència entre la planificació estratègica i la seva execució.
- **Nivell operatiu.** Basat en el monitoratge continu d'indicadors tècnics i d'activitat vinculats a l'operació diària del Centre Balear de Ciberseguretat i dels serveis de ciberseguretat desplegats. Aquests indicadors alimentaran els nivells tàctic i estratègic mitjançant reporting mensual, proporcionant una visió detallada i actualitzada de l'estat d'execució.

Aquest model garanteix un flux d'informació ascendent, des de l'operació diària fins a l'avaluació estratègica, que permet que les decisions de govern de l'Estratègia es fonamentin en dades reals, traçables i actualitzades.

Com a síntesi, la següent Figura recull de forma esquemàtica la relació entre els diferents nivells de seguiment i els òrgans responsables de cadascun d'ells.



Com podem veure, el model de governança s'articula mitjançant un conjunt de comitès que operen de manera coordinada en els nivells estratègic, tàctic i operatiu, assegurant una adequada separació de responsabilitats i un mecanisme estructurat d'escalat de decisions, riscos i desviacions.

A continuació, es descriuen els comitès definits, detallant per a cadascun d'ells la seva composició, funcions, àmbits d'actuació i periodicitat mínima de reunió.

	Comitè Estratègic	Comitè Tàctic
Comitès		
Membres	• Director Gerent d'IB-Digital • Direcció General d'Innovació i Transformació Digital • Direcció General d'Estratègia Digital i Desenvolupament Tecnològic • Representant d'IB-Salut • Representants de FFCCSE • Representant de la UIB	• Responsable de la Estratègia del Centre Balear de Ciberseguretat • Representants de les Direccions Generals amb competències en la implementació de l'Estratègia • Representants d'organismes amb competències en la implementació de l'Estratègia
Funcions	• Anàlisi del compliment i actualització dels objectius de l'Estratègia • Supervisió global del risc de ciberseguretat a les Illes Balears • Presa de decisions estratègiques • Anàlisi global d'indicadors rellevants	• Anàlisi del risc de ciberseguretat a les Illes Balears • Mesura del compliment dels objectius de l'Estratègia • Anàlisi i gestió de pressupostos • Establiment de mecanismes de finançament • Seguiment i coordinació de les línies d'actuació • Avaluació de l'impacte de l'Estratègia per grups d'interès • Anàlisi de les activitats i fites completades • Planificació de noves activitats • Presa de decisions tàctiques • Definició i supervisió d'indicadors • Gestió de riscos • Resolució de problemes, escalant aquells fora del seu àmbit
Àmbits d'actuació	• Transversal	• Transversal
Periodicitat mínima	• Anual	• Trimestral

C

Comitè Operatiu

M

- Responsables de les línies d'actuació del Centre Balear de Ciberseguretat
- Responsables d'execució de les Direccions Generals amb competències en la implementació de l'Estratègia
- Responsables d'execució d'organismes amb competències en la implementació de l'Estratègia
- Representants de l'ecosistema empresarial de Ciberseguretat
- Representants del teixit empresarial Balear

F

- Execució de pressupostos
- Definició de metodologies de treball i accions operatives
- Seguiment detallat d'activitats i tasques associades
- Anàlisi de les tasques completades
- Planificació de noves tasques
- Presa de decisions operatives
- Mesura i manteniment d'indicadors
- Escalat de riscos
- Escalat de problemes

A

- Transformació de l'Administració
- Estratègia i tendències
- Capacitació i conscienciació
- Ciberseguretat en empreses
- Col·laboració i cooperació

P

- Mensual

C Comitè

M Membres

F Funcions

A Àmbits d'actuació

P Periodicitat mínima

En conjunt, aquest esquema de governança, alineat amb el model de seguiment descrit, permet assegurar:

- Una direcció estratègica clara, basada en informació consolidada.
- Una coordinació eficaç del desplegament de les línies d'actuació.
- Un control operatiu continu, recolzat en indicadors objectius.

Tot això constitueix un element clau per garantir l'eficàcia, traçabilitat i sostenibilitat de l'Estratègia al llarg del seu cicle de vida.

7.2

Àmbits de mesura

Per avaluar de forma equilibrada el progrés de l'Estratègia en totes les seves dimensions, el sistema de seguiment s'organitzarà al voltant de set àmbits de mesura. Aquests àmbits no constitueixen indicadors en si mateixos, sinó les dimensions estratègiques sobre les quals s'hauran de definir indicadors concrets, incloent per a cadascun d'ells el seu mètode de càlcul, la font de dades, la periodicitat de mesura, el valor de referència inicial (*baseline*) i la meta a assolir:

1. **Nivell de maduresa i resiliència de l'Administració balear.** Inclou aspectes com la capacitat de prevenció, detecció i resposta, la continuïtat dels serveis essencials i l'evolució del model de governança.
2. **Progrés en el desplegament del Centre Balear de Ciberseguretat i els seus serveis.** Monitoritzant la seva operació, serveis compartits, suport a entitats locals i actuacions de vigilància i observatori.
3. **Estat i evolució de la cultura de ciberseguretat en la ciutadania i l'ocupació pública.** Mesurat a través d'accions formatives, nivells de participació i millora en conductes segures.
4. **Maduresa i preparació del teixit empresarial balear.** Diagnòstics, adopció de mesures bàsiques, participació en programes i evolució del nivell de ciberprotecció empresarial.
5. **Enfortiment de l'ecosistema regional de ciberseguretat.** Desenvolupament del sector, participació en iniciatives, col·laboració amb la UIB, Fundació Bit, ADR, SOIB, Educació, associacions empresarials, cambres de comerç, i ecosistema d'innovació.
6. **Captació i sostenibilitat del finançament per a ciberseguretat.** Seguiment de la inversió, estabilitat pressupostària i capacitat per mantenir i evolucionar serveis crítics.
7. **Progrés en cooperació institucional i participació en xarxes nacionals i internacionals.** Connexió amb organismes estatals i europeus, compartició d'informació i participació en iniciatives conjuntes.

La definició detallada dels indicadors associats a cada àmbit es realitzarà en el pla d'acció, assegurant la seva vinculació directa amb els objectius estratègics i les línies d'actuació de l'Estratègia. No obstant això, com a orientació per a aquest desenvolupament, cada indicador haurà de respondre a criteris de rellevància (que medeixi el que realment importa), viabilitat (que sigui mesurable amb les dades disponibles), claredat (que la seva interpretació sigui inequívoca) i accionabilitat (que el seu resultat permeti prendre decisions concretes).

7.3

Revisió i actualització

El sistema de seguiment incorporarà un mecanisme formal de revisió i actualització de la pròpia Estratègia, amb l'objectiu de garantir la seva adequació permanent al context canviant de la ciberseguretat i a les necessitats reals de les Illes Balears.

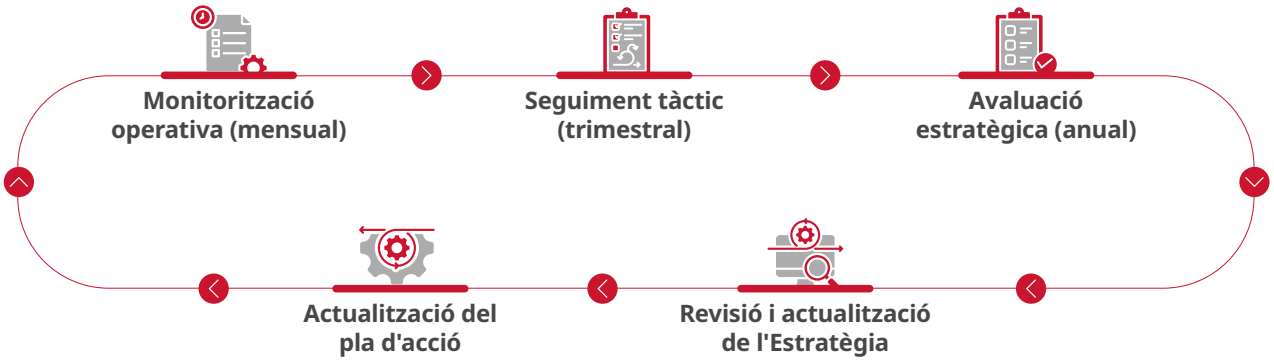
Amb caràcter anual, l'informe de progrés elaborat en el marc del nivell estratègic inclourà, a més de l'avaluació del grau d'avanç i compliment dels objectius, una valoració específica sobre els aspectes següents:

- La vigència i adequació dels objectius estratègics en relació amb l'evolució del context d'amenaces, riscos i prioritats.
- La idoneïtat de les línies d'actuació, considerant tant el seu nivell d'execució com la seva contribució efectiva als objectius de l'Estratègia.
- La necessitat d'introduir ajustos derivats de canvis normatius, avenços tecnològics, evolució de l'entorn institucional o lliçons apreses durant l'execució.

Com a resultat d'aquest procés de revisió, podrà proposar-se, quan procedeixi:

- L'actualització o reformulació de línies d'actuació.
- La incorporació de noves activitats o projectes.
- La revisió d'indicadors i fites associades.
- La reassignació de prioritats o recursos, d'acord amb els mecanismes de governança establerts.

D'aquesta manera, el seguiment, la mesura i l'avaluació s'articulen com un procés continu, integrat i cíclic, que es pot representar de la manera següent:



Aquest enfocament permet assegurar que l'Estratègia Balear de Ciberseguretat es mantingui actualitzada, rellevant i alineada amb l'evolució del context tecnològic, normatiu i d'amenaces al llarg de tot el seu període de vigència.

Al terme del període de vigència de l'Estratègia, es durà a terme una avaluació final, orientada a valorar els resultats globals assolits, el grau de compliment dels objectius estratègics i les principals lliçons apreses. Aquesta avaluació servirà com a base per a la definició de la següent Estratègia, garantint la continuïtat i maduresa del model.

No obstant això, la vocació de la present Estratègia transcendeix el seu marc temporal, assentant les bases d'un model de ciberseguretat territorial sostenible, evolutiu i orientat a la millora contínua.

Annex
Memòria econòmica de l'Estratègia

Aquesta Memòria Econòmica té per objecte justificar i dimensionar l'esforç pressupostari associat al desplegament de l'Estratègia de Ciberseguretat, alineant els objectius estratègics i les línies d'actuació definides amb una estimació econòmica coherent, realista i sostenible en el temps.

En aquest sentit, el conjunt d'actuacions contemplades en l'Estratègia suposa una **inversió total estimada de 20,5 milions d'euros**, planificada de manera progressiva conforme als diferents horitzons temporals d'execució i al model de governança proposat.

A continuació, es recull l'estimació econòmica per als diferents nivells estratègics presentats en el document:

#	Eix	Pressupost estimat
1	Administració Digital ciberresilient i de referència	10.887.500,00 €
2	Ecosistema ciber-balear: empresa, innovació i talent	5.750.000,00 €
3	Societat balear cibersegura	3.850.000,00 €
	Total	**20.487.500,00 €**

#	Objectius estratègics	Pressupost estimat
1	Establir un marc robust i efectiu de governança de la ciberseguretat	637.500,00 €
2	Incrementar la resiliència dels serveis públics davant ciberincidents	9.500.000,00 €
3	Impulsar la col·laboració institucional per millorar les capacitats de ciberseguretat	500.000,00 €
4	Reforçar el posicionament de les Illes Balears en l'ecosistema nacional de ciberseguretat	250.000,00 €
5	Potenciar el desenvolupament d'una indústria de ciberseguretat a les Illes Balears	750.000,00 €

#	Objectius estratègics	Pressupost estimat
6	Fomentar la recerca i innovació en ciberseguretat	3.000.000,00 €
7	Atraure, generar i fidelitzar talent especialitzat en ciberseguretat al territori balear	2.000.000,00 €
8	Reforçar la ciberresiliència del teixit empresarial balear	2.100.000,00 €
9	Desenvolupar una cultura sòlida de ciberseguretat en la ciutadania	1.750.000,00 €
	Total	**20.487.500,00 €**

#	Línia d'Actuació	Pressupost estimat
1	Impulsar l'evolució i millora del model de governança de la ciberseguretat a l'Administració balear, consolidant rols, polítiques i mecanismes de coordinació a tota la CAIB	637.500,00 €
2	Desenvolupar i reforçar les capacitats de prevenció, detecció i resposta davant de ciberincidents mitjançant l'operació i millora contínua del Centre Balear de Ciberseguretat	7.500.000,00 €
3	Desenvolupar plans i mesures específiques per a la protecció d'infraestructures i serveis essencials seguint estàndards avançats de seguretat	1.000.000,00 €
4	Reforçar la capacitat d'anticipació i adaptació de les Illes Balears davant de riscos emergents i tecnologies disruptives	1.000.000,00 €
5	Desenvolupament de marcs estables de coordinació, cooperació institucional i posicionament en matèria de ciberseguretat, a nivell territorial, nacional i internacional	500.000,00 €
6	Consolidació de la presència institucional de les Illes Balears mitjançant la participació en xarxes, fòrums i espais de col·laboració que reforcin el seu posicionament com a territori de referència en matèria de ciberseguretat	250.000,00 €
7	Establiment de plans de desenvolupament d'una indústria i ecosistema especialitzat en el sector de la ciberseguretat a les Illes Balears, impulsant la creació, consolidació i creixement d'empreses proveïdores de solucions i serveis de ciberseguretat	500.000,00 €

#	Línia d'Actuació	Pressupost estimat
8	Impuls d'iniciatives de dinamització empresarial i cooperació públic-privada que afavoreixin l'articulació d'un ecosistema balear de ciberseguretat competitiu, innovador i connectat amb altres pols de referència	250.000,00 €
9	Impuls de programes de recerca, innovació i transferència de coneixement en ciberseguretat, en col·laboració amb universitats, Educació i altres agents del sistema d'R+D+I balear	3.000.000,00 €
10	Elaboració i desplegament de programes formatius i de desenvolupament de competències avançades en ciberseguretat per a estudiants i professionals de l'àmbit digital, així com per a personal empleat públic i privat vinculat a funcions de seguretat, integrant la ciberseguretat en els itineraris formatius i en la formació contínua	1.000.000,00 €
11	Posada en marxa d'iniciatives per a l'atracció i fidelització de talent especialitzat en ciberseguretat a les Illes Balears, promovent itineraris professionals, pràctiques, borses d'ocupació i col·laboració universitats	1.000.000,00 €
12	Desenvolupament de programes per a la millora de les capacitats de ciberseguretat en el teixit empresarial balear, afavorint l'increment del seu nivell de maduresa i resiliència davant de ciberamenaces	2.100.000,00 €
13	Promoció de la conscienciació, sensibilització i bones pràctiques en ciberseguretat a la ciutadania balear, fomentant un ús segur i responsable de les TIC	1.750.000,00 €
	Total	**20.487.500,00 €**

El paper i els processos utilitzats en la producció d‟aquest informe compten amb les certificacions de la Cadena de Custòdia FSC® i PEFC™, que garanteixen que els productes certificats procedeixen de boscos gestionats de forma responsable, d‟acord amb criteris de sostenibilitat. Constitueix l'etapa posterior a la certificació dels boscos i és un procediment necessari per assegurar l'ús de matèries primeres legals i sostenibles.