Estrategia Balear de Ciberseguridad

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

ÍNDICE

00 Resumen ejecutivo

La aceleración de la digitalización y el crecimiento constante de las ciberamenazas han transformado profundamente el entorno en el que operan la ciudadanía, las empresas y las administraciones públicas de las Illes Balears. La expansión de servicios digitales, el aumento de la interconectividad y la adopción de tecnologías emergentes han generado oportunidades de desarrollo económico y social, pero también una mayor exposición a riesgos, tal y como reflejan los datos de ciberdelincuencia, que se multiplicaron durante los últimos años.

Para la elaboración de esta Estrategia se han tenido en cuenta los marcos de referencia vigentes en los tres niveles que condicionan la política de ciberseguridad en les Illes Balears. A nivel europeo, la Directiva NIS2, el Cybersecurity Act y las infraestructuras comunes impulsadas por la UE (EU-SOC Network, Joint Cyber Unit, ENISA), que elevan el nivel de exigencia y refuerzan la cooperación. A nivel nacional, la Estrategia Nacional de Ciberseguridad, el Esquema Nacional de Seguridad y la actuación del CCN-CERT y el INCIBE, que fijan el suelo de cumplimiento y los mecanismos de coordinación. Y a nivel balear, Pacte Social i Polític per la Sostenibilitat Econòmica, Social i Ambiental de les Illes Balears, del que esta Estrategia es pieza operativa, contribuyendo a sus ejes de economía resiliente y sociedad cohesionada y a sus objetivos de gobernanza y adaptación a los retos globales.

Durante los últimos años, el Govern ha impulsado iniciativas clave que constituyen la base de esta Estrategia: la Política de Seguridad del IBSALUT, que permitió consolidar capacidades avanzadas en el sector sanitario; la presentación en 2022 de la primera Estrategia Balear de Ciberseguridad; la aprobación en 2025 de los estatutos de IB Digital como organismo autónomo encargado de concentrar los recursos tecnológicos del Govern; la creación de la Cátedra de Ciberseguridad con la UIB; y el aprovechamiento de fondos europeos que han permitido financiar servicios especializados, infraestructuras, formación y proyectos de investigación.

20,5M€

El conjunto de actuaciones contempladas en la Estrategia se articula sobre una inversión total estimada de 20,5 millones de euros, concebida de forma progresiva y alineada con los distintos horizontes temporales de ejecución y con el modelo de gobernanza propuesto.

Sobre esta base, la Estrategia Balear de Ciberseguridad, con un horizonte de vigencia de cuatro años (2027–2030), se concibe como el instrumento que permitirá dar un salto cualitativo hacia un modelo territorial moderno y resiliente. El conjunto de actuaciones contempladas en la Estrategia se articula sobre **una inversión total estimada de 20,5 millones de euros**, concebida de forma progresiva y alineada con los distintos horizontes temporales de ejecución y con el modelo de gobernanza propuesto.

Su propósito es reforzar la seguridad del espacio digital balear mediante un enfoque centrado en la coordinación institucional, la protección del tejido productivo, la capacitación de la ciudadanía y el impulso del conocimiento y la innovación. Su visión proyecta unas Illes Balears referentes en ciberresiliencia, con una Administración robusta y homogénea en sus medidas de seguridad, un ecosistema empresarial competitivo y protegido, una sociedad formada y consciente del riesgo digital, y un tejido de investigación —UIB, Fundación Bit, DIHBAITUR— capaz de generar talento y soluciones avanzadas.

Para materializar esta visión, se definen **los valores** con los que la Estrategia articulará los **tres ejes estratégicos**:

Administración Digital ciberresiliente y de referencia

Gobernanza robusta, resiliencia de los servicios públicos, colaboración institucional y posicionamiento en el ecosistema nacional de ciberseguridad.

Ecosistema ciber-balear: empresa, innovación y talento

Desarrollo de una industria balear de ciberseguridad, impulso de la investigación y la innovación, y generación, atracción y fidelización de talento especializado.

Sociedad balear cibersegura

Madurez y resiliencia del tejido empresarial frente a ciberamenazas, y cultura de ciberseguridad en la ciudadanía.

9 Objetivos
13 Líneas de actuación

La Estrategia define nueve objetivos estratégicos y trece líneas de actuación que permiten su despliegue coherente.

A partir de estos ejes, la Estrategia define **nueve objetivos estratégicos** y **trece líneas de actuación** que permiten su despliegue coherente, incluyendo la operación del Centre Balear de Ciberseguretat, la prestación de servicios regionales, el apoyo al tejido productivo, el impulso de la formación y la innovación, y la construcción de capacidades avanzadas de vigilancia y análisis.

Con esta Estrategia, el Govern de les Illes Balears expresa su voluntad firme de situar al archipiélago entre las comunidades autónomas de referencia en materia de ciberseguridad. Esta ambición se traduce en tres compromisos concretos: alcanzar un nivel de madurez homogéneo y verificable en la ciberseguridad de toda la Administración balear; consolidar un ecosistema propio de conocimiento, innovación y talento capaz de generar valor económico y social; y garantizar que la ciudadanía y las empresas del territorio dispongan de los recursos, la formación y el acompañamiento necesarios para desenvolverse con confianza en el entorno digital. La Estrategia permitirá reforzar la confianza de la ciudadanía, mejorar la competitividad de las empresas y asegurar la prestación continua y segura de los servicios públicos, consolidando al territorio como una comunidad preparada para los desafíos del futuro digital.

01 Contexto global de la ciberseguridad

La ciberdelincuencia se ha consolidado como uno de los riesgos más relevantes para la estabilidad económica y social a escala mundial. El ransomware, los ataques a cadenas de suministro, la explotación de vulnerabilidades en servicios esenciales y las campañas de fraude masivo no son ya fenómenos excepcionales, sino una constante que afecta por igual a la ciudadanía, empresas y administraciones públicas. La expansión de dispositivos conectados, la migración acelerada a la nube y la adopción de tecnologías como la inteligencia artificial han multiplicado la superficie de exposición, configurando un escenario en el que la capacidad de protección, detección y respuesta resulta determinante para la confianza digital de cualquier territorio.

La Unión Europea ha respondido a este desafío con un marco regulatorio y operativo cada vez más exigente. La Directiva NIS2 ha reforzado sustancialmente los requisitos de gobernanza y gestión del riesgo para los servicios esenciales e importantes, ampliando el perímetro de entidades obligadas en toda la Unión, mientras que el Reglamento DORA ha impuesto estándares específicos de resiliencia operativa al sector financiero y la Cybersecurity Act ha establecido un esquema europeo de certificación de productos y servicios.

En paralelo, la Estrategia Europea de Ciberseguridad para la Década Digital ha articulado un paraguas común de capacidades a través de instrumentos como el European Cybersecurity Competence Centre (ECCC) y la Network of National Coordination Centres (NCCs), infraestructuras compartidas como la EU-SOC Network, y mecanismos avanzados de coordinación operativa como la Joint Cyber Unit (JCU) y la CSIRTs Network.

El conjunto de este edificio normativo e institucional configura el marco sobre el que los Estados miembros —y sus regiones— deben seguir construyendo y evolucionando sus capacidades de ciberseguridad.

En el ámbito nacional, España dispone de un ecosistema de ciberseguridad maduro y en evolución continua. La Estrategia Nacional de Ciberseguridad de 2019, aprobada por el Consejo de Seguridad Nacional, establece los principios y prioridades para garantizar un uso seguro y fiable del ciberespacio, apoyándose en el Esquema Nacional de Seguridad (ENS), actualizado mediante el Real Decreto 311/2022, que define los requisitos de seguridad aplicables al sector público. Sobre esta base, el CCN-CERT y el INCIBE operan como pilares de la respuesta operativa y del apoyo tanto al sector público como al tejido productivo y la ciudadanía, mientras que la transposición de la Directiva NIS2, actualmente en fase de Anteproyecto de Ley, supondrá un nuevo impulso regulatorio que reforzará la supervisión y la gestión del riesgo en los sectores esenciales.

Este entorno, complementado con las inversiones del Plan de Recuperación, Transformación y Resiliencia, refuerza la capacidad del Estado para articular una defensa cohesionada, facilita la coordinación con las comunidades autónomas y sienta las bases para el desarrollo de capacidades avanzadas de prevención, detección y respuesta en todo el territorio.

En este contexto global, europeo y nacional, las Illes Balears afrontan oportunidades y retos específicos derivados de su estructura económica, su condición insular y su elevada dependencia tecnológica. La digitalización del territorio, impulsada por un sector servicios que representa más de un tercio del PIB, un tejido productivo marcado por miles de pymes y micropymes y una ciudadanía altamente conectada, ha generado avances significativos en calidad de vida y competitividad, pero también ha incrementado de forma notable la exposición a riesgos digitales, tal y como reflejan los datos de ciberdelincuencia registrados en el archipiélago durante los últimos años.

Para reforzar sus capacidades, el Govern de les Illes Balears ha impulsado durante este periodo un conjunto de iniciativas que constituyen la base sobre la que se construye esta Estrategia. Entre ellas destaca la creación de una unidad de investigación en ciberseguridad en colaboración con la Universitat de les Illes Balears (UIB), considerada el germen del Centre Balear de Ciberseguretat, así como la consolidación de un organismo de referencia en ciberseguridad sanitaria en el ámbito del IBSalut, que ha permitido desarrollar capacidades avanzadas para la protección de servicios críticos. Más recientemente, la aprobación en 2025 de los estatutos de la Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions (IB Digital) como organismo autónomo ha reforzado el modelo de gobernanza al concentrar los recursos tecnológicos del Govern, a lo que se suma la creación de la Cátedra de Ciberseguridad con la UIB y el aprovechamiento de fondos europeos (especialmente Next Generation EU) que han permitido financiar infraestructuras, servicios especializados, formación y proyectos de investigación orientados a aumentar la resiliencia del ecosistema público y privado del archipiélago.

1.1

Marco jurídico y normativo de referencia

La Estrategia Balear de Ciberseguridad se enmarca en un conjunto articulado de normas e instrumentos regulatorios europeos, nacionales y autonómicos que definen las obligaciones, los estándares y los marcos de cooperación aplicables en materia de ciberseguridad. Su conocimiento resulta esencial para comprender el contexto de exigencia en el que opera la Comunidad Autónoma y para garantizar que las actuaciones previstas en esta Estrategia se alinean plenamente con el ordenamiento jurídico vigente.

Marco europeo

La Unión Europea ha consolidado durante los últimos años un edificio regulatorio ambicioso que establece obligaciones directas e indirectas para las administraciones públicas, los operadores de servicios esenciales y el tejido empresarial de los Estados miembros:

- La **Directiva (UE) 2022/2555 (NIS2),** que sustituye a la Directiva NIS original, refuerza sustancialmente los requisitos de gobernanza, gestión del riesgo y notificación de incidentes para un perímetro ampliado de entidades esenciales e importantes, estableciendo un marco de supervisión más exigente y armonizado en toda la Unión. Su transposición al ordenamiento español, actualmente en fase de Anteproyecto de Ley, condicionará de forma significativa la evolución de las obligaciones en materia de ciberseguridad en los próximos años.
- La **Directiva (UE) 2022/2557 (CER — Critical Entities Resilience**) complementa a la NIS2 desde la perspectiva de la resiliencia física y operativa de las entidades críticas. Mientras que la NIS2 se centra en la seguridad de las redes y sistemas de información, la Directiva CER establece obligaciones para que los Estados miembros identifiquen entidades críticas en sectores esenciales y garanticen su resiliencia frente a amenazas de toda naturaleza —incluidas las cibernéticas, las físicas, las naturales y las provocadas por el hombre—. Su relevancia para las Illes Balears reside en la estrecha interrelación entre la protección digital y la continuidad operativa de infraestructuras esenciales en un territorio insular, donde la interrupción de servicios críticos tiene un impacto amplificado sobre la población y la actividad económica.

- El **Reglamento (UE) 2022/2554 (DORA),** sobre resiliencia operativa digital del sector financiero, impone requisitos específicos de gestión de riesgos TIC, pruebas de resiliencia y supervisión de proveedores tecnológicos críticos. Aunque su alcance directo se centra en entidades financieras, su enfoque y exigencias influyen en la evolución de los estándares de resiliencia aplicables al conjunto del sector público y privado.
- El **Reglamento (UE) 2019/881 (*Cybersecurity Act*)** establece un marco permanente para la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y crea un esquema europeo de certificación de productos, servicios y procesos de ciberseguridad, orientado a reforzar la confianza en las soluciones digitales que operan en el mercado interior.
- El **Reglamento General de Protección de Datos (RGPD) — Reglamento (UE) 2016/679** constituye el pilar fundamental de la protección de datos personales en la Unión Europea, imponiendo obligaciones de seguridad del tratamiento, notificación de brechas y evaluación de impacto que se integran directamente en el marco de ciberseguridad de cualquier organización pública o privada.
- El **programa Digital Europe (DIGITAL)** y los instrumentos financieros asociados proporcionan el marco de financiación europea para el desarrollo de capacidades en ciberseguridad, inteligencia artificial, supercomputación y competencias digitales avanzadas, constituyendo una fuente clave de recursos para las iniciativas previstas en esta Estrategia.

Marco nacional

España ha desarrollado un ecosistema normativo e institucional robusto que establece las bases sobre las que las comunidades autónomas deben articular sus capacidades de ciberseguridad:

- La **Ley 36/2015, de 28 de septiembre, de Seguridad Nacional configura el marco general del Sistema de Seguridad Nacional** y establece los principios de contribución de recursos de las administraciones públicas, incluidas las comunidades autónomas, a la seguridad del Estado, incorporando expresamente la ciberseguridad como ámbito de interés.
- La **Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC)**, y su normativa de desarrollo —principalmente el **Real Decreto 704/2011** que aprueba el Reglamento de protección de las infraestructuras críticas—, configuran el sistema nacional de protección de infraestructuras críticas. Esta ley establece el catálogo de infraestructuras estratégicas, define las responsabilidades de los operadores críticos y crea las estructuras de coordinación (Centro Nacional de Protección de Infraestructuras Críticas — CNPIC, actualmente integrado en la Oficina de Coordinación de Ciberseguridad). La LPIC resulta particularmente relevante para las Illes Balears por la dependencia del archipiélago de infraestructuras esenciales de conectividad, energía, transporte y telecomunicaciones cuya protección integral exige una coordinación estrecha entre las dimensiones física y digital de la seguridad. La futura transposición de la Directiva CER al ordenamiento español actualizará y ampliará este marco, reforzando las obligaciones de resiliencia de las entidades críticas.
- El R**eal Decreto-ley 12/2018, de 7 de septiembre**, transpone la primera Directiva NIS al ordenamiento español, estableciendo un marco de seguridad para las redes y sistemas de información de los operadores de servicios esenciales y los proveedores de servicios digitales, y definiendo las autoridades competentes y los CSIRT de referencia a nivel nacional.
- La **Estrategia Nacional de Ciberseguridad 2019,** aprobada por el Consejo de Seguridad Nacional, establece los principios, objetivos y líneas de acción que guían la política de ciberseguridad del Estado, definiendo el Consejo Nacional de Ciberse-

guridad como órgano de apoyo al Consejo de Seguridad Nacional y articulando la cooperación con las comunidades autónomas.

- El **Esquema Nacional de Seguridad (ENS) — Real Decreto 311/2022, de 3 de mayo**, que actualiza el RD 3/2010, define los principios básicos y requisitos mínimos de seguridad que deben aplicar todas las administraciones públicas españolas para la protección de la información y los servicios electrónicos. El ENS, complementado por las guías CCN-STIC, constituye el estándar de referencia obligatorio para el sector público balear y el eje sobre el que se articulan las medidas de protección de la Administración autonómica.
- La **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)** adapta el RGPD al ordenamiento español, establece garantías complementarias y regula derechos digitales de la ciudadanía, reforzando las obligaciones de seguridad que las administraciones y empresas deben aplicar en el tratamiento de datos personales.
- La **Estrategia de Ciberseguridad del Sistema Nacional de Salud 2025-2028** impulsada por el Ministerio de Sanidad y aprobada en el seno del Consejo Interterritorial del Sistema Nacional de Salud (CISNS), establece el marco común de actuación en materia de ciberseguridad para el conjunto del SNS, definiendo los principios, objetivos y líneas estratégicas dirigidos a proteger la información sanitaria, garantizar la continuidad asistencial y reforzar la resiliencia del sector frente a incidentes cibernéticos. Reconociendo a la sanidad como sector de alta criticidad en línea con la Directiva NIS2, articula la cooperación entre el Ministerio, los servicios de salud autonómicos y los CERT de referencia, y constituye la referencia sectorial sobre la que se proyectan las medidas aplicables al ámbito sanitario balear, en particular al Servei de Salut de les Illes Balears (IBSALUT).
- La **transposición de la Directiva NIS2,** actualmente en fase de Anteproyecto de Ley, supondrá una ampliación significativa de las obligaciones en materia de gobernanza de la ciberseguridad, gestión del riesgo, notificación de incidentes y supervisión, afectando tanto a operadores de servicios esenciales como a un número considerablemente mayor de entidades públicas y privadas. Esta Estrategia se concibe con vocación de anticipar y facilitar la adaptación del ecosistema balear a las nuevas exigencias que derivarán de dicha transposición.

02

Diagnóstico balear: situación actual

Las Illes Balears, en su compromiso por consolidar un entorno digital seguro para la ciudadanía, las empresas y la administración pública, se enfrentan a un contexto marcado por una creciente digitalización de los servicios y por un ecosistema tecnológico en rápida evolución. En este escenario, la ciberseguridad se ha convertido en un elemento esencial para garantizar la continuidad, la calidad y la confianza en los sistemas digitales que sustentan la actividad económica, social y administrativa del archipiélago, tal como ya recogía la estrategia balear previa.

2.1

Contexto balear de amenazas y exposición

Alineado con otras comunidades autónomas que han desarrollado enfoques, las Illes Balears han avanzado en los últimos años en iniciativas de refuerzo institucional, capacidades técnicas y colaboración con agentes clave del ecosistema regional.

Este diagnóstico sintetiza la situación actual de la ciberseguridad en la región, identificando las principales tendencias de amenazas, el grado de exposición del territorio y el estado de madurez de la administración y del ecosistema regional. Su propósito es ofrecer una visión clara y equilibrada del punto de partida, como base para orientar las líneas estratégicas que se desarrollarán a continuación, alineado con la realidad balear y con las necesidades presentes y futuras del territorio.

La creciente digitalización de los servicios públicos, las empresas y la ciudadanía en las Illes Balears ha venido acompañada de un aumento sostenido de los incidentes reportados y del volumen de actividad delictiva en el entorno digital. A fecha de elaboración de este documento, los datos disponibles evidencian un crecimiento sostenido de la cibercriminalidad que afecta de forma directa al territorio balear. Según el Informe sobre la Cibercriminalidad en España 2024 del Ministerio del Interior, los hechos conocidos alcanzaron los 464.801 en 2024, representando el 18,9 % del total de infracciones penales —prácticamente el doble que en 2019 (9,9 %)—, con el fraude informático como tipología ampliamente dominante (88,8 %). En paralelo, los incidentes de nivel alto o superior en operadores de servicios esenciales casi se duplicaron en un solo año, pasando de 81 en 2023 a 160 en 2024. Las Illes Balears, con una economía altamente digitalizada y dependiente del sector servicios, no son ajenas a esta realidad, lo que refuerza la urgencia de las medidas contempladas en esta Estrategia.

Este crecimiento responde a la confluencia de varios factores estructurales:

- La adopción acelerada de servicios digitales por parte de ciudadanía, empresas y administración ha ampliado significativamente la superficie de exposición.
- La interconexión creciente entre sistemas públicos y privados ha multiplicado los vectores de ataque disponibles.
- La obsolescencia tecnológica y la deuda técnica acumulada en parte de las infraestructuras del sector público y del tejido empresarial, donde conviven sistemas heredados con arquitecturas modernas, generando entornos heterogéneos difíciles de proteger de forma homogénea.
- La mayor capacidad de detección y denuncia por parte de ciudadanía y organizaciones.

Todos estos factores completan un escenario en el que el volumen de incidentes registrados refleja tanto el aumento real de la amenaza como una mayor madurez en su identificación.

Más allá de estos factores compartidos con el resto del Estado, las Illes Balears presentan particularidades que configuran un perfil de riesgo propio:

- La condición insular del archipiélago implica una dependencia crítica de las infraestructuras de conectividad y comunicaciones que enlazan las cuatro islas principales, cuya interrupción tendría un impacto amplificado respecto a territorios peninsulares.

- El peso del sector turístico, que representa más de un tercio del PIB regional, genera una superficie de ataque que fluctúa con la estacionalidad: durante los meses de mayor afluencia, el volumen de transacciones digitales, dispositivos conectados y datos personales en circulación se multiplica, exponiendo al territorio a picos de riesgo que requieren capacidades de respuesta escalables.

- La existencia de un tejido productivo dominado por pymes y micropymes con recursos limitados para invertir en ciberseguridad, que operan en sectores (hostelería, comercio, logística, servicios) donde la dependencia digital es alta y la madurez en protección frecuentemente baja.

En este contexto, el territorio se ve afectado tanto por campañas de alcance estatal (incluyendo ataques de *ransomware* dirigidos a organismos públicos y empresas, campañas de *phishing* cada vez más sofisticadas y explotación de vulnerabilidades en servicios expuestos) como por riesgos asociados a la adopción acelerada de tecnologías emergentes cuyo despliegue no siempre va acompañado de las medidas de seguridad adecuadas.

El panorama resultante es el de un entorno dinámico y en evolución, con retos asumibles pero que exigen reforzar de forma decidida las capacidades de prevención, detección y respuesta, la cultura de seguridad en todos los niveles y la coordinación institucional entre los actores del territorio, en línea con lo que ya anticipaba la primera Estrategia Balear de Ciberseguridad y el planteamiento del Centre Balear de Ciberseguretat.

2.2

Estado actual y evolución de la ciberseguridad en el ecosistema balear

El ecosistema balear de ciberseguridad ha experimentado en los últimos años un avance progresivo que abarca a la administración pública, el tejido empresarial y la ciudadanía, aunque con grados de madurez desiguales. Las Illes Balears parten hoy de un conjunto de fortalezas que permiten abordar el desarrollo de esta Estrategia desde una base sólida, pero también de carencias que es necesario identificar con claridad para orientar adecuadamente las prioridades de actuación.

En el ámbito de la Administración pública, la evolución de las capacidades ha sido gradual y sostenida, con hitos institucionales que han ido consolidando una base cada vez más robusta. El primer paso relevante se produjo en 2018, con la aprobación del Decreto 2/2018, que estableció la Política de Seguridad de la Información del IBSALUT, alineada con el ENS y orientada a definir responsabilidades, objetivos y una estructura organizativa específica para la protección de los sistemas sanitarios. Este marco formal fue el punto de partida para el desarrollo de capacidades avanzadas, como el SOC 24x7 y el alto nivel de cumplimiento ENS alcanzado por el sector sanitario, que constituye hoy una de las referencias más maduras del ecosistema público balear.

Posteriormente, en 2022, la presentación de la primera Estrategia Balear de Ciberseguridad marcó un salto cualitativo al plantear la creación del Centre Balear de Ciberseguretat, la contratación de un SOC regional —actualmente en fase de implementación—, la definición de políticas comunes y la coordinación activa con el CCN e INCIBE.

En el ámbito sanitario, el Plan Estratégico de Salud Digital 2025-2029 reforzó aún más la centralidad de la ciberseguridad dentro de la transformación digital asistencial, articulando proyectos vinculados a la gobernanza del dato, la interoperabilidad, la inteligencia artificial y la teleasistencia.

La creación en noviembre de 2025 de la Cátedra de Ciberseguridad con la UIB, concebida para impulsar la formación especializada, la investigación aplicada y la transferencia de conocimiento, y la aprobación en diciembre de 2025 de los estatutos de la Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions (IB Digital) como organismo autónomo con el mandato de concentrar los recursos tecnológicos del Govern, han completado un ciclo institucional que sitúa a la Administración balear en una posición de partida significativamente más sólida que la de apenas unos años atrás.

No obstante, la madurez en ciberseguridad dentro del propio sector público presenta diferencias relevantes. Mientras que el ámbito sanitario y los servicios centrales del Govern han alcanzado niveles de protección significativos, los consells insulars y buena parte de los ayuntamientos del archipiélago disponen de capacidades técnicas y recursos humanos considerablemente más limitados, lo que genera una protección heterogénea en el territorio y refuerza la necesidad de un modelo de servicios compartidos que garantice un nivel de seguridad homogéneo en toda la Administración pública local

En el ámbito empresarial, el panorama refleja la realidad de un territorio cuyo tejido productivo está dominado por pymes y micropymes que operan en sectores de alta exposición digital con niveles de madurez en ciberseguridad generalmente bajos. La mayoría de estas empresas carecen de personal especializado, de políticas formalizadas de seguridad y de capacidad para invertir de forma significativa en protección digital. Las iniciativas de concienciación y apoyo impulsadas desde INCIBE y desde el propio ecosistema balear (a través de la Fundació Bit, las cámaras de comercio y las asociaciones empresariales) han contribuido a elevar la sensibilización, pero la brecha entre el nivel de amenaza al que se enfrenta el tejido productivo y su capacidad real de respuesta sigue siendo considerable, especialmente en las empresas de menor tamaño. La estacionalidad turística agrava esta situación, al generar picos de actividad digital durante los cuales muchas empresas operan con personal temporal y sistemas no siempre adecuadamente protegidos.

En el ámbito de la ciudadanía, la sociedad balear presenta un perfil altamente digitalizado, con tasas elevadas de uso de servicios en línea, administración electrónica, comercio digital y redes sociales. Sin embargo, esta elevada conectividad no siempre va acompañada de hábitos de seguridad digital adecuados. Las estafas *online*, el *phishing* y la suplantación de identidad afectan de forma creciente a la ciudadanía, con especial incidencia en colectivos más vulnerables como las personas mayores, los jóvenes y los usuarios con baja alfabetización digital. Las acciones de sensibilización desarrolladas hasta la fecha han sentado una primera base, pero la cultura de ciberseguridad en la ciudadanía balear se encuentra aún en una fase incipiente que requiere un esfuerzo sostenido, continuado y adaptado a los distintos perfiles de la población.

En conjunto, el ecosistema balear de ciberseguridad se encuentra en un momento de inflexión: la Administración ha dado pasos institucionales relevantes que proporcionan una base organizativa sólida, pero tanto el tejido empresarial como la ciudadanía necesitan un impulso decidido para elevar su nivel de protección y concienciación. Esta Estrategia parte precisamente de este diagnóstico para articular actuaciones que cubran los tres ámbitos de forma equilibrada y coordinada.

2.3

Capacidades sólidas, respuesta fragmentada: el reto balear

El estado actual de la ciberseguridad en les Illes Balears refleja un recorrido sólido pero desigual. La última década ha consolidado capacidades reales que sitúan a la comunidad autónoma en una posición de partida favorable. Sin embargo, estas capacidades se han desarrollado de forma fragmentada, con niveles de madurez heterogéneos entre administraciones, dependencias funcionales dispares y un tejido empresarial —mayoritariamente pyme y altamente expuesto al sector turístico— con un grado de protección muy desigual.

De este diagnóstico se desprende la necesidad de transitar de un modelo de capacidades fragmentadas a un modelo de resiliencia coordinada: articular, escalar y proyectar lo ya construido bajo una gobernanza única, con una visión territorial común y una capacidad de protección, detección y respuesta homogénea para Govern, consells, ayuntamientos, empresas y ciudadanía. La experiencia acumulada confirma además que la eficacia de este tipo de instrumentos no depende tanto de la amplitud de su catálogo como de su capacidad de ejecución real y de su adaptación al contexto territorial.

Por todo ello se hace necesaria una Estrategia Balear de Ciberseguridad propia, con un enfoque diferencial basado en la especialización sectorial, la proximidad al territorio, los servicios compartidos y la prioridad a la ejecución sobre la teoría, capaz de dar respuesta efectiva a las particularidades y a las necesidades reales del archipiélago.

03

Misión, visión, valores y ejes estratégicos

3.1

Misión

La Estrategia Balear de Ciberseguridad, tiene como propósito reforzar la resiliencia digital del territorio mediante un modelo de gobernanza sólido y coordinado que garantice la protección de los servicios públicos, eleve la madurez del tejido empresarial frente a las ciberamenazas e impulse una cultura de seguridad digital en el conjunto de la ciudadanía.

Para ello, la Estrategia se orienta a la provisión de capacidades y servicios de ciberseguridad concretos, al acompañamiento operativo de las administraciones, las empresas (especialmente pymes y micropymes) y la ciudadanía, y a la generación de un impacto real y medible en la capacidad de prevención, detección, respuesta y recuperación del territorio frente a incidentes de ciberseguridad.

Su objetivo es consolidar capacidades avanzadas de prevención, detección y respuesta, promover la investigación, la innovación y el talento en ciberseguridad, y apoyar especialmente a las pymes y a los colectivos más vulnerables, alineándose con los marcos nacionales y europeos para construir un entorno digital seguro, confiable y sostenible en las Illes Balears.

3.2

Visión

Convertir a las Illes Balears en un territorio referente en ciberresiliencia, en el que una Administración pública protegida por un modelo robusto y homogéneo de seguridad digital garantice servicios confiables y alineados con los estándares nacionales y europeos; un tejido empresarial preparado y competitivo opere en un entorno digital seguro, con capacidad para prevenir, resistir y recuperarse de los ciberincidentes; y una ciudadanía formada y consciente de los riesgos digitales se desenvuelva con confianza en el espacio digital.

Esta visión se sustenta en un ecosistema de conocimiento e innovación —articulado en torno a la UIB, la Fundació Bit, DIHBAITUR y otros agentes del territorio— capaz de generar talento, investigación y soluciones avanzadas, y en un modelo de coordinación integral que consolide a las Illes Balears como un territorio digital seguro, innovador y preparado para los desafíos del futuro. La singularidad del archipiélago balear —con una economía en la que cobra gran relevancia el turismo, una administración distribuida por islas y un tejido productivo compuesto mayoritariamente por pymes— posiciona a las Illes Balears como un laboratorio natural de ciberresiliencia en entornos insulares y turísticos, capaz de generar soluciones, modelos y buenas prácticas transferibles a otros territorios con características similares.

En este sentido, la Estrategia Balear de Ciberseguridad se configura como el instrumento director que permitirá articular, de forma ordenada y sostenida, las capacidades, recursos y actuaciones necesarias para hacer efectiva esta visión. A través de sus ejes estratégicos, objetivos y líneas de actuación, la Estrategia establece el marco de referencia para reforzar la gobernanza de la ciberseguridad en la Administración, impulsar el desarrollo de un ecosistema empresarial e innovador propio, y construir una cultura de seguridad digital extendida al conjunto de la sociedad balear. Su vocación es servir de hoja de ruta compartida entre instituciones, empresas, agentes de conocimiento y ciudadanía, asegurando que la ciberseguridad se integre como un elemento estructural de la transformación digital del territorio y no como una respuesta puntual a incidentes o amenazas.

TERRITORIO DIGITAL SEGURO

3.3

Valores

La ciberseguridad no es responsabilidad exclusiva de un único actor. En un territorio insular, altamente digitalizado e interconectado como las Illes Balears, la protección del espacio digital requiere la implicación activa y coordinada de todos los colectivos: administraciones públicas, empresas, agentes de conocimiento y ciudadanía. Todos forman parte de un ecosistema digital compartido en el que la seguridad es una responsabilidad colectiva.

Sobre esta premisa, se definen los principios rectores que deben guiar el desarrollo, la ejecución y la evolución de la presente Estrategia:

Corresponsabilidad y colaboración

La ciberseguridad efectiva solo es posible mediante la colaboración entre todos los actores del territorio. La Estrategia promueve modelos de cooperación entre administraciones públicas, empresas, universidades y organismos de referencia nacionales e internacionales, con el objetivo de construir capacidades compartidas que ningún actor puede desarrollar de forma aislada. En un archipiélago donde la condición insular amplifica la interdependencia entre sistemas y organizaciones, la cooperación no es una opción sino una necesidad estructural.

Transversalidad de la ciberseguridad

La ciberseguridad debe integrarse como un elemento estructural de la transformación digital, no como una capa añadida a posteriori. Este principio exige que la seguridad se incorpore desde el diseño en todos los servicios digitales, políticas públicas y procesos de innovación, garantizando la confidencialidad, integridad y disponibilidad de la información y anticipando los riesgos derivados de tecnologías emergentes como la inteligencia artificial, la computación en la nube o el Internet de las Cosas.

Orientación a resultados y pragmatismo

La Estrategia se guía por un enfoque pragmático y orientado a resultados, priorizando aquellas actuaciones que generen un impacto real y verificable en la mejora de la ciberseguridad del territorio. Este principio impulsa la adopción de soluciones simples, eficaces y cercanas a la realidad de las administraciones, las empresas y la ciudadanía, favoreciendo la utilidad práctica, la ejecución progresiva y la obtención de beneficios tangibles frente a planteamientos excesivamente complejos o meramente teóricos.

Resiliencia y continuidad

El objetivo no es solo prevenir los ciberincidentes, sino garantizar la capacidad de detectarlos con rapidez, responder de forma eficaz y recuperar la operatividad en el menor tiempo posible. Este principio orienta la Estrategia hacia el refuerzo de la continuidad de los servicios públicos esenciales, la protección de las infraestructuras críticas y la mejora continua de las capacidades de respuesta en todo el territorio, con especial atención a la dependencia de las infraestructuras de conectividad que enlazan las cuatro islas. La Estrategia incorpora, además, mecanismos de seguimiento, evaluación y revisión periódica que garanticen su vigencia y permitan incorporar lecciones aprendidas, ajustar prioridades y responder a cambios en el entorno de amenazas, la evolución tecnológica y el marco regulatorio de forma ágil.

Servicios públicos seguros y de confianza

La Administración balear debe garantizar que los servicios digitales que presta a la ciudadanía y a las empresas son seguros, fiables y conformes con los estándares nacionales y europeos. Este principio impulsa la evolución hacia una Administración que no solo protege sus sistemas, sino que genera confianza activa en el uso de los servicios públicos digitales, alineándose con los requisitos del ENS, la NIS2 y las guías CCN-STIC.

Protección de la ciudadanía y atención a colectivos vulnerables

La Estrategia sitúa a las personas en el centro de la ciberseguridad. Esto implica promover una cultura de seguridad digital accesible para todos los perfiles de la sociedad balear, con especial atención a los colectivos más expuestos —personas mayores, jóvenes y usuarios con baja alfabetización digital—, garantizando que nadie quede al margen de la protección en el entorno digital.

Proporcionalidad, adaptación al territorio e impulso del conocimiento

Las medidas de ciberseguridad deben ser proporcionadas al nivel de riesgo, a la capacidad de cada actor y a las particularidades del tejido socioeconómico balear. En un territorio donde las pymes y micropymes representan la inmensa mayoría del tejido productivo y donde las administraciones locales disponen de recursos limitados, la Estrategia apuesta por un modelo de actuación gradual, accesible y escalable que permita a cada organización avanzar desde su nivel de partida. Para que este modelo sea sostenible, resulta imprescindible contar con un ecosistema capaz de generar conocimiento propio, formar profesionales especializados y desarrollar soluciones avanzadas adaptadas al territorio, impulsando la colaboración con la UIB, la Fundació Bit, DIHBAITUR y otros agentes de innovación para convertir la ciberseguridad en un vector de desarrollo económico y tecnológico del archipiélago.

3.4

Ejes

Tomando como punto de partida la misión, la visión y los principios rectores definidos en los apartados anteriores, la Estrategia Balear de Ciberseguridad establece una serie de objetivos estratégicos orientados a hacer efectiva su implantación. Estos objetivos se estructuran en tres ejes complementarios que, de forma conjunta, permiten abordar las necesidades específicas de los distintos colectivos y ámbitos de actuación de las Illes Balears:

- Administración Digital ciberresiliente y de referencia.
- Ecosistema ciber-balear: empresa, innovación y talento.
- Sociedad balear cibersegura.

EJE 1

Administración Digital ciberresiliente y de referencia

OBJETIVO 1

MARCO DE GOBERNANZA EN LA ADMINISTRACIÓN

Línea de Actuación 1
Evolución del modelo gobernanza de la ciberseguridad en la Administración

OBJETIVO 2

RESILIENCIA EN SERVICIOS PÚBLICOS

Línea de Actuación 2
Reforzar capacidades de prevención, detección y respuesta

Línea de Actuación 3
Protección de infraestructuras y servicios

Línea de Actuación 4
Adaptación a riesgos emergentes y nuevas tecnologías

OBJETIVO 3

COLABORACIÓN INSTITUCIONAL

Línea de Actuación 5
Marcos de cooperación institucional

OBJETIVO 4

POSICIONAMIENTO ILLES BALEARS

Línea de Actuación 6
Participación en redes, foros y espacios de colaboración

EJE 2

Ecosistema ciber-balear empresa, innovación y talento

OBJETIVO 5

INDUSTRIA BALEAR DE CIBERSEGURIDAD

Línea de Actuación 7
Planes de desarrollo de industria ciberseguridad

Línea de Actuación 8
Dinamización empresarial y cooperación público-privada

OBJETIVO 6

INVESTIGACIÓN E INNOVACIÓN EN CIBERSEGURIDAD

Línea de Actuación 9
Impulso de programas I+D+i en colaboración centros de referencia

OBJETIVO 7

ATRAER, GENERAR Y FIDELIZAR CIBERTALENTO

Línea de Actuación 10
Elaboración de planes formativos para la generación de talento

Línea de Actuación 11
Impulso de iniciativas de atracción y fidelización de talento

EJE 3

Sociedad balear cibersegura

OBJETIVO 8

CIBERRESILIENCIA TEJIDO EMPRESARIAL

Línea de Actuación 12
Programas para la mejora de las capacidades en ciberseguridad en el tejido empresarial

OBJETIVO 9

CULTURA SÓLIDA EN CIBERSEGURIDAD

Línea de Actuación 13
Promoción de la concienciación y buenas prácticas de ciberseguridad en la ciudadanía balear

EJE 1

Administración Digital ciberresiliente y de referencia

Este eje orienta los esfuerzos hacia la consolidación de una Administración balear más segura, cohesionada y preparada frente a ciberamenazas, posicionando al sector público autonómico como referente en protección digital dentro del panorama nacional.

Se fundamenta en la creación de un marco robusto de gobernanza, liderado por el Centre Balear de Ciberseguretat y concebido explícitamente como un habilitador de la acción para que establezca criterios homogéneos, roles claros y mecanismos de coordinación entre todos los niveles de la Administración —Govern, Consells Insulars, ayuntamientos y FFCSE—, con el objetivo de facilitar la toma de decisiones, priorizar actuaciones y acelerar la implantación efectiva de medidas de protección, favoreciendo un uso más eficiente y sostenible de los recursos públicos y no como un fin en sí mismo.

Asimismo, impulsa la resiliencia de los servicios públicos, reforzando la capacidad de anticipación, detección, respuesta y recuperación ante incidentes, apoyándose en capacidades centralizadas como la monitorización continua, la alerta temprana, el soporte operativo y la planificación de la continuidad. Este eje integra también la capacidad de anticipación frente a riesgos emergentes y tecnologías disruptivas, asegurando que la Administración no solo reaccione ante amenazas conocidas, sino que identifique tendencias incipientes y adapte sus políticas y controles de forma proactiva.

El eje abarca igualmente la colaboración institucional como palanca estratégica, consolidando la presencia de las Illes Balears en redes, foros y espacios de cooperación nacionales e internacionales que refuercen su posicionamiento y permitan el intercambio de conocimiento, inteligencia de amenazas y buenas prácticas. Su alcance se extiende al conjunto de la Administración autonómica — Consellerias, entes instrumentales del sector público (organismos autónomos, empresas públicas, fundaciones y consorcios), Consells Insulars y ayuntamientos—, prestando especial atención a aquellos ámbitos y entidades con menores recursos y capacidades propias, todos ellos considerados agentes esenciales para el despliegue e implementación efectiva de esta Estrategia.

Este eje reconoce la necesidad de reforzar el posicionamiento de la Comunidad Autónoma en el ecosistema nacional de ciberseguridad, impulsando programas que faciliten el acceso de las empresas baleares a ayudas, incentivos y mecanismos de apoyo a la inversión en soluciones y servicios de ciberseguridad, así como la extensión de servicios compartidos de ciberseguridad a Consells Insulars y ayuntamientos, con el fin de garantizar un nivel de protección homogéneo y sostenible en todo el territorio.

Su finalidad es garantizar una Administración sólida, coordinada y de referencia, capaz de operar de manera segura y confiable, alineada con los estándares nacionales y europeos (ENS, CCN-STIC, NIS2) y preparada para afrontar los desafíos de un entorno digital en constante evolución.

Ecosistema ciber-balear: empresa, innovación y talento

Este eje se dirige a impulsar la creación y consolidación de un ecosistema propio de ciberseguridad en las Illes Balears, capaz de generar actividad económica, conocimiento avanzado y profesionales especializados que refuercen la posición competitiva del territorio.

Parte de la convicción de que la ciberseguridad no es únicamente una necesidad defensiva, sino también una oportunidad de desarrollo económico y tecnológico. El crecimiento sostenido de la demanda de soluciones y servicios de ciberseguridad, unido a la elevada exposición digital del archipiélago —con un sector turístico que representa más de un tercio del PIB y un tejido productivo compuesto mayoritariamente por pymes—, configura un entorno propicio para el surgimiento de empresas especializadas, la atracción de inversión y la especialización sectorial del ecosistema ciber-balear en aquellos ámbitos donde el territorio presenta mayores fortalezas y necesidades específicas.

En este sentido, el sector turístico se identifica de forma explícita como foco prioritario de especialización, junto con otros ámbitos estratégicos vinculados a la realidad insular, como la logística portuaria y marítima, el sector náutico, la salud y los servicios intensivos en digitalización. La Estrategia contempla el desarrollo progresivo de subprogramas sectoriales de ciberseguridad, orientados a abordar los riesgos específicos de estos ámbitos y a favorecer la generación de soluciones adaptadas, escalables y con potencial de transferencia a otros territorios con características similares.

El eje se articula en torno a tres dimensiones complementarias. En primer lugar, el desarrollo de una industria balear de ciberseguridad, impulsando la creación, consolidación y crecimiento de empresas proveedoras de soluciones y servicios, y favoreciendo la articulación de un ecosistema competitivo, innovador y conectado con otros polos de referencia nacionales e internacionales mediante iniciativas de dinamización empresarial y cooperación público-privada. En segundo lugar, el fomento de la investigación y la innovación, promoviendo programas de I+D+i y transferencia de conocimiento en colaboración con la UIB, la Fundació Bit, DIHBAI-TUR y demás agentes del sistema de innovación balear, con una orientación prioritaria hacia la aplicación práctica, la resolución de retos reales del tejido productivo y la generación de impacto económico. En tercer lugar, la generación, atracción y fidelización de talento especializado, mediante el despliegue de programas formativos, el desarrollo de competencias avanzadas y la puesta en marcha de iniciativas que promuevan itinerarios profesionales, prácticas, bolsas de empleo y colaboración universidad-empresa, integrando la ciberseguridad en los itinerarios formativos y en la formación continua del territorio.

La Estrategia reconoce de forma explícita las dificultades estructurales para la captación de profesorado especializado y la necesidad de articular soluciones específicas y realistas que permitan reforzar la oferta formativa en ciberseguridad, especialmente en el ámbito de la Formación Profesional. En este contexto, la Formación Profesional Dual se identifica como un instrumento particularmente relevante para el desarrollo del talento en ciberseguridad, al articular un modelo de alternancia entre el centro educativo y la empresa en el que el alumno adquiere competencias prácticas reales en un entorno productivo, con la participación de la empresa como agente formador. La promoción de ciclos de FP Dual vinculados a la ciberseguridad —en coordinación con centros educativos, empresas del sector y la Administración— permitirá generar una cantera de profesionales con competencias actualizadas y directamente aplicables, acelerar su inserción laboral y, al mismo tiempo, reforzar las capacidades de las propias empresas participantes, que se benefician del talento formado a medida de sus necesidades. El desarrollo del talento se concibe, así, como un proceso progresivo y escalable, alineado con la capacidad real del territorio y con las necesidades del mercado laboral, garantizando la consolidación de capacidades propias que refuercen la sostenibilidad del ecosistema digital balear.

La experiencia de otras regiones muestra que la consolidación de un sector de ciberseguridad insular y lo-

cal - con capacidades empresariales, talento cualificado y polos de innovación— contribuye no solo a reforzar la seguridad del territorio, sino también a dinamizar la economía mediante un mercado en crecimiento, servicios de alto valor añadido y empresas capaces de competir a escala nacional e internacional. Siguiendo esta línea, el eje aspira a posicionar a las Illes Balears como un territorio que conecta educación, administraciones, empresas tecnológicas y ecosistema de innovación en un circuito continuo de conocimiento, talento y soluciones, proyectando al archipiélago como referente en ámbitos como la investigación aplicada, la innovación en sectores estratégicos y la colaboración pública-privada en materia de ciberseguridad, desde un enfoque realista, progresivo y orientado a la escalabilidad del ecosistema.

Este eje reconoce, además, que la condición insular y turística del territorio no es solo un reto, sino una ventaja competitiva diferencial que permite posicionar a las Illes Balears como referente en el desarrollo de soluciones de ciberseguridad aplicadas a entornos insulares, turísticos y de alta estacionalidad, reforzando la especialización sectorial como elemento distintivo y estratégico del ecosistema ciber-balear.

Sociedad balear cibersegura

Este eje se orienta a fortalecer la protección y la madurez digital del tejido empresarial y de la ciudadanía, dos pilares esenciales para la resiliencia social y económica del archipiélago. Su objetivo es reducir la exposición al riesgo, promover la prevención y concienciación frente a las ciberamenazas, y reforzar la capacidad de respuesta y recuperación ante incidentes, consolidando un uso seguro y responsable de las tecnologías en todo el territorio.

En el ámbito empresarial, el eje pone el foco en pymes y micropymes —predominantes en sectores de alta exposición digital como turismo, comercio, logística y servicios— que presentan vulnerabilidades significativas ante ciberataques capaces de comprometer su continuidad operativa y su competitividad. Para revertir esta situación, se impulsa un modelo de apoyo progresivo, realista y accesible, basado en sensibilización, diagnósticos ligeros, guías sectoriales y acompañamiento técnico especializado, tanto en fase preventiva como tras la ocurrencia de incidentes. Estas actuaciones se articularán desde el Centre Balear de Ciberseguretat, en coordinación con asociaciones empresariales, cámaras de comercio y agentes económicos del territorio, con el fin de elevar la madurez del tejido productivo, facilitar una gestión más eficaz de los incidentes de ciberseguridad y reducir de forma sostenida su superficie de exposición.

De forma complementaria, el eje promueve una ciudadanía balear más preparada y consciente, dotándola de conocimientos, hábitos seguros y recursos prácticos que permitan afrontar amenazas crecientes como fraudes digitales, suplantaciones de identidad y estafas en línea. Las acciones se centrarán en programas continuados de sensibilización y formación, con especial atención a colectivos de mayor vulnerabilidad —personas mayores, jóvenes y usuarios con baja alfabetización digital—, integrando un punto de entrada claro y accesible a los servicios de orientación y apoyo en ciberseguridad, que permita a las personas afectadas recibir información fiable, pautas de actuación inicial y derivación a los recursos disponibles.

Este eje se apoya de manera estructural en la coordinación efectiva con las Fuerzas y Cuerpos de Seguridad del Estado, reconociendo su papel esencial en la investigación y persecución del cibercrimen y promoviendo una colaboración fluida que facilite la correcta gestión de incidentes, la preservación de evidencias y la adecuada atención a las víctimas, sin duplicar las funciones que corresponden a los organismos estatales competentes.

La experiencia de otras comunidades autónomas confirma que la concienciación social y la preparación empresarial son elementos esenciales para la resiliencia colectiva cuando se complementan con capacidades de acompañamiento y respuesta. En un territorio con una elevada dependencia de servicios digitales y una marcada estacionalidad turística —factores que amplifican la superficie de ataque—, este eje resulta determinante para reforzar la confianza digital, garantizar un uso seguro de las tecnologías y consolidar un ecosistema balear más robusto frente a las ciberamenazas.

04

Objetivos estratégicos

Los objetivos de la Estrategia Balear de Ciberseguridad constituyen la concreción operativa del propósito, la visión y los tres ejes estratégicos previamente definidos. Su formulación permite orientar de manera clara y coherente las capacidades que las Illes Balears deben desarrollar para fortalecer la protección del territorio insular frente a amenazas cada vez más sofisticadas, garantizando un marco de actuación coordinado, eficiente y alineado con las directrices estatales y europeas.

En este contexto, los objetivos se presentan como los pilares fundamentales que guiarán la creación y despliegue de estructuras como el Centre Balear de Ciberseguretat, así como la articulación de políticas, mecanismos de coordinación y servicios esenciales que permitan cumplir adecuadamente con las responsabilidades en materia de ciberseguridad.

Asimismo, los objetivos de esta Estrategia se alinean de forma directa con los del Pacte Social i Polític per la Sostenibilitat Econòmica, Social i Ambiental de les Illes Balears, tanto en su dimensión estratégica como de desarrollo.

En particular, la Estrategia contribuye a la articulación de un ecosistema de innovación y clústeres tecnológicos, a la promoción de una transformación digital segura, a la reducción de la brecha digital desde la vertiente de la ciberseguridad, a la mejora integral de la ciberseguridad y la protección de datos —objetivo para el que esta Estrategia constituye el instrumento principal de respuesta— , y al incremento de la inversión en I+D en ciberseguridad. Del mismo modo, apuntala los objetivos de desarrollo del Pacte relativos a la mejora de las infraestructuras TIC, la formación en tecnologías emergentes, el establecimiento de una estrategia regional de digitalización segura, la innovación tecnológica aplicada al turismo regenerativo y la protección de los sistemas de monitorización ambiental basados en tecnologías digitales.

De este modo, la ciberseguridad se configura como un habilitador transversal del conjunto de la agenda de innovación y digitalización del territorio.

EJE 1

Administración Digital ciberresiliente y de referencia

OBJETIVO 1

Establecer un marco robusto y efectivo de gobernanza de la ciberseguridad

DESCRIPCIÓN

La Administración balear necesita un modelo de gobernanza que unifique criterios, responsabilidades y mecanismos de coordinación en materia de ciberseguridad. La creación del Centre Balear de Ciberseguretat, contemplada dentro de la visión institucional, y la reciente constitución de la Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions (IB Digital) como organismo autónomo, ofrecen la oportunidad de estructurar un sistema coherente en el que los distintos actores públicos trabajen bajo una dirección estratégica común.

Un marco de gobernanza efectivo permitirá alinear políticas, optimizar recursos, mejorar la coordinación entre los organismos de la Comunidad Autónoma y asegurar una toma de decisiones más informada y consistente. Las experiencias de otras regiones demuestran que la existencia de un modelo claro de gobernanza (con órganos definidos, funciones asignadas y periodicidad establecida) impulsa la supervisión, la cooperación interadministrativa y la capacidad para implantar medidas de seguridad de forma homogénea.

Este objetivo incluye, además, la definición de marcos estables de coordinación y cooperación entre las instituciones públicas de las Illes Balears y los organismos nacionales e internacionales competentes, asegurando que la interlocución con el CCN, INCIBE y las estructuras europeas de ciberseguridad se realice de forma planificada, continua y alineada con los objetivos estratégicos del territorio.

RESULTADOS ESPERADOS

01 **Un modelo de gobernanza formalizado y aprobado que establezca de manera clara los órganos responsables, sus funciones y la forma en que se coordinan entre sí y con el Centre Balear de Ciberseguretat.**

02 **Marco normativo y procedimental homogéneo, asegurando que todas las entidades del sector público autonómico aplican criterios comunes de seguridad, conformes con el ENS, la NIS2 y las guías CCN-STIC.**

03 **Órganos de coordinación plenamente operativos entre el Govern, los consells insulars, los ayuntamientos, FFCCSE y los organismos públicos, permitiendo una supervisión continua y una respuesta coordinada ante incidentes.**

04 **Capacidad reforzada de supervisión y control, que incluya métricas estratégicas, gestión integral del riesgo, seguimiento de cumplimiento regulatorio y evaluación periódica de madurez.**

05 **Mayor eficiencia institucional, reduciendo duplicidades, optimizando recursos y facilitando la adopción de servicios compartidos y capacidades centralizadas de seguridad.**

06 **Marcos estables de cooperación con organismos nacionales e internacionales, garantizando una interlocución fluida, planificada y orientada a resultados.**

OBJETIVO 2

Incrementar la resiliencia de los servicios públicos frente a ciberincidentes

DESCRIPCIÓN

Reforzar la resiliencia de los servicios públicos de les Illes Balears implica mejorar la capacidad operativa real de la Administración para anticipar, detectar, gestionar y recuperarse de ciberincidentes que puedan afectar a la prestación de servicios esenciales a la ciudadanía. La puesta en marcha de capacidades y servicios compartidos de ciberseguridad, como las funciones de monitorización y respuesta del Centre Balear de Ciberseguretat, permitirá elevar la protección institucional y ofrecer un soporte más consistente a todas las entidades públicas del archipiélago.

Un modelo de resiliencia sólido combina procedimientos unificados, vigilancia continua, capacidad de respuesta coordinada y disponibilidad de planes de continuidad que reduzcan el impacto de los incidentes. La integración de estos elementos, desde un enfoque eminentemente operativo, permitirá a la Administración balear prestar servicios más seguros, reducir los tiempos de respuesta y minimizar interrupciones en escenarios de riesgo elevado.

Este objetivo incorpora asimismo una dimensión anticipatoria: la evolución constante del panorama de ciberamenazas, unida al rápido avance de tecnologías disruptivas como la inteligencia artificial, la computación en la nube, el IoT o la automatización, exige que la Administración balear desarrolle una capacidad anticipatoria sólida y permanente, que le permita no solo reaccionar ante amenazas conocidas, sino también identificar tendencias incipientes, evaluar impactos potenciales y adaptar sus políticas y controles antes de que los riesgos se materialicen. Este enfoque de anticipación se integra plenamente en la labor del Centre Balear de Ciberseguretat, que actuará como nodo de conocimiento avanzado, integrando inteligencia de amenazas, tendencias tecnológicas y señales tempranas relevantes para el territorio.

Finalmente, este objetivo integra la extensión de servicios compartidos de ciberseguridad a consells insulars y ayuntamientos, reconociendo que la protección homogénea de todo el sector público territorial requiere un modelo de prestación compartida que optimice recursos y garantice un nivel de protección consistente en las cuatro islas.

RESULTADOS ESPERADOS

01 **Capacidad de gestión de incidentes reforzada y coherente, con procedimientos comunes y una respuesta más ágil y coordinada en todo el sector público autonómico.**

02 **Servicios y funciones compartidas de detección y respuesta plenamente operativas, proporcionando soporte transversal y elevando la capacidad de protección del conjunto de la Administración.**

03 **Servicios públicos esenciales más protegidos, sustentados en mecanismos de continuidad y recuperación probados y actualizados y ejercitados de forma periódica.**

04 **Mayor capacidad de identificación temprana de riesgos emergentes, mediante vigilancia tecnológica continua, análisis de tendencias y participación en redes de intercambio de información especializadas.**

05 **Adaptación ágil de políticas, controles y capacidades, permitiendo ajustar las medidas de protección sin esperar a la aparición de incidentes significativos.**

06 **Integración de capacidades avanzadas en el Centre Balear de Ciberseguretat, que actúe como observatorio regional y plataforma operativa conectando inteligencia de amenazas, evolución tecnológica y análisis de impacto.**

07 **Esquema de servicios compartidos formalizado, que facilite a los consells insulars y a los ayuntamientos acceder a servicios de ciberseguridad de manera coordinada y con un nivel de calidad homogéneo.**

08 **Mejora real del nivel de protección en entidades con menos recursos, gracias a soporte técnico especializado, servicios compartidos operativos, acceso a alertas y acompañamiento efectivo en la gestión de la ciberseguridad.**

OBJETIVO 3

Impulsar la colaboración institucional para mejorar las capacidades de ciberseguridad

DESCRIPCIÓN

La ciberseguridad es, por su propia naturaleza, una función que trasciende las fronteras de cualquier organización individual. En un territorio insular como las Illes Balears, donde las infraestructuras digitales conectan administraciones, empresas y ciudadanía en un ecosistema altamente interdependiente, la colaboración institucional resulta esencial para construir capacidades que ningún actor puede desarrollar de forma aislada.

Este objetivo persigue consolidar la presencia institucional de las Illes Balears en los principales espacios de cooperación en materia de ciberseguridad, tanto a nivel nacional como internacional. Se trata de garantizar una participación y sostenida en redes, foros y grupos de trabajo que permitan el intercambio de conocimiento, inteligencia de amenazas, alertas, buenas prácticas y recursos técnicos, reforzando simultáneamente el posicionamiento del archipiélago como territorio de referencia.

La experiencia de otras comunidades autónomas confirma que la participación en estructuras cooperativas (como la red nacional de SOCs, los grupos de trabajo del CCN, las iniciativas de INCIBE o las redes europeas de CSIRTs) genera beneficios directos: mejora la capacidad de detección y respuesta, acelera el acceso a recursos especializados, permite la homologación de procedimientos y eleva la visibilidad institucional. Para las Illes Balears, esta dimensión colaborativa adquiere una relevancia singular dada su condición insular, que convierte la conectividad y la cooperación en activos estratégicos de primer orden.

RESULTADOS ESPERADOS

01 **Participación estable de las Illes Balears en redes nacionales e internacionales de ciberseguridad, con presencia consolidada en los foros y grupos de trabajo de mayor relevancia estratégica.**

02 **Canales formales de coordinación con organismos nacionales especializados (CCN, INCIBE) e internacionales (ENISA, redes europeas de CSIRTs), que garanticen un flujo continuo de información, alertas y recursos técnicos.**

03 **Integración del Centre Balear de Ciberseguretat en la red nacional de SOCs y en las iniciativas de compartición de inteligencia de amenazas, elevando las capacidades operativas del territorio.**

04 **Acuerdos de colaboración público-privada que permitan compartir información relevante, capacidades técnicas y experiencia especializada en materia de ciberseguridad.**

05 **Mayor visibilidad y reconocimiento institucional de las Illes Balears como comunidad autónoma comprometida y activa en el ámbito de la ciberseguridad.**

06 **Refuerzo de la cooperación interadministrativa con consells insulars y ayuntamientos, estableciendo mecanismos continuos de comunicación, apoyo técnico y coordinación operativa.**

OBJETIVO 4

Reforzar el posicionamiento de las Illes Balears en el ecosistema nacional de ciberseguridad

DESCRIPCIÓN

Más allá de la protección interna de sus sistemas y servicios, las Illes Balears deben proyectar su compromiso con la ciberseguridad como un elemento diferenciador que refuerce su posición en el ecosistema nacional. Esto implica no solo desarrollar capacidades propias, sino también facilitar que las empresas del territorio accedan a los instrumentos de apoyo disponibles para mejorar su seguridad digital, y posicionar a la Comunidad Autónoma como un interlocutor relevante en las políticas nacionales de ciberseguridad.

Este objetivo se materializa mediante el desarrollo de programas que impulsen y faciliten la inversión en ciberseguridad por parte del tejido empresarial balear, facilitando el acceso a ayudas, incentivos y mecanismos de apoyo procedentes tanto de la propia Comunidad Autónoma como de fondos estatales y europeos. En un archipiélago donde las pymes y micropymes representan la inmensa mayoría del tejido productivo, la capacidad de canalizar recursos financieros hacia la mejora de la seguridad digital constituye un elemento clave de competitividad y resiliencia territorial.

Asimismo, el posicionamiento en el ecosistema nacional requiere que la Comunidad Autónoma sea capaz de articular su oferta de capacidades, demostrar su compromiso institucional y participar activamente en las decisiones estratégicas que se adopten a nivel estatal en materia de ciberseguridad, estableciendo a las Illes Balears como un territorio de referencia y un socio fiable en la construcción de una España digitalmente segura.

RESULTADOS ESPERADOS

01 **Programas operativos de impulso y financiación de la ciberseguridad en las empresas de les Illes Balears, con mecanismos claros de acceso a ayudas, incentivos y apoyo a la inversión.**

02 **Mayor capacidad de captación de fondos estatales y europeos destinados a ciberseguridad, optimizando la participación en convocatorias y programas competitivos.**

03 **Incremento significativo de la inversión en ciberseguridad por parte de las pymes y micropymes de les Illes Balears, elevando el nivel de protección del tejido productivo.**

04 **Posicionamiento reconocido de las Illes Balears como comunidad autónoma activa y comprometida en el ecosistema nacional de ciberseguridad.**

05 **Articulación de una interlocución estable y propositiva con los organismos nacionales competentes, contribuyendo a las políticas y decisiones estratégicas del Estado en esta materia.**

EJE 2

Ecosistema ciber-balear: empresa, innovación y talento

OBJETIVO 5

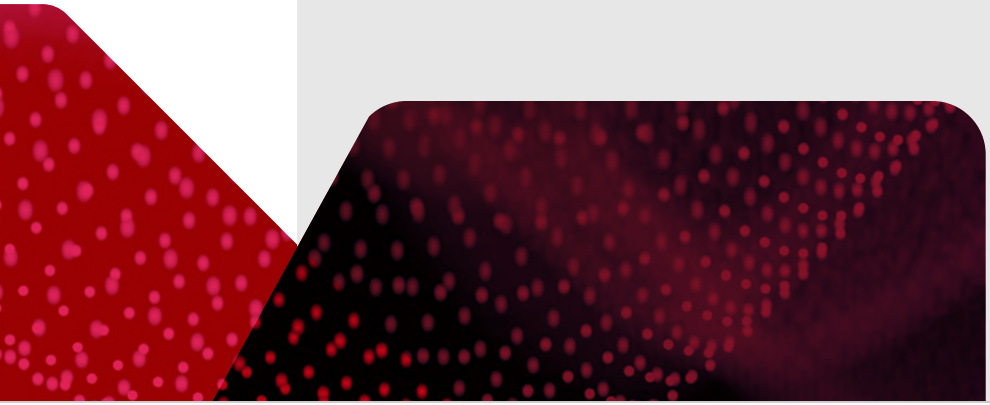
Potenciar el desarrollo de una industria de ciberseguridad en las Illes Balears

DESCRIPCIÓN

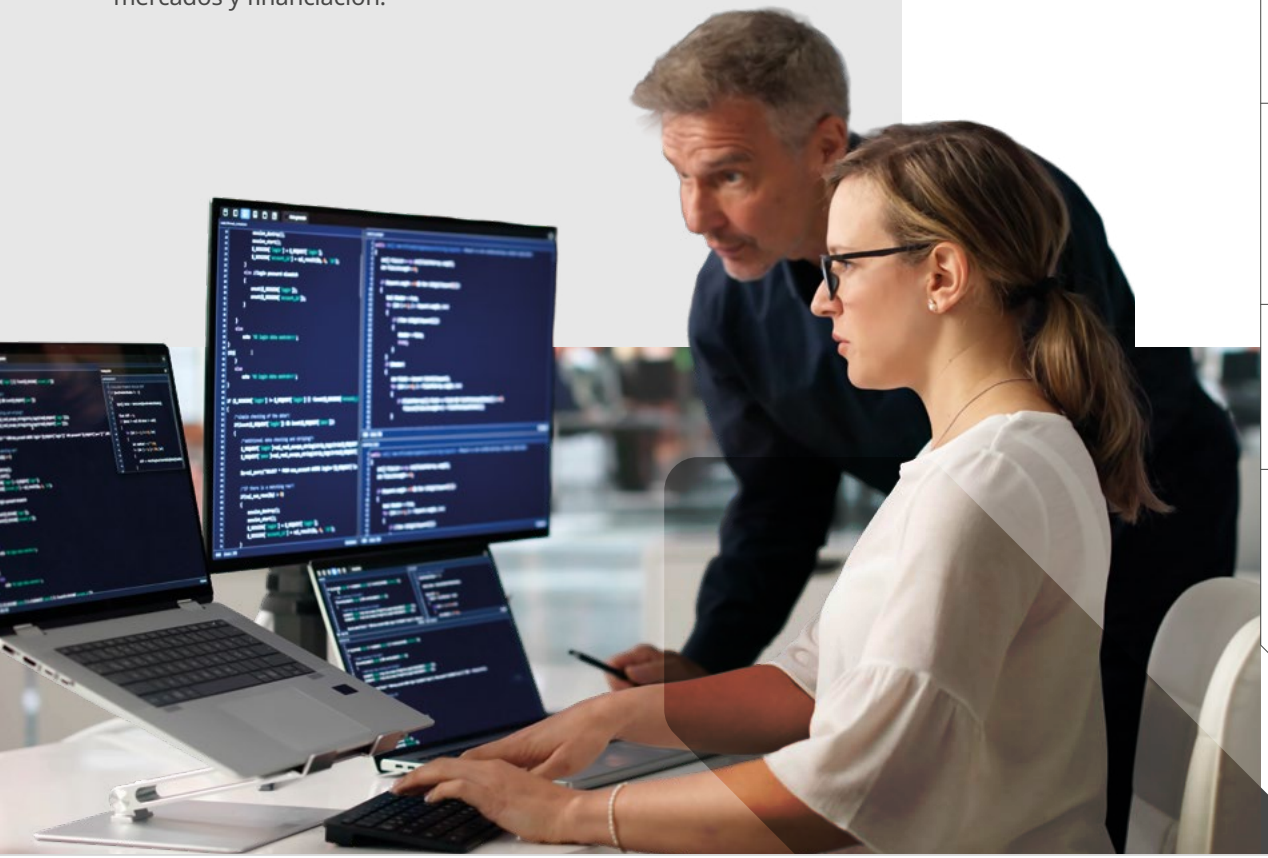
El desarrollo de un sector industrial de ciberseguridad propio constituye una oportunidad estratégica para las Illes Balears. El crecimiento sostenido de la demanda de soluciones y servicios de protección digital, impulsado tanto por el endurecimiento regulatorio europeo (NIS2, DORA, Cybersecurity Act) como por la creciente sofisticación de las amenazas, configura un mercado en expansión que el archipiélago puede aprovechar para diversificar su base económica y generar actividad de alto valor añadido.

Este objetivo persigue impulsar la creación, consolidación y crecimiento de empresas proveedoras de soluciones y servicios de ciberseguridad en las Illes Balears, favoreciendo la articulación de un ecosistema empresarial competitivo, innovador y conectado con otros polos de referencia nacionales e internacionales. Su alcance abarca desde el apoyo al emprendimiento tecnológico y la maduración de startups, hasta la dinamización de empresas ya existentes y la atracción de compañías especializadas que consideren el archipiélago como sede de operaciones o centro de desarrollo.

La condición insular y turística del territorio, lejos de suponer únicamente un reto, ofrece un entorno diferenciado para el desarrollo de soluciones de ciberseguridad en ámbitos con alta demanda y escasa oferta especializada: protección del sector hotelero y de servicios turísticos, seguridad en entornos Smart destination, protección de infraestructuras distribuidas entre islas o ciberseguridad aplicada a la logística y el transporte interinsular. Estos nichos convierten al archipiélago en un laboratorio natural de ciberresiliencia insular y turística, con capacidad para desarrollar soluciones exportables y posicionar a las Illes Balears como referente ante territorios con problemáticas similares en el ámbito nacional, europeo y mediterráneo.



La experiencia de otras regiones confirma que la consolidación de un sector local de ciberseguridad requiere combinar instrumentos de política industrial —planes sectoriales, mecanismos de compra pública innovadora, proyectos tractores— con iniciativas de dinamización empresarial y cooperación público-privada que vertebren la oferta, conecten a los actores del ecosistema y faciliten el acceso a mercados y financiación.



RESULTADOS ESPERADOS

01 **Consolidación de un tejido empresarial especializado en ciberseguridad, con empresas locales capaces de ofrecer servicios y soluciones competitivas en el mercado nacional e internacional.**

02 **Desarrollo de una oferta diferenciada de ciberseguridad en sectores estratégicos del archipiélago (turismo, servicios, logística, salud), aprovechando las particularidades del territorio como ventaja competitiva.**

03 **Incremento de iniciativas de emprendimiento e innovación empresarial en ciberseguridad, impulsadas por programas de apoyo, espacios de prueba y acompañamiento en la maduración de soluciones.**

04 **Mayor capacidad de atracción de inversión y de empresas especializadas, posicionando a las Illes Balears como un territorio atractivo para la actividad empresarial en ciberseguridad.**

05 **Dinamización de la cooperación público-privada como motor del ecosistema, con mecanismos estables de diálogo, proyectos conjuntos y compra pública que actúe como tractora de la industria local.**

06 **Proyección de las Illes Balears como polo de referencia en ciberseguridad aplicada a entornos turísticos, insulares y de servicios, generando visibilidad y reconocimiento en redes nacionales y europeas.**

OBJETIVO 6

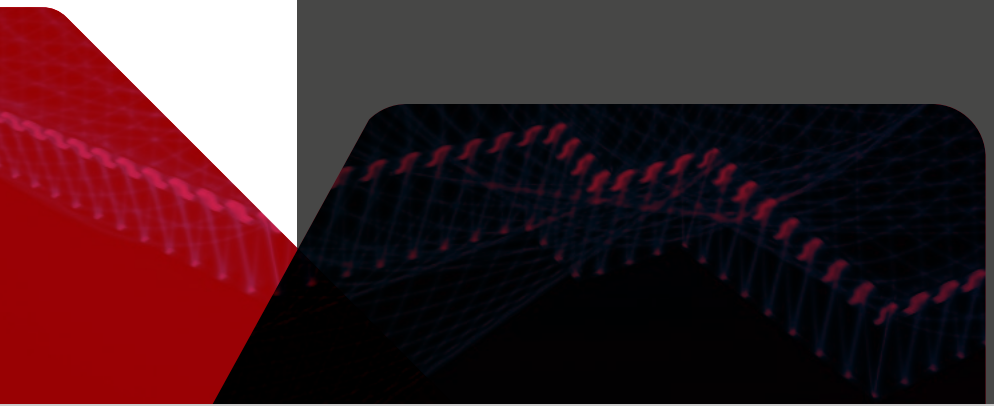
Fomentar la investigación e innovación en ciberseguridad

DESCRIPCIÓN

La consolidación de un ecosistema de investigación e innovación en ciberseguridad es clave para fortalecer la posición de las Illes Balears como un territorio competitivo, seguro y capaz de anticipar desafíos tecnológicos. El impulso a la colaboración con la Universitat de les Illes Balears, la Cátedra de Ciberseguridad, la Fundació Bit y DIHBAITUR permite aprovechar capacidades existentes y orientarlas hacia la creación de conocimiento, el desarrollo de soluciones avanzadas y la transferencia efectiva de resultados al sector público y al tejido productivo.

El crecimiento de la ciberdelincuencia y la dependencia digital de la economía balear hacen imprescindible contar con capacidades de I+D+i que permitan generar respuestas propias, adaptar soluciones a las particularidades del archipiélago y anticipar escenarios de riesgo que las medidas convencionales no pueden abordar. Las experiencias de otras regiones confirman que la combinación de programas de investigación aplicada, proyectos piloto y colaboración público-privada acelera la madurez del sector y genera oportunidades económicas directamente vinculadas a la ciberseguridad.

Este objetivo busca situar a las Illes Balears en esa senda, fomentando un entorno que conecte universidad, administración, empresas tecnológicas, Digital Innovation Hubs y centros de innovación, generando un circuito continuo de conocimiento y soluciones que refuercen la seguridad del territorio.



RESULTADOS ESPERADOS

01 **Alianzas consolidadas con la UIB, la Fundació Bit, DIHBAITUR y los agentes del sistema de I+D+i balear, permitiendo la creación de proyectos de investigación aplicada orientados a resolver retos reales del sector público y privado.**

02 **Mayor producción de conocimiento aplicable, mediante proyectos de investigación, pilotos tecnológicos y validación de soluciones de seguridad en entornos reales.**

03 **Incremento de la participación de instituciones y empresas de les Illes Balears en convocatorias y proyectos nacionales y europeos de I+D+i en ciberseguridad.**

04 **Programas efectivos de transferencia tecnológica que faciliten que los resultados de investigación se conviertan en soluciones aplicables en administraciones públicas y empresas.**

05 **Refuerzo de las capacidades del Centre Balear de Ciberseguretat, al integrar conocimiento, investigación e innovación en su funcionamiento y en la evolución de sus servicios.**

OBJETIVO 7

Atraer, generar y fidelizar talento especializado en ciberseguridad en el territorio balear

DESCRIPCIÓN

El fortalecimiento del talento especializado en ciberseguridad es un elemento clave para consolidar un ecosistema innovador y competitivo en las Illes Balears. Tal como recoge la planificación estratégica balear, la colaboración con la Universitat de les Illes Balears (UIB), la creación de una cátedra de ciberseguridad y entidades de innovación constituyen pilares esenciales para avanzar en esta línea . Este objetivo se orienta a impulsar iniciativas que permitan desarrollar capacidades avanzadas, atraer perfiles especializados y favorecer que los profesionales formados en las islas puedan desarrollar su carrera en el territorio.

El enfoque se basa en actuaciones coordinadas entre la administración, el ámbito académico y el ecosistema innovador, donde la formación continua, la especialización técnica, la transferencia de conocimiento y el desarrollo de programas de capacitación se consideran elementos estructurales para el impulso del talento en ciberseguridad . Asimismo, la promoción de programas formativos específicos, itinerarios de especialización y mecanismos que faciliten la conexión entre estudiantes, investigadores y empresas resulta fundamental para consolidar un flujo estable de talento que apoye el crecimiento del sector.

El Centre Balear de Ciberseguretat actúa como agente articulador para facilitar esta colaboración, promover iniciativas de formación avanzada, impulsar proyectos conjuntos con la UIB, la Fundación Bit y los hubs de innovación, y contribuir a la generación de nuevas oportunidades profesionales, en línea con las actuaciones recogidas en los acuerdos institucionales vigentes.

RESULTADOS ESPERADOS

01 **Incremento de la oferta formativa especializada en ciberseguridad en el territorio balear, mediante la colaboración con la UIB y entidades de innovación, incluyendo programas de especialización y actividades formativas avanzadas.**

02 **Mayor incorporación de talento joven y especializado, gracias a programas de prácticas, estancias, becas y oportunidades de colaboración universidad-empresas alineadas con las acciones previstas en la estrategia balear .**

03 **Retención de profesionales cualificados, mediante itinerarios profesionales, participación en proyectos estratégicos y oportunidades de desarrollo vinculadas al ecosistema regional de ciberseguridad.**

04 **Impulso de iniciativas de transferencia de conocimiento, conectando investigación aplicada, innovación y necesidades reales de administraciones y empresas.**

05 **Fortalecimiento de la colaboración entre administración, universidad y sector privado, consolidando un entorno que facilite la generación continua de talento y la creación de perfiles especializados en ciberseguridad.**

EJE 3

Sociedad balear cibersegura

OBJETIVO 8

Reforzar la ciberresiliencia del tejido empresarial balear

DESCRIPCIÓN

El tejido empresarial balear, integrado mayoritariamente por pymes y micropymes y representado de forma relevante en actividades como el turismo, el comercio, la logística y los servicios, constituye un componente esencial de la economía del archipiélago. En coherencia con la Estrategia Balear de Ciberseguretat, que identifica explícitamente la necesidad de apoyar a empresas y entidades públicas mediante capacidades centralizadas y servicios de acompañamiento técnico articulados desde el Centre Balear de Ciberseguretat , este objetivo se orienta a elevar de manera gradual y sostenible la preparación del tejido productivo ante riesgos digitales.

El enfoque se basa en un modelo de apoyo progresivo, accesible y adaptado a la realidad operativa de las pymes. Este modelo incluye actividades de sensibilización, difusión de recomendaciones prácticas, diagnósticos de alcance limitado, orientación técnica y colaboración con agentes del ecosistema regional —universidades y entidades de innovación—. El objetivo es facilitar que cada empresa pueda adoptar medidas de mejora proporcionadas a su tamaño, recursos y necesidades concretas, permitiendo evolucionar hacia niveles de madurez superiores a medida que avance la consolidación de capacidades en el territorio.

Asimismo, el fortalecimiento de la colaboración público-privada contribuye a crear un entorno estable que promueva la confianza, el intercambio de información útil y la adopción de buenas prácticas entre empresas, asociaciones sectoriales y administraciones.

RESULTADOS ESPERADOS

01 **Mejora progresiva de la preparación de las empresas mediante el acceso a recursos, orientaciones y recomendaciones prácticas proporcionadas a distintos niveles de madurez (sensibilización, guías, diagnósticos de base, acciones formativas).**

02 **Consolidación de un servicio de apoyo especializado coordinado desde el Centre Balear de Ciberseguretat, que facilite acompañamiento gradual a pymes y micropymes.**

03 **Incremento de la cultura de ciberseguridad en el ámbito empresarial, promovido mediante acciones de difusión y colaboración con la UIB, la Fundación Bit y los hubs de innovación, según prácticas ya mencionadas en iniciativas de referencia autonómica .**

04 **Incremento de la capacidad de prevención y respuesta del tejido productivo, gracias a la implantación progresiva de medidas básicas de protección y a la mejora del acceso a orientación técnica cualificada.**

05 **Refuerzo de la colaboración público-privada, facilitando el intercambio estructurado de información, el desarrollo de iniciativas conjuntas y la creación de un entorno de confianza que permita abordar necesidades comunes del tejido empresarial.**

OBJETIVO 9

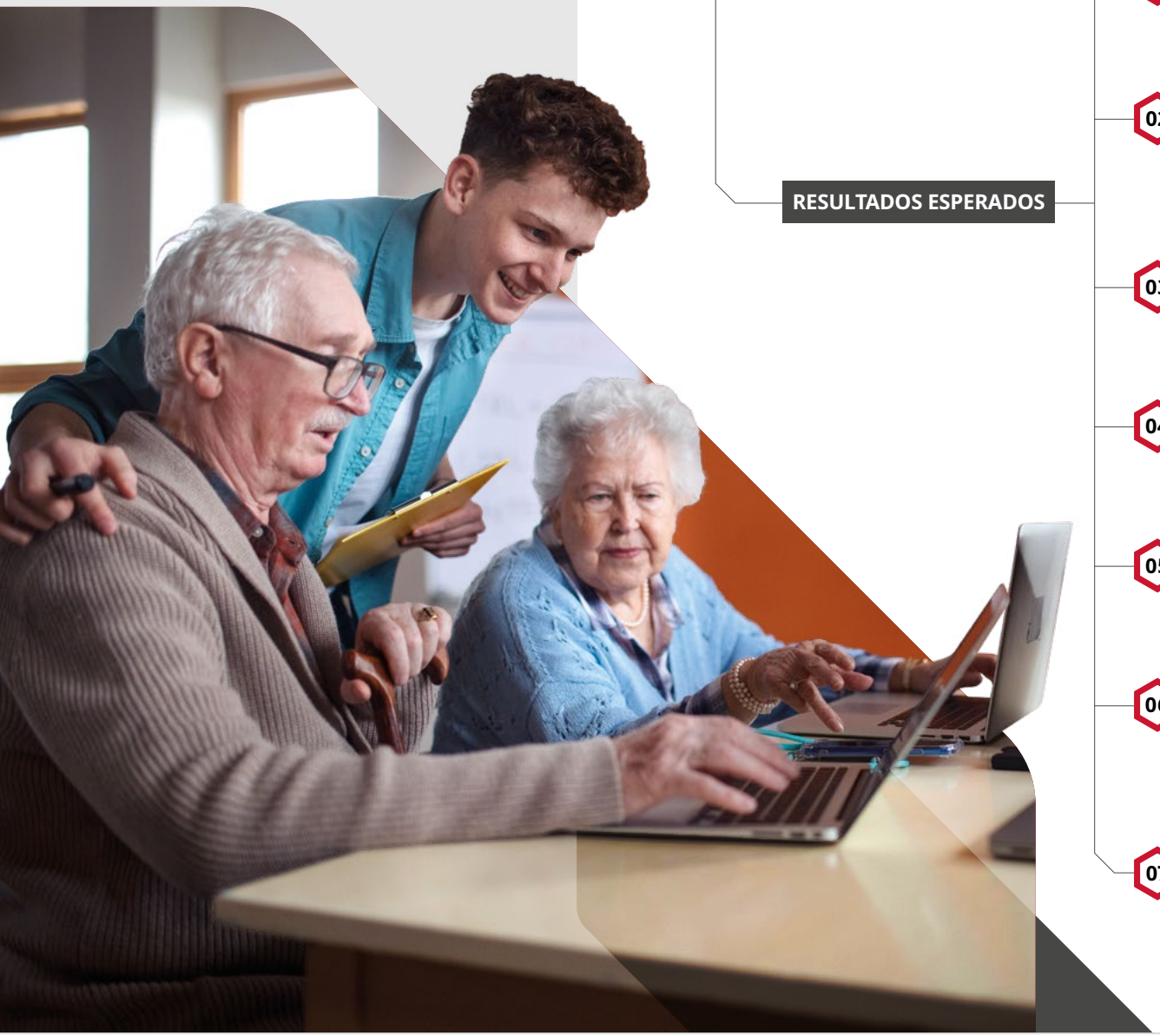
Desarrollar una cultura sólida de ciberseguridad en la ciudadanía

DESCRIPCIÓN

Desarrollar una cultura sólida de ciberseguridad en la ciudadanía balear requiere impulsar actuaciones continuadas que fomenten hábitos seguros, habilidades digitales críticas y una mayor concienciación frente a riesgos crecientes como fraudes en línea, suplantaciones de identidad o estafas digitales. Este objetivo incorpora, además, la necesidad de ofrecer orientación y apoyo a las personas afectadas tras la ocurrencia de incidentes de ciberseguridad, reconociendo que la respuesta adecuada posterior al incidente es un elemento clave para reducir impactos, evitar recurrencias y reforzar la confianza digital. La experiencia de otras regiones confirma que las sociedades digitalmente maduras son más resilientes cuando combinan prevención, concienciación y capacidades de acompañamiento accesibles para todas las edades y perfiles.

Este objetivo también abarca el refuerzo de las competencias de los empleados públicos, que constituyen la primera línea de defensa en la protección de los servicios públicos. La profesionalización, la formación continua y la reducción de prácticas de riesgo en la Administración resultan esenciales para garantizar la seguridad de los sistemas, alineándose con las orientaciones europeas y nacionales para fortalecer la protección integral de datos y servicios públicos .

La Estrategia Balear ya reconoce la importancia de implicar a agentes educativos y de innovación —como la UIB, la Fundación Bit y los hubs tecnológicos— para impulsar programas de sensibilización, capacitación y orientación post-incidente, adaptados a colectivos diversos y articulados de manera accesible para la ciudadanía. Consolidar esta cultura permitirá no solo reducir la exposición al riesgo, sino también mejorar la capacidad de reacción y de recuperación de las personas afectadas, elevando de forma sostenida la confianza digital en la ciudadanía y en el sector público.



RESULTADOS ESPERADOS

01 **Incremento del nivel de concienciación ciudadana ante fraudes digitales, suplantaciones de identidad y otras amenazas comunes, gracias a campañas accesibles y continuadas.**

02 **Mayor capacitación digital de la población, especialmente en colectivos vulnerables (personas mayores, jóvenes y usuarios con baja alfabetización digital), mediante programas formativos adaptados.**

03 **Refuerzo de las competencias en ciberseguridad del empleo público, integrando itinerarios formativos obligatorios y formación continua orientada a reducir prácticas de riesgo.**

04 **Incremento de la participación social en la ciberseguridad, fomentando la denuncia de incidentes, la adopción de hábitos seguros y la corresponsabilidad en la protección digital.**

05 **Disponibilidad de mecanismos de orientación y asistencia a víctimas de ciberincidentes, que faciliten pautas claras de actuación post incidente y el acceso a los recursos de apoyo existentes.**

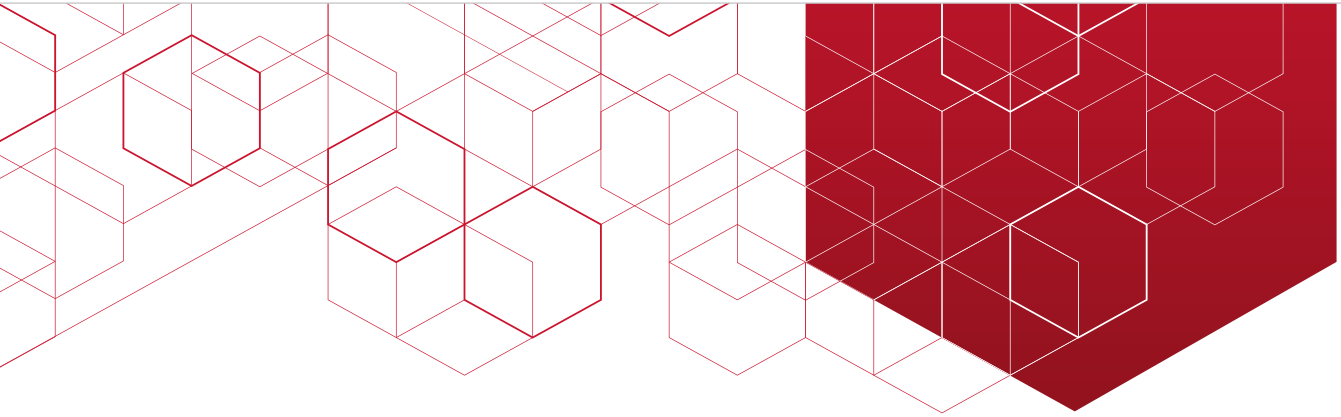
06 **Coordinación estable con centros educativos, universidades y agentes de innovación, garantizando la integración de la ciberseguridad y de la orientación post-incidente en programas educativos, campañas institucionales y actividades divulgativas.**

07 **Mejora del nivel general de confianza digital en la sociedad balear, reduciendo la exposición a amenazas y aumentando la resiliencia del ecosistema social y administrativo.**

05

Líneas de actuación

Las líneas de actuación constituyen el marco operativo que permitirá transformar los objetivos estratégicos en avances tangibles para la Administración balear, las empresas y la ciudadanía. A través de ellas se organizan las actividades clave que deben ponerse en marcha para reforzar la protección digital del territorio, mejorar la capacidad de respuesta ante amenazas y desplegar los servicios y estructuras previstos en la Estrategia.



En este marco, las líneas de actuación cumplen funciones diferenciadas y complementarias. Por un lado, se identifican líneas de carácter habilitador, orientadas a crear las condiciones necesarias para una ejecución eficaz de la Estrategia —como el refuerzo de la gobernanza, las capacidades técnicas, la coordinación interadministrativa y las infraestructuras de soporte—. Por otro, se incluyen líneas con impacto directo inmediato, enfocadas a generar beneficios tangibles desde fases tempranas del despliegue, mediante servicios operativos, apoyo directo a los distintos actores del territorio y actuaciones visibles para empresas, administraciones y ciudadanía.

Su diseño permite articular las acciones de manera estructurada, facilitando que cada ámbito disponga de un conjunto coherente de iniciativas que guíen su desarrollo, y permiten coordinar esfuerzos entre administraciones, entidades locales, empresas, universidades y agentes tecnológicos, garantizando que la Estrategia avance de forma conjunta y convergente. Este enfoque, alineado con las mejores prácticas, impulsa una ejecución ordenada y eficaz en la que las líneas de actuación funcionan como nexo entre los desafíos identificados y las medidas necesarias para superarlos.

Conviene señalar que el nivel de detalle y la naturaleza de las líneas de actuación varían de forma deliberada en función del eje al que se vinculan, reflejando el distinto grado de responsabilidad directa y capacidad de intervención que la Administración autonómica tiene sobre cada ámbito. En el Eje 1, las líneas son más prescriptivas y operativas, dado que actúan sobre recursos, sistemas y estructuras que la propia CAIB gestiona directamente: gobernanza, infraestructuras digitales, servicios públicos y coordinación interadministrativa. En los Ejes 2 y 3, las líneas adoptan un enfoque de impulso, acompañamiento y facilitación, porque el Govern no opera directamente sobre el tejido empresarial ni sobre los hábitos de la ciudadanía, sino que actúa como catalizador mediante programas de apoyo, sensibilización, formación, incentivos y cooperación con agentes del ecosistema.

Del mismo modo, las actividades incluidas en cada línea de actuación se presentan como un conjunto de iniciativas relevantes para la consecución del objetivo al que se vinculan, sin que su orden de aparición implique secuencia temporal ni nivel de prioridad. La priorización, calendarización y asignación de recursos de cada actividad se concretará en los sucesivos planes de acción que desarrollen esta Estrategia, atendiendo a criterios de impacto, viabilidad, disponibilidad de recursos y evolución del contexto de amenazas. Este enfoque permite mantener la flexibilidad necesaria para adaptar la ejecución a las circunstancias de cada momento sin comprometer la coherencia estratégica del conjunto.

A continuación, se presenta de forma gráfica las líneas de actuación propuestas para la consecución de los objetivos estratégicos y la concreción de los ejes identificados:

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 1. Establecer un marco robusto y efectivo de gobernanza de la ciberseguridad

ESTIMACIÓN PRESUPUESTARIA

637.500,00 €
[IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Formalizar el rol del Centre Balear de Ciberseguretat como órgano técnico de referencia para coordinación, soporte y supervisión	■	■														
2 P	Definir la estructura de gobernanza de la ciberseguridad en la CAIB (órganos, funciones, responsabilidades, incluyendo sector público instrumental)	■	■	■													
3 P	Constituir el Comité de Ciberseguridad de la CAIB (composición, funciones, periodicidad)			■	■												
4 P	Unificar políticas, directrices y procedimientos de ciberseguridad (marco documental común aplicable a toda la Administración autonómica)			■	■	■	■	■									
5 P	Crear un sistema de coordinación interna para intercambio estructurado de información de seguridad entre responsables TIC, equipos operativos y unidades directivas				■	■	■										
6 P	Definir flujos de escalado y toma de decisiones para incidentes, crisis y situaciones de riesgo relevante				■	■	■										
7 P	Establecer un modelo común de gestión del riesgo de ciberseguridad (criterios estandarizados de identificación, evaluación y tratamiento)					■	■	■									
8 P	Establecer canales de coordinación con entes locales y organismos nacionales (consells, ayuntamientos, CCN, INCIBE)						■	■	■	■							
9 C	Implantar mecanismo periódico de seguimiento y reporte (cumplimiento, desviaciones, avance del modelo de gobernanza)								■	▨	▨	▨	▨	▨	▨	▨	▨

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

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 2. Incrementar la resiliencia de la Administración balear frente a ciberincidentes

ESTIMACIÓN PRESUPUESTARIA

7.500.000,00 € [IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Poner en marcha las capacidades operativas del Centre Balear de Ciberseguretat (vigilancia, detección, análisis y respuesta ante incidentes)	■	■														
2 P	Desarrollar repositorio centralizado de alertas, IoCs y amenazas relevantes accesible para los equipos técnicos de la CAIB	■	■														
3 P	Establecer servicio de apoyo técnico inmediato para incidentes significativos en conselleries, entes instrumentales, consells insulars y ayuntamientos		■	■													
4 P	Implantar procedimientos unificados de gestión de incidentes (fases, responsables, flujos de comunicación, tiempos de respuesta, escalados)		■	■	■												
5 C	Realizar análisis periódicos de vulnerabilidades en sistemas y servicios críticos, con priorización y remediación			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
6 P	Coordinar la respuesta a incidentes con organismos nacionales e internacionales (CCN-CERT, INCIBE-CERT, etc.)			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
7 P	Integrar capacidades de recuperación y continuidad, asegurando participación del Centre en activación y coordinación tras incidentes graves				■	■	■										
8 C	Ejecutar ejercicios y simulacros regulares de respuesta ante incidentes (internos y con entidades externas)					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
9 P	Extender capacidades del SOC a consells insulars, ayuntamientos y entes instrumentales del sector público balear					■	■	■	■	■	■	■	■				
10 C	Desarrollar informes operativos periódicos (tendencias, patrones de ataque, deficiencias y mejoras)							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
11 C	Actualizar de forma continua herramientas, procesos y capacidades del Centre, incorporando mejoras tecnológicas y revisiones de procedimientos									▨	▨	▨	▨	▨	▨	▨	▨

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

LÍNEA 03

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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 2. Incrementar la resiliencia de la Administración balear frente a ciberincidentes

ESTIMACIÓN PRESUPUESTARIA

1.000.000,00 € [IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Identificar y clasificar las infraestructuras y servicios esenciales de la Administración balear, incluyendo dependencias técnicas, funcionales y operativas	■	■														
2 P	Desarrollar plan sectorial de ciberseguridad turística	■	■	■	■												
3 P	Realizar análisis de riesgos específicos para cada servicio esencial (impactos, vulnerabilidades, escenarios de interrupción)			■	■												
4 P	Definir requisitos avanzados de seguridad aplicables a los servicios esenciales, alineados con buenas prácticas nacionales e internacionales				■	■											
5 P	Diseñar planes de protección específicos para cada servicio esencial (medidas preventivas, controles reforzados, actuaciones prioritarias)					■	■										
6 C	Coordinar actuaciones con operadores y proveedores clave para servicios externalizados o soportados por terceros					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
7 P	Implementar arquitecturas de red y comunicaciones más robustas (separación y protección de entornos críticos)							■	■	■	■	■	■				
8 C	Establecer procedimientos de supervisión continua (eventos, alertas y métricas integradas en el Centre Balear de Ciberseguretat)							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
9 P	Definir planes de continuidad y recuperación específicos (RTO/RPO coherentes con criticidad del servicio)								■	■							
10 C	Aplicar programas periódicos de revisión y pruebas de seguridad (test de resistencia, revisiones de configuración)									▨	▨	▨	▨	▨	▨	▨	▨
11 C	Realizar ejercicios y simulacros focalizados en servicios esenciales (tiempos de respuesta, coordinación, efectividad)												▨	▨	▨	▨	▨
12 C	Actualizar de forma periódica los planes y medidas, basándose en cambios tecnológicos, nuevas amenazas y lecciones aprendidas													▨	▨	▨	▨

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

LÍNEA 04

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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 2. Incrementar la resiliencia de la Administración balear frente a ciberincidentes

ESTIMACIÓN PRESUPUESTARIA

1.000.000,00 € [IVA N/I]

ACTIVIDADES — **PROYECCIÓN TEMPORAL**

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Reforzar el servicio de Observatorio de Ciberseguridad del Centre Balear de Ciberseguretat, ampliando fuentes, alcance analítico y periodicidad de los informes	■	■														
2 P	Fortalecer la coordinación con organismos nacionales e internacionales para asegurar flujo continuo de indicadores, alertas, vulnerabilidades y buenas prácticas que alimenten al Observatorio	■	■														
3 P	Poner en marcha el Laboratorio de Ciberseguridad, coordinado con el Observatorio, para validar nuevas soluciones de seguridad y analizar técnicas emergentes de ataque		■	■	■	■	■	■	■	■	■	■	■				
4 P	Integrar capacidades de análisis avanzado (threat intelligence) en el Observatorio: correlación de datos, enriquecimiento de indicadores e informes de riesgo adaptados a Administración, empresas y entidades locales			■	■	■	■	■	■								
5 C	Crear un programa de vigilancia tecnológica continua centrado en tecnologías disruptivas (IA, automatización, nuevas arquitecturas de red, identidades digitales avanzadas, IoT)			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
6 C	Publicar informes estratégicos periódicos que sinteticen riesgos emergentes, tendencias tecnológicas y recomendaciones para la toma de decisiones				▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
7 P	Desarrollar un sistema de alerta temprana basado en la información del Observatorio y en contribuciones de organismos nacionales e internacionales					■	■	■	■								
8 C	Realizar ejercicios de prospectiva y análisis de escenarios para identificar amenazas futuras, evaluar probabilidad e impacto y definir medidas preventivas							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
9 C	Incorporar los resultados del Observatorio en la planificación de la CAIB (políticas, arquitecturas, prioridades de inversión y medidas de protección)												▨	▨	▨	▨	▨

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

LÍNEA 05

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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 3. Impulsar la colaboración institucional para mejorar las capacidades de ciberseguridad.

ESTIMACIÓN PRESUPUESTARIA

500.000,00 €
[IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Establecer un marco formal de cooperación interadministrativa entre CAIB, consells insulars, ayuntamientos, FFCCSE y entes instrumentales, articulado desde el Centre Balear de Ciberseguretat																
2 P	Establecer canales formales de coordinación con organismos nacionales especializados en ciberseguridad (CCN, INCIBE) para intercambio de información, alertas, guías y recursos técnicos																
3 P	Crear comités y grupos de trabajo permanentes en materia de ciberseguridad con representación técnica y directiva de todas las administraciones del territorio balear																
4 C	Reforzar la cooperación con consells insulars, ayuntamientos y FFCCSE mediante mecanismos continuos de comunicación, apoyo técnico y coordinación operativa																
5 P	Definir procedimientos compartidos de coordinación ante incidentes (flujos de comunicación, criterios de escalado, pautas de actuación coordinada)																
6 P	Consolidar acuerdos de cooperación con organismos nacionales (CCN, INCIBE) mediante protocolos de intercambio, coordinación de alertas, participación en programas conjuntos																
7 P	Formalizar acuerdos de colaboración con otras comunidades autónomas que dispongan de centros de ciberseguridad o CSIRTs regionales																
8 P	Definir protocolos de interlocución estable con instituciones europeas en materia de ciberseguridad (ENISA, redes de CSIRTs, ECCC)																
9 C	Favorecer la participación de las Illes Balears en redes y foros europeos e internacionales, asegurando alineación con ENS y NIS2																
10 C	Impulsar proyectos y actuaciones conjuntas entre administraciones (ejercicios, pilotos tecnológicos, formación compartida, documentación común)																
11 C	Establecer un sistema de seguimiento y evaluación del modelo de cooperación (indicadores de actividad, participación, eficacia, alineación)																

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

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 4. Reforzar el posicionamiento de las Illes Balears en el ecosistema nacional de ciberseguridad

ESTIMACIÓN PRESUPUESTARIA

250.000,00 €
[IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 C	Establecer la participación del Centre Balear de Ciberseguretat en redes y foros nacionales de ciberseguridad (CCN, INCIBE y otros organismos de referencia)			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
2 P	Crear un programa institucional de alianzas estratégicas con asociaciones sectoriales, universidades, agencias públicas y entidades tecnológicas					■	■	■	■								
3 C	Impulsar la presencia de las Illes Balears en eventos, congresos y jornadas de ciberseguridad mediante ponencias, intervenciones y presentación de proyectos regionales							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
4 C	Representar a las Illes Balears en iniciativas y grupos de trabajo estatales y europeos, contribuyendo a la definición de políticas, estándares y líneas estratégicas								▨	▨	▨	▨	▨	▨	▨	▨	▨
5 C	Desarrollar acciones de posicionamiento institucional coordinado (publicaciones estratégicas, informes de capacidades regionales, materiales divulgativos)									▨	▨	▨	▨	▨	▨	▨	▨
6 C	Favorecer la integración del ecosistema balear de ciberseguridad en redes colaborativas, facilitando la participación de empresas y agentes de innovación en plataformas nacionales e internacionales												▨	▨	▨	▨	▨

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

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 5. Potenciar el desarrollo de una industria de ciberseguridad en las Illes Balears

ESTIMACIÓN PRESUPUESTARIA

500.000,00 € [IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	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 del ecosistema de ciberseguridad de las Illes Balears (empresas especializadas, proveedores TIC, startups, clústeres, hubs, centros de investigación, asociaciones)																
2 P	Diseñar mecanismos de innovación abierta o compra pública innovadora en materia de ciberseguridad — modelo GovTechLab —, posicionando a la Administración balear como «cliente tractor».																
3 P	Diseñar un plan de desarrollo sectorial de la industria de ciberseguridad balear (objetivos, prioridades, recursos, horizonte temporal)																
4 P	Crear un observatorio del ecosistema de ciberseguridad balear, integrado en el Centre Balear de Ciberseguretat																
5 P	Impulsar un programa de apoyo a empresas y startups de ciberseguridad (mentorización, sandboxes, acompañamiento)																
6 C	Establecer reconocimientos o premios periódicos a iniciativas destacadas en ciberseguridad (proyectos empresariales, soluciones innovadoras, buenas prácticas)																
7 C	Impulsar proyectos tractores de ciberseguridad en sectores estratégicos de la economía balear (turismo, servicios, logística, salud)																
8 C	Impulsar el posicionamiento de las Illes Balears como laboratorio de ciberresiliencia en entornos insulares y turísticos (proyectos piloto, publicaciones, foros)																

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

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 5. Potenciar el desarrollo de una industria de ciberseguridad en las Illes Balears

ESTIMACIÓN PRESUPUESTARIA

250.000,00 € [IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Crear espacios de colaboración estables entre administración, empresas tecnológicas y agentes de innovación, coordinados desde el Centre Balear de Ciberseguretat	■	■	■	■												
2 C	Impulsar iniciativas de dinamización empresarial (encuentros sectoriales, mesas técnicas, jornadas de innovación, foros especializados)					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
3 C	Establecer acuerdos de colaboración público-privada con empresas especializadas (proyectos piloto, capacidades avanzadas)								▨	▨	▨	▨	▨	▨	▨	▨	▨
4 C	Fomentar la visibilidad y difusión de las capacidades empresariales del territorio (catálogos sectoriales, repositorios de soluciones, eventos de presentación)									▨	▨	▨	▨	▨	▨	▨	▨
5 C	Promover mecanismos de cooperación entre empresas locales y otros polos de referencia (misiones tecnológicas, redes temáticas, conexión con ecosistemas nacionales e internacionales)										▨	▨	▨	▨	▨	▨	▨
6 C	Impulsar proyectos de emprendimiento y crecimiento empresarial (startups y pymes en innovación, laboratorios, aceleración vinculada al sistema balear de I+D+i)											▨	▨	▨	▨	▨	▨

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

LÍNEA 09

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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 6. Fomentar la investigación e innovación en ciberseguridad

ESTIMACIÓN PRESUPUESTARIA

3.000.000,00 €
[IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 C	Organizar seminarios, jornadas técnicas y foros de investigación e innovación para conectar grupos de investigación, empresas y entidades públicas			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
2 C	Impulsar proyectos de investigación aplicada en ciberseguridad							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
3 C	Promover la participación del ecosistema balear en programas de I+D+i								▨	▨	▨	▨	▨	▨	▨	▨	▨
4 P	Crear un programa estructurado de transferencia de conocimiento									■	■	■					
5 C	Crear repositorios y publicaciones técnicas periódicas (resultados de investigación, estudios sectoriales, análisis de tendencias, experiencias piloto)										▨	▨	▨	▨	▨	▨	▨
6 C	Incorporar la investigación y la innovación en la evolución de los servicios del Centre Balear de Ciberseguretat												▨	▨	▨	▨	▨

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

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 7. Atraer, generar y fidelizar talento especializado en ciberseguridad en el territorio balear

ESTIMACIÓN PRESUPUESTARIA

1.000.000,00 € [IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Diseñar un marco formativo integral en ciberseguridad estructurado en niveles (básico, intermedio y avanzado) alineado con ENS, NIS2 y guías CCN-STIC	■	■														
2 P	Desplegar programas de formación continua para el personal empleado público impartidos desde el Centre Balear de Ciberseguretat (buenas prácticas, protección de datos, gestión segura, uso seguro de sistemas)			■	■	■	■	■	■	■	■	■	■	■	■	■	■
3 P	Coordinar un repositorio formativo centralizado integrado en el Centre (recursos educativos, materiales didácticos, contenidos audiovisuales, guías técnicas)					■	■	■	■								
4 P	Impulsar programas formativos para jóvenes y futuros profesionales (semanas de la ciberseguridad, charlas en centros educativos, laboratorios, actividades STEM)					■	■	■	■	■	■	■	■	■	■	■	■
5 P	Crear un catálogo de cursos avanzados y talleres técnicos especializados (EDR, SIEM, análisis forense, gestión de incidentes, automatización de seguridad)							■	■	■	■						
6 P	Integrar asignaturas, módulos y competencias de ciberseguridad en los itinerarios formativos oficiales de la UIB, centros de FP y programas especializados								■	■	■	■	■				
7 P	Establecer programas de certificación y microcredenciales en ciberseguridad reconocidas (auditoría, análisis de malware, gestión de riesgos)								■	■	■	■					

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

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 7. Atraer, generar y fidelizar talento especializado en ciberseguridad en el territorio balear

ESTIMACIÓN PRESUPUESTARIA

1.000.000,00 € [IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Establecer programas de prácticas y estancias formativas en empresas			■	■												
2 P	Organizar competiciones y actividades de detección de talento (CTF, hackathons, retos, laboratorios) para fomentar vocaciones tempranas e identificar perfiles destacados					■	■	■	■	■	■	■	■	■	■	■	■
3 P	Crear una bolsa de empleo sectorial en ciberseguridad gestionada por el Centre Balear de Ciberseguretat					■	■	■	■								
4 P	Impulsar acuerdos universidad-empresa (proyectos conjuntos, TFG/TFM aplicados a necesidades reales, programas de mentoría)						■	■	■	■	■	■	■	■	■	■	■
5 P	Desarrollar itinerarios profesionales especializados (rutas de progresión para perfiles técnicos, analistas y gestores con formación, experiencia y certificaciones)									■	■	■					
6 P	Poner en marcha programas de fidelización del talento formado en las islas (oportunidades de desarrollo profesional, participación en proyectos estratégicos, formación avanzada con la UIB)												■	■	■	■	■

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

LÍNEA 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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 8. Reforzar la ciberresiliencia del tejido empresarial balear

ESTIMACIÓN PRESUPUESTARIA

2.100.000,00 €
[IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1 P	Desarrollar herramientas de autodiagnóstico de ciberseguridad para pymes, adaptadas a la realidad empresarial balear																
2 C	Promover ciclos de FP Dual en ciberseguridad mediante un modelo de alternancia centro educativo-empresa que garantice la adquisición de competencias prácticas aplicables al mercado laboral balear.																
3 P	Establecer un servicio estable de acompañamiento técnico desde el Centre Balear de Ciberseguretat para asesorar a empresas en medidas básicas, configuraciones y resolución de dudas																
4 P	Elaborar guías sectoriales de seguridad digital (turismo, comercio, logística, servicios) alineadas con ENS, NIS2 y CCN-STIC																
5 P	Poner en marcha un programa de alertas técnicas dirigido a empresas (vulnerabilidades, configuraciones críticas, medidas recomendadas) apoyado en el Observatorio																
6 C	Organizar talleres y jornadas empresariales (protección de activos, gestión de riesgos, buenas prácticas)																
7 P	Impulsar la adopción de soluciones seguras y servicios certificados mediante criterios objetivos que orienten a pymes y micropymes																

Ejecución / implantación Operación continua / recurrente P Puntual C Continua

LÍNEA 13

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

OBJETIVO ESTRATÉGICO IMPACTADO

OBJETIVO 9. Desarrollar una cultura sólida de ciberseguridad en la ciudadanía

ESTIMACIÓN PRESUPUESTARIA

1.750.000,00 € [IVA N/I]

ACTIVIDADES

PROYECCIÓN TEMPORAL

#	Actividad	2027				2028				2029				2030			
		T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
1	Elaborar materiales divulgativos accesibles (infografías, vídeos breves, guías prácticas) sobre riesgos digitales comunes y hábitos responsables (P)																
2	Diseñar y ejecutar campañas periódicas de concienciación en ciberseguridad dirigidas a la ciudadanía balear (medios digitales, redes sociales, instituciones públicas, soportes locales) (P)																
3	Crear un portal ciudadano de ciberseguridad integrado en el Centre Balear de Ciberseguretat (recursos, alertas verificadas, recomendaciones, autoevaluaciones, guías) (P)																
4	Establecer un sistema de avisos y alertas públicas sobre fraudes, estafas y riesgos emergentes mediante canales digitales institucionales (P)																
5	Habilitar un canal de consulta y orientación básica en ciberseguridad para dudas habituales (fraudes, protección de información personal, uso seguro de dispositivos) (P)																
6	Desarrollar talleres y sesiones de alfabetización digital segura en colaboración con ayuntamientos, consells, asociaciones y entidades educativas (P)																
7	Establecer acuerdos de colaboración con entidades educativas, asociaciones de consumidores, organizaciones sociales y medios de comunicación para la difusión coordinada de mensajes clave (P)																
8	Implementar programas de sensibilización específicos para colectivos con mayor vulnerabilidad digital (personas mayores, jóvenes, baja alfabetización digital, nuevas familias digitales) (P)																
9	Organizar actividades participativas (retos, gamificación, campañas temáticas, concursos educativos) para fomentar el aprendizaje activo (P)																
10	Evaluar periódicamente el impacto de las acciones de sensibilización (indicadores de participación, alcance, satisfacción, adopción de buenas prácticas) y ajustar las actuaciones (P)																

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

06 Evolución progresiva de capacidades

La presente hoja de ruta ordena el despliegue de la Estrategia Balear de Ciberseguridad, ofreciendo una visión sintética de la secuencia de implantación, la priorización de las líneas de actuación y la evolución progresiva de las capacidades a consolidar en el territorio.

La Estrategia agrupa actuaciones orientadas a reforzar la gobernanza de la ciberseguridad, mejorar la prevención, detección y respuesta ante incidentes, proteger los servicios esenciales, apoyar al tejido empresarial, impulsar el talento y la innovación, y promover una cultura de ciberseguridad entre la ciudadanía.

Para facilitar una ejecución gradual, flexible y orientada a resultados, la hoja de ruta se estructura en tres etapas progresivas:

- **Etapa Fundacional:** establece las bases institucionales, organizativas, normativas y operativas de la Estrategia como son la gobernanza única CAIB, marco normativo común, plena operación del Centre Balear de Ciberseguretat y cumplimiento ENS/NIS2 en los servicios esenciales.
- **Etapa de Escalado:** extiende las capacidades al conjunto del territorio, incluyendo administraciones locales, tejido empresarial, sectores estratégicos, talento y ciudadanía.
- **Etapa de Posicionamiento:** consolida a les Illes Balears como territorio de referencia en ciberseguridad, reforzando su presencia en redes nacionales e internacionales, su ecosistema innovador y su capacidad de atracción de inversión y talento.

Estas etapas no constituyen compartimentos cerrados ni fases estrictamente secuenciales. La priorización identifica el foco predominante de cada momento, manteniendo la flexibilidad necesaria para adaptar la ejecución a la evolución del contexto tecnológico, presupuestario y de amenazas.

MADUREZ CRECIENTE DE LAS CAPACIDADES

Etapa 1: FUNDACIONAL (Crear las bases comunes)	Etapa 2: ESCALADO (Extender capacidades al territorio)	Etapa 3: POSICIONAMIENTO (Consolidar liderazgo y referencia)
Cimientos institucionales, organizativos, normativos y operativos de la Estrategia	**Ampliación de capacidades hacia consells, ayuntamientos, empresas, talento y ciudadanía**	**Proyección de les Illes Balears como territorio de referencia en ciberseguridad**
L1 Gobernanza de la ciberseguridad en la Administración de les Illes Balears	**L2** Extensión de capacidades operativas, ejercicios y mejora continua	**L4** Prospectiva, escenarios futuros y adaptación estratégica ante riesgos emergentes
L2 Operación inicial del Centre Balear de Ciberseguretat	**L3** Implantación de medidas reforzadas en infraestructuras y servicios esenciales	**L6** Presencia institucional en redes, foros y espacios de colaboración
L3 Identificación y protección inicial de servicios esenciales	**L5** Cooperación interadministrativa consolidada y procedimientos compartidos	**L7** Industria y ecosistema balear especializado en ciberseguridad
L4 Observatorio, riesgos emergentes y vigilancia tecnológica	**L8** Dinamización empresarial y cooperación público-privada	**L8** Ecosistema empresarial conectado con otros polos de referencia
L5 Coordinación institucional inicial con administraciones y organismos de referencia	**L10** Formación avanzada, repositorio formativo y colaboración educativa	**L9** Investigación, innovación y transferencia de conocimiento
L10 Marco formativo inicial y formación continua para personal empleado público	**L11** Prácticas, bolsa de empleo, retos y acuerdos universidad-empresa	**L11** Atracción y fidelización sostenida de talento especializado
L12 Herramientas básicas y acompañamiento inicial al tejido empresarial	**L12** Programas de mejora de la ciberresiliencia empresarial	**L13** Cultura ciudadana madura, evaluada y ajustada de forma continua
L13 Materiales, portal y campañas ciudadanas de concienciación	**L13** Talleres, alfabetización digital segura y campañas para colectivos específicos	

Nota: las etapas son progresivas y solapadas. Cada línea de actuación puede mantenerse activa en más de una etapa, aunque con diferente grado de intensidad.

07

Seguimiento, medición y evaluación

La Estrategia Balear de Ciberseguridad, con un horizonte de vigencia de 4 años (2027–2030), requiere un modelo de seguimiento que permita evaluar de forma continua el grado de avance de sus líneas de actuación y su impacto real en la Administración, las empresas y la ciudadanía. Este modelo es esencial para garantizar la adecuada ejecución de la Estrategia, identificar desviaciones a tiempo y orientar las decisiones necesarias para asegurar su eficacia a lo largo de todo su ciclo de vigencia.

El presente apartado establece las bases del sistema de seguimiento, medición y evaluación que deberá desarrollarse de forma detallada en el plan de acción que concrete la ejecución de esta Estrategia. En este sentido, no se pretende definir aquí el catálogo exhaustivo de indicadores ni los procedimientos operativos de reporte, sino fijar los principios, la estructura y los criterios que garanticen un seguimiento coherente, riguroso y alineado con los objetivos estratégicos.

Para ello, este marco se articula en torno a tres componentes:

- **Definición de la gobernanza del seguimiento**, articulado en tres niveles complementarios —estratégico, táctico y operativo— que determinan la responsabilidad, su alcance, así como la periodicidad de cada una de las actuaciones.
- **Identificación de los ámbitos de medición e indicadores**, que agrupan las dimensiones clave sobre las que se evaluará el despliegue de la Estrategia.
- **Definición de los mecanismos de revisión**, que garantizará su adaptación continua a los cambios en el entorno de amenazas, la evolución tecnológica y las lecciones aprendidas durante su ejecución.

La información generada por este sistema se integrará en un cuadro de mando accesible para los órganos de gobernanza, facilitando la toma de decisiones basada en evidencia y asegurando que la Estrategia se mantenga viva, relevante y alineada con las necesidades reales del territorio.

7.1

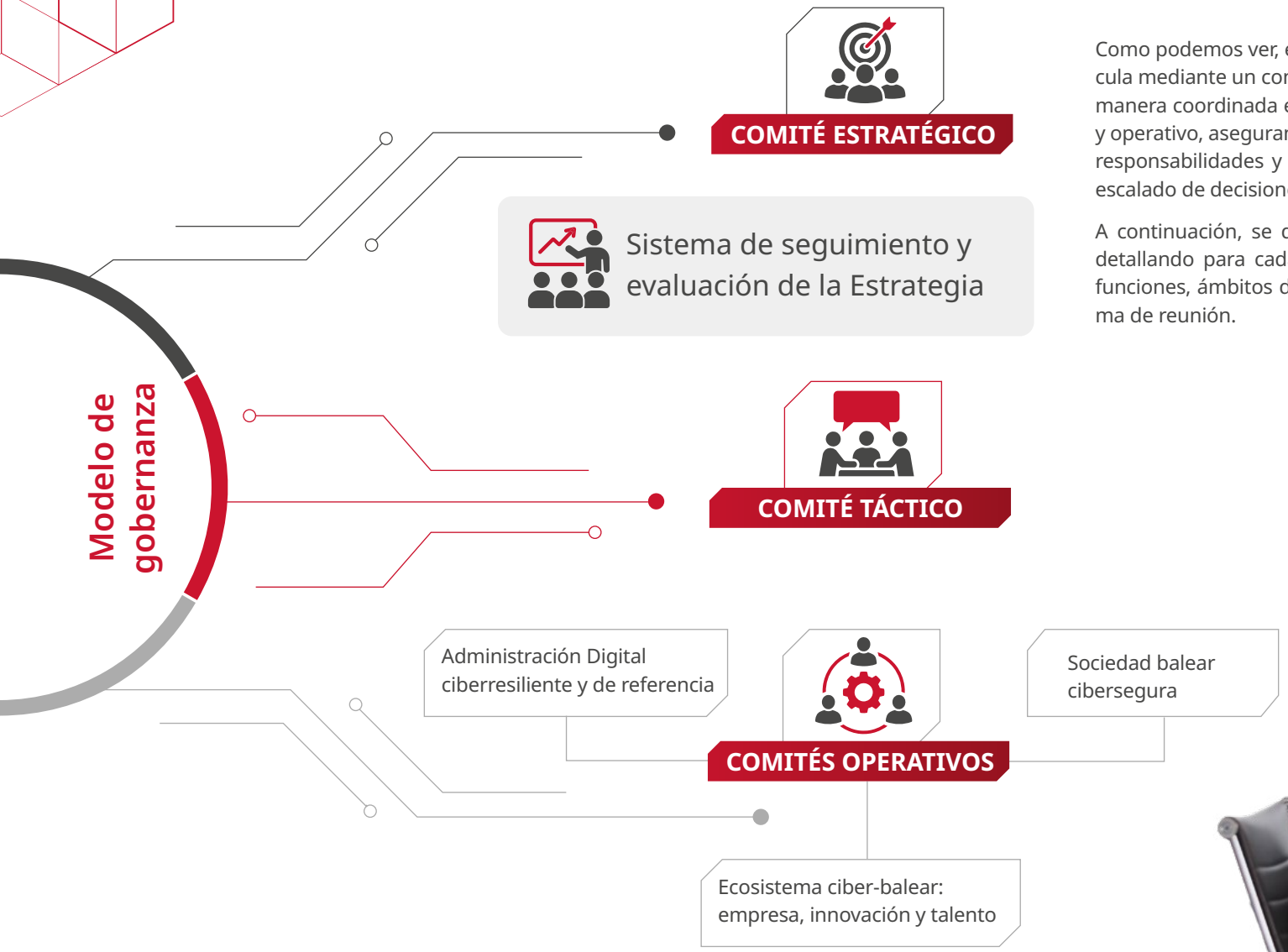
Modelo de seguimiento

El seguimiento de la Estrategia se articulará mediante un modelo estructurado y sistemático, orientado a garantizar el control del grado de avance, la identificación temprana de desviaciones y la toma de decisiones informadas para su corrección. Este modelo se apoya en una estructura de tres niveles complementarios, alineados con el modelo de gobernanza definido para la Estrategia:

- **Nivel estratégico.** Orientado a evaluar el avance global de la Estrategia respecto a sus objetivos y ejes, con una periodicidad anual. Esta evaluación será responsabilidad del órgano de gobernanza de la Estrategia y se materializará en un informe anual de progreso que sintetice los avances alcanzados, las desviaciones detectadas y, en su caso, las recomendaciones de ajuste.
- **Nivel táctico.** Centrado en el seguimiento trimestral del despliegue de las líneas de actuación y de los hitos intermedios asociados a cada una de ellas. Este seguimiento será coordinado por el Centre Balear de Ciberseguretat y permitirá detectar bloqueos, reasignar prioridades y proponer medidas correctoras de forma ágil, asegurando la coherencia entre la planificación estratégica y su ejecución.
- **Nivel operativo.** Basado en la monitorización continua de indicadores técnicos y de actividad vinculados a la operación diaria del Centre Balear de Ciberseguretat y de los servicios de ciberseguridad desplegados. Estos indicadores alimentarán los niveles táctico y estratégico mediante reporting mensual, proporcionando una visión detallada y actualizada del estado de ejecución.

Este modelo garantiza un flujo de información ascendente, desde la operación diaria hasta la evaluación estratégica, que permite que las decisiones de gobierno de la Estrategia se fundamenten en datos reales, trazables y actualizados.

A modo de síntesis, la Figura de a continuación recoge de forma esquemática la relación entre los distintos niveles de seguimiento y los órganos responsables de cada uno de ellos.



Como podemos ver, el modelo de gobernanza se articula mediante un conjunto de comités que operan de manera coordinada en los niveles estratégico, táctico y operativo, asegurando una adecuada separación de responsabilidades y un mecanismo estructurado de escalado de decisiones, riesgos y desviaciones.

A continuación, se describen los comités definidos, detallando para cada uno de ellos su composición, funciones, ámbitos de actuación y periodicidad mínima de reunión.

	Comité Estratégico	Comité Táctico
Comités		**C**
Miembros	• Director Gerente de IB-Digital • Dirección General de Innovación y Transformación Digital • Dirección General de Estrategia Digital y Desarrollo Tecnológico • Representante de IB-Salut • Representantes de FFCCSE • Representante de la UIB	**M** • Responsable de la Estrategia del Centre Balear de Ciberseguretat • Representantes de la Direcciones Generales con competencias en la implementación de la Estrategia • Representantes de organismos con competencias en la implementación de la Estrategia
Funciones	• Análisis del cumplimiento y actualización de los objetivos de la Estrategia • Supervisión global del riesgo de ciberseguridad en les Illes Balears • Toma de decisiones estratégicas • Análisis global de indicadores relevantes	**F** • Análisis del riesgo de ciberseguridad en les Illes Balears • Medición del cumplimiento de los objetivos de la Estrategia • Análisis y gestión de presupuestos • Establecimiento de mecanismos de financiación • Seguimiento y coordinación de las líneas de actuación • Evaluación del impacto de la Estrategia por grupos de interés • Análisis de las actividades e hitos completados • Planificación de nuevas actividades • Toma de decisiones tácticas • Definición y supervisión de indicadores • Gestión de riesgos • Resolución de problemas, escalando aquellos fuera de su ámbito
Ambitos de actuación	• Transversal	**A** • Transversal
Periodicidad mínima	• Anual	**P** • Trimestral

C

Comités Operativos

M

- Responsables de las líneas de actuación del Centre Balear de Ciberseguretat
- Responsables de ejecución de las Direcciones Generales con competencias en la implementación de la Estrategia
- Responsables de ejecución de organismos con competencias en la implementación de la Estrategia
- Representantes del ecosistema empresarial de Ciberseguridad
- Representantes del tejido empresarial Balear

F

- Ejecución de presupuestos
- Definición de metodologías de trabajo y acciones operativas
- Seguimiento detallado de actividades y tareas asociadas
- Análisis de las tareas completadas
- Planificación de nuevas tareas
- Toma de decisiones operativas
- Medición y mantenimiento de indicadores
- Escalado de riesgos
- Escalado de problemas

A

- Transformación de la Administración
- Estrategia y tendencias
- Capacitación y concienciación
- Ciberseguridad en empresas
- Colaboración y cooperación

P

- Mensual

C Comité

M Miembros

F Funciones

A Ámbitos de actuación

P Periodicidad mínima

En conjunto, este esquema de gobernanza, alineado con el modelo de seguimiento descrito, permite asegurar:

- Una dirección estratégica clara, basada en información consolidada.
- Una coordinación eficaz del despliegue de las líneas de actuación.
- Un control operativo continuo, apoyado en indicadores objetivos.

Todo ello constituye un elemento clave para garantizar la eficacia, trazabilidad y sostenibilidad de la Estrategia a lo largo de su ciclo de vida.

7.2

Ámbitos de medición

Para evaluar de forma equilibrada el progreso de la Estrategia en todas sus dimensiones, el sistema de seguimiento se organizará en torno a siete ámbitos de medición. Estos ámbitos no constituyen indicadores en sí mismos, sino las dimensiones estratégicas sobre las que se deberán definir indicadores concretos, incluyendo para cada uno de ellos su método de cálculo, la fuente de datos, la periodicidad de medición, el valor de referencia inicial (*baseline*) y la meta a alcanzar:

1. **Nivel de madurez y resiliencia de la Administración balear.** Incluye aspectos como la capacidad de prevención, detección y respuesta, la continuidad de los servicios esenciales y la evolución del modelo de gobernanza.
2. **Progreso en el despliegue del Centre Balear de Ciberseguretat y sus servicios.** Monitorizando su operación, servicios compartidos, soporte a entidades locales y actuaciones de vigilancia y observatorio.
3. **Estado y evolución de la cultura de ciberseguridad en la ciudadanía y el empleo público.** Medido a través de acciones formativas, niveles de participación y mejora en conductas seguras.
4. **Madurez y preparación del tejido empresarial balear.** Diagnósticos, adopción de medidas básicas, participación en programas y evolución del nivel de ciberprotección empresarial.
5. **Fortalecimiento del ecosistema regional de ciberseguridad.** Desarrollo del sector, participación en iniciativas, colaboración con la UIB, Fundació Bit, ADR, SOIB, Educación, asociaciones empresariales, cámaras de comercio, y ecosistema de innovación.
6. **Captación y sostenibilidad de la financiación para ciberseguridad.** Seguimiento de la inversión, estabilidad presupuestaria y capacidad para mantener y evolucionar servicios críticos.
7. **Progreso en cooperación institucional y participación en redes nacionales e internacionales.** Conexión con organismos estatales y europeos, compartición de información y participación en iniciativas conjuntas.

La definición detallada de los indicadores asociados a cada ámbito se realizará en el plan de acción, asegurando su vinculación directa con los objetivos estratégicos y las líneas de actuación de la Estrategia. No obstante, como orientación para dicho desarrollo, cada indicador deberá responder a criterios de relevancia (que mida lo que realmente importa), viabilidad (que sea medible con los datos disponibles), claridad (que su interpretación sea inequívoca) y accionabilidad (que su resultado permita tomar decisiones concretas).

7.3

Revisión y actualización

El sistema de seguimiento incorporará un mecanismo formal de revisión y actualización de la propia Estrategia, con el objetivo de garantizar su adecuación permanente al contexto cambiante de la ciberseguridad y a las necesidades reales de les Illes Balears.

Con carácter anual, el informe de progreso elaborado en el marco del nivel estratégico incluirá, además de la evaluación del grado de avance y cumplimiento de los objetivos, una valoración específica sobre los siguientes aspectos:

- La vigencia y adecuación de los objetivos estratégicos en relación con la evolución del contexto de amenazas, riesgos y prioridades.
- La idoneidad de las líneas de actuación, considerando tanto su nivel de ejecución como su contribución efectiva a los objetivos de la Estrategia.
- La necesidad de introducir ajustes derivados de cambios normativos, avances tecnológicos, evolución del entorno institucional o lecciones aprendidas durante la ejecución.

Como resultado de este proceso de revisión, podrá proponerse, cuando proceda:

- La actualización o reformulación de líneas de actuación.
- La incorporación de nuevas actividades o proyectos.
- La revisión de indicadores y metas asociadas.
- La reasignación de prioridades o recursos, de acuerdo con los mecanismos de gobernanza establecidos.

De este modo, el seguimiento, la medición y la evaluación se articulan como un proceso continuo, integrado y cíclico, que puede representarse de la siguiente forma:

Este enfoque permite asegurar que la Estrategia Balear de Ciberseguridad se mantenga actualizada, relevante y alineada con la evolución del contexto tecnológico, normativo y de amenazas a lo largo de todo su periodo de vigencia.

Al término del periodo de vigencia de la Estrategia, se llevará a cabo una evaluación final, orientada a valorar los resultados globales alcanzados, el grado de cumplimiento de los objetivos estratégicos y las principales lecciones aprendidas. Esta evaluación servirá como base para la definición de la siguiente Estrategia, garantizando la continuidad y madurez del modelo.

No obstante, la vocación de la presente Estrategia trasciende su marco temporal, sentando las bases de un modelo de ciberseguridad territorial sostenible, evolutivo y orientado a la mejora continua.

Anexo
Memoria económica de la Estrategia

La presente Memoria Económica tiene por objeto justificar y dimensionar el esfuerzo presupuestario asociado al despliegue de la Estrategia de Ciberseguridad, alineando los objetivos estratégicos y las líneas de actuación definidas con una estimación económica coherente, realista y sostenible en el tiempo.

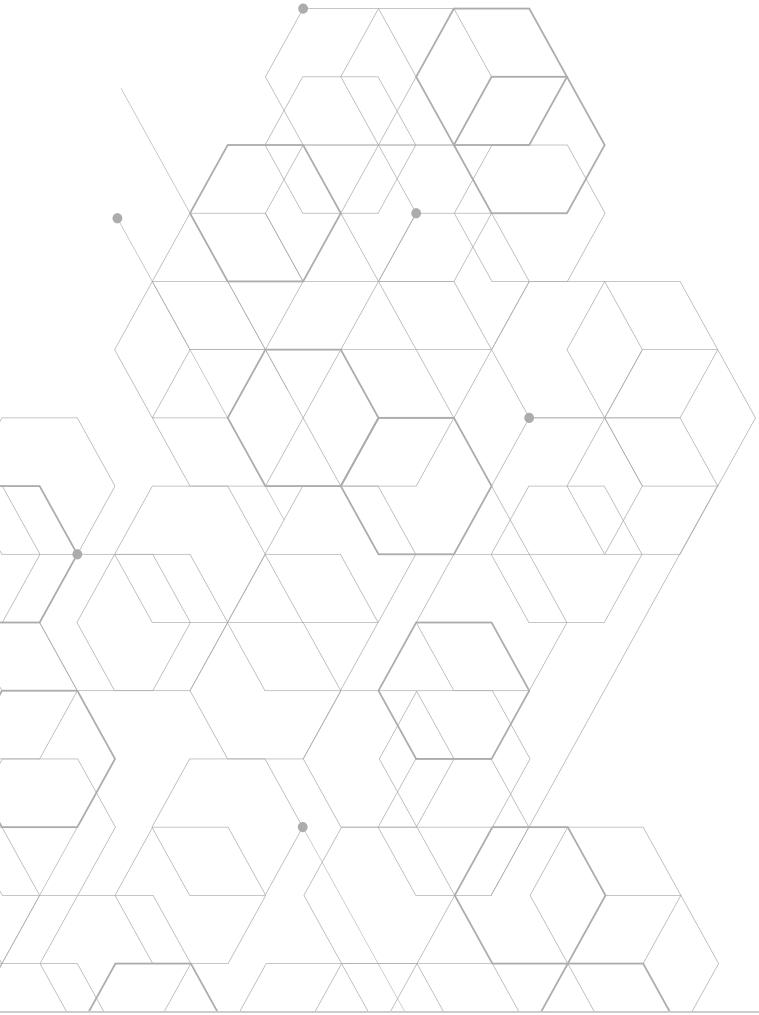
En este sentido, el conjunto de actuaciones contempladas en la Estrategia supone una **inversión total estimada de 20,5 millones de euros**, planificada de manera progresiva conforme a los distintos horizontes temporales de ejecución y al modelo de gobernanza propuesto.

A continuación, se recoge la estimación económica para los distintos niveles estratégicos presentados en el documento:

#	Ejes	Presupuesto estimado
1	Administración Digital ciberresiliente y de referencia	10.887.500,00 €
2	Ecosistema ciber-balear: empresa, innovación y talento	5.750.000,00 €
3	Sociedad balear cibersegura	3.850.000,00 €
	Total	**20.487.500,00 €**

#	Objetivos estratégicos	Presupuesto estimado
1	Establecer un marco robusto y efectivo de gobernanza de la ciberseguridad	637.500,00 €
2	Incrementar la resiliencia de los servicios públicos frente a ciberincidentes	9.500.000,00 €
3	Impulsar la colaboración institucional para mejorar las capacidades de ciberseguridad	500.000,00 €
4	Reforzar el posicionamiento de las Illes Balears en el ecosistema nacional de ciberseguridad	250.000,00 €
5	Potenciar el desarrollo de una industria de ciberseguridad en las Illes Balears	750.000,00 €

#	Objetivos estratégicos	Presupuesto estimado
6	Fomentar la investigación e innovación en ciberseguridad	3.000.000,00 €
7	Atraer, generar y fidelizar talento especializado en ciberseguridad en el territorio balear	2.000.000,00 €
8	Reforzar la ciberresiliencia del tejido empresarial balear	2.100.000,00 €
9	Desarrollar una cultura sólida de ciberseguridad en la ciudadanía	1.750.000,00 €
	Total	**20.487.500,00 €**



#	Líneas de actuación	Presupuesto estimado
1	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	637.500,00 €
2	Desarrollar y reforzar las capacidades de prevención, detección y respuesta frente a ciberincidentes mediante la operación y mejora continua del Centre Balear de Ciberseguretat	7.500.000,00 €
3	Desarrollar planes y medidas específicas para la protección de infraestructuras y servicios esenciales siguiendo estándares avanzados de seguridad	1.000.000,00 €
4	Reforzar la capacidad de anticipación y adaptación de las Illes Balears frente a riesgos emergentes y tecnologías disruptivas	1.000.000,00 €
5	Desarrollo de marcos estables de coordinación, cooperación institucional y posicionamiento en materia de ciberseguridad, a nivel territorial, nacional e internacional	500.000,00 €
6	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	250.000,00 €
7	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	500.000,00 €

#	Líneas de actuación	Presupuesto estimado
8	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	250.000,00 €
9	Impulso de programas de investigación, innovación y transferencia de conocimiento en ciberseguridad, en colaboración con universidades y ecosistema de I+D+i balear	3.000.000,00 €
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	1.000.000,00 €
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	1.000.000,00 €
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	2.100.000,00 €
13	Promoción de la concienciación, sensibilización y buenas prácticas en ciberseguridad en la ciudadanía balear, fomentando un uso seguro y responsable de las TIC	1.750.000,00 €
	Total	**20.487.500,00 €**