



## Secció III. Altres disposicions i actes administratius CONSELL INSULAR D'EIVISSA

4211

*Acord del Consell Executiu del Consell per a l'aprovació de la política de seguretat de les tecnologies de la informació i les comunicacions del Consell Insular d'Eivissa*

Per acord del Consell Executiu del Consell Insular d'Eivissa en sessió celebrada en data 24 de març de 2023, s'ha aprovat per unanimitat la proposta per a l'aprovació de la política de seguretat de les tecnologies de la informació i les comunicacions del Consell Insular d'Eivissa, del tenor literal següent:

"Atès el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), que substitueix al Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, el qual obliga al Consell Insular d'Eivissa a definir la política de seguretat en l'àmbit de les seues competències per tal d'assolir els objectius legals definits a l'ENS.

Vist que l'Esquema Nacional de Seguretat persegueix els següents grans objectius:

- Crear les condicions necessàries de seguretat en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeti l'exercici de drets i el compliment de deures mitjançant aquests mitjans.
- Definir les responsabilitats del personal del Consell Insular d'Eivissa
- Promoure la gestió continuada de la seguretat.
- Promoure la prevenció, detecció i correcció per a una millor resiliència en l'escenari de ciberamenaces i ciberatacs.
- Promoure un tractament homogeni de la seguretat que faciliti la cooperació en la prestació de serveis públics digitals quan participen diverses entitats. Això suposa proporcionar els elements comuns que han de guiar l'actuació de les entitats del Sector Públic i dels seus proveïdors tecnològics en matèria de seguretat de les tecnologies de la informació.
- Servir de model de bones pràctiques, en línia amb l'apuntat a les recomanacions de l'OCDE Digital Security Risk Management for Economic and Social Prosperity OECD
- Recommendation and Companion Document.

Vistos els articles 11, 12 i 13 del RD 311/2022, on es regula la diferenciació de les responsabilitats en matèria de seguretat, així com el marc regulador de la política de seguretat que el Consell Insular d'Eivissa ha d'incorporar.

Atesa la proposta del cap de Secció de Sistemes d'Informació i Seguretat de data 20 de març de 2023.

Per tot l'anterior, en virtut de les facultats que tenc conferides, pels Decrets de Presidència de data 10 de juliol de 2019 (publicats en el BOIB núm. 95 de 11 de juliol de 2019) pel qual es regula l'estructura orgànica del Consell Insular d'Eivissa, de data 16 de juliol de 2019, pel que es determinen les atribucions dels diferents òrgans de la Corporació (publicat en el BOIB núm. 98 de 17 de juliol de 2019), elev al Consell Executiu la següent,

### PROPOSTA

**Primer.** Aprovar la política de seguretat de les tecnologies de la informació i les comunicacions del Consell Insular d'Eivissa, basada en el document que es transcriu a continuació,

#### “Sumari

1. Introducció.....	3
2. La seguretat com a procés integral.....	3
2.1. Prevenció.....	3
2.2. Detecció.....	4
2.3. Resposta.....	4
2.4. Recuperació.....	4
3. Abast.....	4
4. Marc normatiu.....	4
5. Missió i objectius.....	5
6. Organització de la seguretat.....	5



6.1. Comitè de Gestió i Coordinació de la Seguretat de la Informació.....	6
6.2. Responsable de la Informació.....	7
6.3. Responsable del Servei.....	8
6.4. Responsable de Seguretat de la Informació.....	8
6.5. Responsable dels Sistemes d'informació .....	8
6.6. Delegat de Protecció de Dades .....	9
6.7. Procediments de designació .....	9
7. Dades de caràcter personal.....	10
8. Gestió de riscos.....	10
9. Desenvolupament de la Política de Seguretat.....	10
10. Obligacions del personal.....	10
11. Terceres parts.....	11
12. Entrada en vigor .....	11

## 1. Introducció

El Consell Insular d'Eivissa depèn dels sistemes TIC (Tecnologies de la Informació i la Comunicació) per aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguin afectar a la disponibilitat, integritat o confidencialitat de la informació tractada o dels serveis prestats.

L'Esquema Nacional de Seguretat (ENS) té per objecte l'establiment dels principis i requisits d'una política de seguretat en la utilització dels mitjans electrònics que permeti l'adequada protecció de la informació, alhora que persegueix fonamentar la confiança en que els sistemes prestaran els seus serveis i custodiaran la informació d'acord amb les seues especificacions funcionals, sense interrupcions o modificacions fora de control i sense que la informació pugui arribar al coneixement de persones no autoritzades.

L'adaptació a l'ENS implica que el Consell Insular d'Eivissa i el seu personal han d'aplicar les mesures mínimes de seguretat exigides per aquest, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades i preparar una resposta efectiva als possibles incidents que puguin sorgir per a garantir la continuïtat dels serveis prestats.

Els diferents serveis de gestió del Consell Insular d'Eivissa han d'assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema.

## 2. La seguretat com a procés integral

La seguretat de la informació és el resultat d'un procés que depèn de tots i cadascun dels elements humans, tècnics, materials i organitzatius que intervenen en el tractament. Els qui participin en qualsevol fase del tractament hauran de respondre, en la mesura de les seues responsabilitats, de la seguretat i bon ús de la informació. De manera especial, hauran de col·laborar en la prevenció, detecció i control dels riscos derivats d'actuacions negligents, ignorància de les normes, fallades tècniques, d'organització o de coordinació, o instruccions inadequades.

El Consell Insular d'Eivissa, mitjançant els diversos agents amb responsabilitats específiques en matèria de seguretat de la informació, s'encarregarà de proporcionar els canals de participació adequats que facin efectiva la col·laboració esmentada en el paràgraf anterior. De la mateixa manera, s'encarregarà de mantenir permanentment informats a tots els destinataris d'aquesta política, del propòsit de la mateixa, així com dels documents que la desenvolupen i dels canals de participació habilitats.

El procés de gestió de la seguretat de la informació haurà d'estar sotmès a monitorització, control i millora continus per confirmar la seua eficiència davant la constant evolució dels riscos i dels sistemes de protecció.

### 2.1. Prevenció

El Consell Insular d'Eivissa ha d'evitar o, almenys, prevenir en la mesura que sigui possible que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per a això, s'han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaques i riscos. Aquests controls així com els rols i responsabilitats de seguretat de tot el personal han d'estar clarament definits i documentats. Per garantir el compliment de la política, l'organització ha de:

- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració realitzats de forma rutinària.
- Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

## 2.2. Detecció

Donat que els serveis es poden degradar ràpidament degut a incidents, s'ha de monitoritzar l'operació de manera continuada per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència, segons l'establert a l'article 9 de l'ENS.

La monitorització és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i report que arribin als responsables regularment i quan es produeixi una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

## 2.3. Resposta

El Consell Insular d'Eivissa ha de:

- Establir mecanismes per respondre de manera eficaç als incidents de seguretat.
- Designar punts de contacte per les comunicacions en relació a incidents detectats a àrees de l'entitat o a altres organismes relacionats amb el Consell Insular d'Eivissa.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en els dos sentits, amb els Equips de Resposta a Emergències (CERT) reconeguts a nivell nacional com Iris-CERT, CCN-CERT i altres equivalents.

## 2.4. Recuperació

Per restaurar la disponibilitat dels serveis, s'hauran de desenvolupar plans de contingència dels sistemes TIC que incloguin activitats de recuperació de la informació que contribueixin a la continuïtat del servei.

## 3. Abast

El Consell Insular d'Eivissa aplicarà la present Política de Seguretat sobre aquells sistemes que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu.

## 4. Marc normatiu

El marc normatiu que afecta al desenvolupament de les activitats i competències del Consell

Insular d'Eivissa està constituït per normes jurídiques estatals i autonòmiques, si procedeix, orientades a l'administració electrònica, a la seguretat de la informació i els serveis que la manegen, així com a la protecció de dades de naturalesa personal.

Les normes que constitueixen aquest marc es troben recollides en un registre creat a aquest efecte, el qual es manté actualitzat segons assenyalat el corresponent procediment de gestió de requisits legals.

També podran formar part d'aquest marc, aquelles normes aplicables a l'Administració Electrònica del Consell que s'hagin desenvolupat a partir de les anteriors o estiguin relacionades, podent ser addicionalment publicades a les seues electròniques compreses dins l'àmbit d'aplicació d'aquesta Política.

## 5. Missió i objectius

El Consell Insular d'Eivissa, per a la gestió dels seus interessos i de les funcions i competències que té encomanades, promou activitats i presta serveis públics que contribueixen a satisfer les necessitats i aspiracions de la població.

Per aquest motiu, posa a disposició de la mateixa la realització de tràmits online amb l'objectiu d'impulsar la participació de la ciutadania en els assumptes públics establint, d'aquesta manera, noves vies de participació que garanteixin el desenvolupament de la democràcia participativa i l'eficàcia de l'acció pública. Es pretén potenciar, d'altra banda, l'ús de les noves tecnologies en el Consell i entre la pròpia ciutadania.

Els principals objectius que es persegueixen, entre d'altres, són: fomentar la relació electrònica de la ciutadania amb el Consell i crear la confiança necessària entre ciutadà i Consell.

## 6. Organització de la seguretat

Poden distingir-se tres nivells a l'organigrama del Consell Insular d'Eivissa:



- **Nivell 1 – Òrgans de Govern:** alta direcció que entén la missió de l'organització, determina els objectius que es proposa aconseguir i respon que s'aconsegueixin.  
Aquest nivell correspon a la figura del **Responsable de la Informació ENS**, que assumirà la presidència de la Corporació i que podrà delegar en el conseller executiu responsable de l'àrea TIC, junt amb el **Comitè de Seguretat de la Informació** com a òrgan consultiu, assistits per totes les direccions d'Àrea del Consell.
- **Nivell 2 – Direcció Executiva:** responsables dels serveis que entenen què fa cada unitat de gestió i com les diferents unitats es coordinen entre elles per aconseguir els objectius marcats per la Direcció.  
Aquest nivell correspon a la figura del **Responsable de la Seguretat** i el **Responsable dels Serveis**
- **Nivell 3 – Operacional** que es centra en una activitat concreta i controla com es fan les coses.  
Aquest nivell correspon a la figura del **Responsable dels Sistemes d'Informació**, assistit pels responsables de sistema delegats i pels administradors de la seguretat del sistema que es nomenin.

Seguint el mateix esquema i, d'acord amb l'ENS, s'estructura un organigrama de seguretat en el Consell Insular d'Eivissa en tres nivells:

- **Nivell 1:**
  - -Comitè de Gestió i Coordinació de la Seguretat de la Informació.
  - -Responsable de la Informació ENS.
- **Nivell 2:**
  - -Responsable de la Seguretat de la Informació.
  - -Responsable del Servei.
- **Nivell 3:**
  - -Tècnic de Seguretat dels Sistemes.
  - -Responsables dels Sistemes d'Informació.

L'especificació de requisits de seguretat (Nivell 1) correspon als responsables de la informació i dels serveis. L'operació (nivell 3) correspon als responsables dels sistemes, mentre que la supervisió correspon al responsable de la seguretat (nivell 2) i al tècnic de seguretat (nivell 3).

Per damunt de tots ells existeix el Comitè de Coordinació i Gestió de la Seguretat (nivell 1).

### 6.1. Comitè de Gestió i Coordinació de la Seguretat de la Informació

El Comitè de Gestió i Coordinació de la Seguretat de la Informació, d'ara endavant Comitè de Seguretat, coordina la seguretat de la informació a nivell d'organització.

D'acord amb l'ENS, les funcions indicades que corresponen al Comitè de Seguretat són:

- Elaborar (i revisar periòdicament) la Política de Seguretat de la informació per a que sigui aprovada pel responsable de la informació.
- Aprovar i divulgar els procediments de seguretat del Consell Insular d'Eivissa.
- Promoure la millora contínua de la gestió de la seguretat de la informació del Consell Insular d'Eivissa.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que els esforços siguin consistents, alineats amb l'estratègia decidida en la matèria i evitar duplicitats.
- Avaluar els principals riscos residuals assumits pel Consell Insular d'Eivissa i recomanar possibles actuacions respecte a ells.
- Avaluar el compliment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte a ells. En particular, vetllar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.
- Promoure la realització de les auditories periòdiques i avaluar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Prioritzar les actuacions en matèria de seguretat d'acord amb els recursos disponibles.
- Vetllar perquè la seguretat de la informació es tingui en compte en tots els projectes TIC des de la seua especificació inicial fins a la seua posada en marxa. En particular, s'haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i suportin un funcionament homogeni de tots els sistemes TIC.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents àrees del Consell Insular d'Eivissa, elevant aquells casos en els que no tingui suficient autoritat per decidir.
- Avaluar les necessitats de recursos requerits per al compliment dels plans d'actuació derivats de l'aplicació de la Política de Seguretat.
- Elaborar un informe anual de l'estat de la seguretat dels sistemes d'informació.

El Comitè de Seguretat estarà format per les persones titulars, o aquelles en que deleguin, dels següents càrrecs:

- **President:** El Responsable de la informació.





- Vocals:
  - El Delegat de Protecció de Dades del Consell Insular d'Eivissa.
  - El Responsable dels serveis ENS.
  - El Responsable de Seguretat de la Informació, actuant també com a Secretar del Comitè.
  - El Responsable dels Sistemes d'Informació.

A requeriment del president, podran incorporar-se als treballs i sessions del Comitè altres membres del Consell, inclosos grups de treball especialitzats, ja siguin aquests de caràcter intern, extern o mixt.

El Comitè de Seguretat no és un comitè tècnic, però recaptarà regularment del personal tècnic propi o extern, la informació pertinent per prendre decisions. El Comitè de Seguretat s'assessorarà en els temes sobre els quals hagi de decidir o emetre una opinió.

La Secretaria del Comitè l'assumeix el Responsable de la Seguretat de la Informació, al qual com a tal li correspon:

- Convocar les reunions del Comitè de Seguretat de la Informació.
- Preparar els temes a tractar a les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elaborar l'acta de les reunions.
- És responsable de l'execució directa o delegada de les decisions del Comitè.
- El comitè de seguretat es reunirà amb caràcter ordinari dos vegades a l'any i, amb caràcter extraordinari per acord de la Presidència, a iniciativa pròpia o prèvia sol·licitud motivada d'un dels seus membres.

## 6.2. Responsable de la Informació

El Responsable de la Informació establirà els requisits sobre la informació proporcionada per mitjans electrònics a través dels serveis del Consell Insular d'Eivissa i, per tant, tindrà la darrer paraula a l'hora de decidir el tipus d'informació accessible i l'ús que se li pugui donar, en virtut de la reglamentació vigent i de les bones pràctiques en matèria de Protecció de Dades.

Li corresponen les següents funcions:

- Establiment dels requisits de la informació en matèria de seguretat.
- Treball en col·laboració amb el responsable de seguretat i els responsables dels sistemes en el manteniment dels sistemes catalogats segons l'Annex I de l'Esquema Nacional de Seguretat.

El Responsable de la Informació serà el president del Consell Insular d'Eivissa que podrà delegar en el conseller responsable dels serveis TIC.

## 6.3. Responsable del Servei.

El Responsable del Servei establirà els requisits de seguretat aplicables als serveis proporcionats pel Consell Insular d'Eivissa a través de mitjans electrònics i, en aquest sentit, tindrà com a funcions:

- Establiment dels requisits dels serveis TIC en matèria de seguretat.
- Treball en col·laboració amb el Responsable de Seguretat i els responsables dels sistemes on s'englobi/n el/s servei/s per al manteniment dels sistemes catalogats segons l'Annex I de l'Esquema Nacional de Seguretat.

Serà exercit pel **Secretari** del Consell Insular d'Eivissa, sense perjudici que es designin responsables delegats, els quals podran ser convocats al Comitè de Seguretat de la informació amb veu però sense vot.

## 6.4. Responsable de Seguretat de la Informació

El Responsable de Seguretat de la Informació del Consell Insular d'Eivissa té per funcions les següents:

- Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes TIC.
- Promoure la formació i conscienciació de la seguretat de la informació dintre del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establertes són adequades per a la protecció de la informació manejada i els serveis prestats.
- Aprovar tota la documentació relacionada amb la seguretat dels sistemes.
- Verificar els informes de motorització i auditoria dels estats de seguretat dels sistemes.
- Donar suport i supervisar la investigació dels incidents de seguretat des de la seua notificació fins a la seua resolució.
- Elaborar l'informe periòdic de seguretat per al Comitè de Seguretat incloent els incidents més rellevants del període a informar.
- Aprovació dels procediments de seguretat elaborats pels responsables dels sistemes quan, en virtut del contingut, no requereixi l'aprovació del Comitè de Seguretat.



- Proposar la redacció d'aquella normativa de seguretat del Consell Insular d'Eivissa que consideri necessari formalitzar.
- Determinar la categorització dels sistemes i els requisits de seguretat amb caràcter previ a la posada en marxa d'un nou servei vinculat a l'ENS.
- Serà desenvolupat pel **cap de Secció dels Sistemes d'Informació i Seguretat** del Consell Insular d'Eivissa

### 6.5. Responsable dels Sistemes d'informació

El Responsable dels Sistemes d'Informació té per funcions:

- Vetllar pel correcte funcionament del sistema durant tot el seu cicle de vida, de les seues especificacions i instal·lació, incorporant els requisits de seguretat necessaris per a l'operativa en el sistema.
- Definir la tipologia i política de gestió del sistema establint els criteris d'ús i els serveis disponibles en el mateix.
- Definir la política de connexió o desconnexió d'equips i usuaris nous en el sistema.
- Proposar al Responsable de Seguretat els canvis que afectin a la seguretat del sistema.
- Decidir les mesures de seguretat que aplicaran els subministradors de components del sistema a les etapes de desenvolupament, instal·lació i prova del mateix.
- Implantar i controlar les mesures específiques de seguretat del sistema i assegurar-se que aquestes s'integrin adequadament en el marc general de seguretat.
- Determinar els requisits de la configuració autoritzada del hardware i software a utilitzar en el sistema, en allò que afecti a la seua seguretat.
- Aprovar tota modificació substancial de la configuració de qualsevol element del sistema que afecti a la seguretat i disponibilitat del servei.
- Portar a terme el preceptiu procés de revisió periòdica de l'anàlisi i gestió de riscos en el sistema.
- Elaborar i aprovar la documentació de seguretat del sistema.
- Delimitar les actuacions que afectin a la Política de Seguretat de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del sistema.
- Investigar els incidents de seguretat que afectin al sistema i, en el seu cas, comunicar-ho al Responsable de Seguretat o a qui aquest determini.
- Establir plans de contingència i emergència.
- A més, el responsable del sistema pot acordar la suspensió del maneig d'una informació determinada o la prestació d'un servei determinat si és informat de greus deficiències de seguretat que poguessin afectar a la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els responsables de la informació afectada, del servei afectat i amb el Responsable de Seguretat, abans de ser executada.

### 6.6. Delegat de Protecció de Dades

El Delegat de Protecció de Dades serà únic per a tots els serveis que presta l'entitat.

Aquesta figura ha d'estar registrada a l'Agencia Espanyola de Protecció de Datos.

Les funcions del Delegat de Protecció de Dades seran les indicades a l'esmentat Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, i altres disposicions reguladores de la matèria.

### 6.7. Procediments de designació

El desenvolupament de les responsabilitats definides en aquesta Política de Seguretat vendrà determinada per l'accés als diferents càrrecs que s'han vinculat a elles. En el cas que desaparegués o canviés de denominació d'algun d'aquests càrrecs serà competència del Consell Insular d'Eivissa assignar el nou lloc al que quedarà vinculada la figura.

## 7. Dades de caràcter personal

El Consell Insular d'Eivissa realitza tractaments en els que fa ús de dades de caràcter personal sotmeses al que es disposa en el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en allò que respecta al tractament de dades personals i de conformitat amb la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

Les polítiques de seguretat aplicables als tractaments es regeixen per les mesures de seguretat implantades d'acord amb l'Annex II (Mesures de seguretat) del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat a l'àmbit de l'Administració Electrònica. Al RAT (Registre d'activitats del tractament, del sistema de gestió de la privacitat) s'indexen els diferents tractaments de dades afectades per la normativa.

Tots els sistemes d'informació del Consell Insular d'Eivissa s'ajustaran als nivells de seguretat requerits per la normativa per la naturalesa i finalitat de les dades de caràcter personal.

## 8. Gestió de riscos

Tots els sistemes subjectes a aquesta Política de Seguretat realitzaran una anàlisi de riscos, avaluant les amenaces i els riscos als que estan exposats. Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada a l'any.
- Quan canviï la informació manejada.
- Quan canviïn els serveis prestats.
- Quan tingui lloc un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

Per a l'harmonització de les anàlisi de riscos, el Comitè de Seguretat establirà una valoració de referència per als diferents tipus d'informació gestionats i els diferents serveis prestats.

## 9. Desenvolupament de la Política de Seguretat

Aquesta Política es desenvoluparà per mitjà d'una **Normativa de Seguretat** que afronti aspectes específics. La Normativa de Seguretat estarà a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular, per aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

Altres documents que complementen aquesta Política de Seguretat són:

- La normativa de seguretat, la qual estarà disponible a la intranet del Consell Insular d'Eivissa.

## 10. Obligacions del personal

Tots els membres del Consell Insular d'Eivissa tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat desenvolupada a partir d'ella, sent responsable del Comitè de Seguretat disposar dels mitjans necessaris per a que la informació arribi a les persones afectades, tenint sempre en compte les disponibilitats pressupostàries del Consell Insular d'Eivissa.

Tots els treballadors i treballadores del Consell Insular d'Eivissa, sota l'abast de l'ENS, atendran a una acció de conscienciació en matèria de seguretat TIC, almenys una vegada cada dos anys. S'establirà un programa d'accions en conscienciació contínua per atendre a tots els membres del Consell Insular d'Eivissa relacionats amb serveis d'administració electrònica, en particular als de nova incorporació, tenint en compte sempre les disponibilitats pressupostàries del Consell Insular d'Eivissa. Es realitzarà una acció de conscienciació durant els dos anys següents a l'aprovació d'aquesta Política de Seguretat i, de manera continuada, per al personal de nova incorporació.

En el seu cas, si es requereix formació específica per el maneig segur dels sistemes, les persones amb responsabilitat en l'operació o administració de sistemes TIC la rebran en la mesura en que la necessitin per a realitzar la seua tasca.

## 11. Terceres parts

Quan el Consell Insular d'Eivissa presti serveis a altres organismes o manegi informació d'altres organismes, se'ls farà participat d'aquesta Política de Seguretat de la Informació. Per això, s'establiran canals per informació i coordinació dels respectius Comitès de Seguretat de l'ENS i s'establiran procediments d'actuació davant possibles incidents de seguretat.

Quan el Consell Insular d'Eivissa utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà participat d'aquesta Política de Seguretat i de la Normativa de Seguretat que impliqui als esmentats serveis o informació. Aquesta tercera part quedarà subjecte a les obligacions establertes a l'esmentada normativa, havent-se d'incorporar als plecs i encomanes del Consell Insular d'Eivissa. D'aquesta manera, el proveïdor haurà de garantir que el seu personal està adequadament format en matèria de seguretat d'acord amb els requeriments del Consell Insular d'Eivissa.

## 12. Entrada en vigor

Aquesta Política de Seguretat de la Informació és efectiva des del dia següent al de la seua data d'aprovació i fins que sigui reemplaçada per una nova Política.

El Consell Insular d'Eivissa disposarà dels mitjans per publicar, donar a conèixer i facilitar el compliment d'aquesta política i dels documents que la desenvolupen, així com per verificar la seua aplicació i efectivitat. Així mateix, habilitarà canals de participació que permetin als destinataris d'aquesta política i dels documents complementaris, participar en la seua revisió i millora.



## Annex A. Glossari de termes

- **Anàlisi de riscos:** Utilització sistemàtica de la informació disponible per identificar perills i estimar els riscos.
- **Dades de caràcter personal:** Qualsevol informació que es refereix a persones físiques identificades o identificables.
- **Gestió d'incidents:** Pla d'acció per atendre a les incidències que es donin. A més de resoldre-les ha d'incorporar mesures de desenvolupament que permetin conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en problemes grans. ENS.
- **Gestió de riscos:** Activitats coordinades per dirigir i controlar una organització respecte als riscos. ENS.
- **Incident de seguretat:** Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació. ENS.
- **Informació:** Cas concret d'un cert tipus d'informació.
- **Política de seguretat:** Conjunt de directrius plasmades en un document escrit, que regeixen la forma en que una organització gestiona i protegeix la informació i els serveis que consideren crítics. ENS.
- **Principis bàsics de seguretat:** Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis. ENS.
- **Responsable de la informació:** Persona que té la potestat d'establir els requisits d'una informació en matèria de seguretat.
- **Responsable de la seguretat:** Persona que determinarà les decisions per satisfer els requisits de seguretat de la informació i dels serveis.
- **Responsable del servei:** Persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.
- **Responsable del sistema:** Persona que s'encarrega de l'explotació del sistema d'informació.
- **Servei:** Funció o prestació desenvolupada per alguna entitat oficial destinada a cuidar els interessos o satisfer les necessitats dels ciutadans.
- **Sistema d'informació:** Conjunt organitzat de recursos per a que la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

## Annex B. Abreviatures

- **CCN:** Centre Criptològic Nacional
- **CERT:** Computer Emergency Reaction Team
- **ENS:** Esquema Nacional de Seguretat
- **STIC:** Seguretat Tecnologies de la Informació i les Comunicacions
- **TIC:** Tecnologies de la Informació i les Comunicacions

**Segon.** Publicar aquest acord al butlletí oficial de les Illes Balears.

**Tercer.** Comunicar-ho als diferents responsables."

Eivissa, 4 de maig de 2023

**El cap de servei de Transports**

Antonio Montero Guasch

