POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

INFORMACIÓ DEL DOCUMENT

Títol del document	**PO-01 POLÍTICA DE SEGURETAT DE LA INFORMACIÓ**
Tipus de document	Política de Seguretat
Descripció	La Política de Seguretat de la Informació és un document d'alt nivell que defineix què significa la seguretat de la informació dins d'una organització. El document ha d'estar accessible per a tots els membres de l'organització.
Nivell de seguretat recomanat	Públic
Propietari del documento	Agència Tributària de les Illes Balears (ATIB)

Registre de versions		
Descripció	**Versió**	**Data**
Versió inicial del document	1.0	27/02/2024
Correcció del Marc Legislatiu	1.1	08/05/2024
S'annexa punto 6.5 resolució de conflictes	1.1	08/05/2024
S'annexa l'apartat 10. Gestió documental	1.1	08/05/2024
S'ajusta el apartat 7. Dades de Caràcter Personal	1.1	08/05/2024
S'han adaptat els apartats que no s'ajustaven en la seva totalitat a l'organització i la seva estructura organitzacional	1.2	16/05/2024
S'han corregit errades en les responsabilitats en l'apartat 6	1.2	17/05/2024
Adequació guia CCN_805	2.0	30/12/2025

Taula de contingut

1. APROVACIÓ I ENTRADA EN VIGOR/EFECTIVITAT

Text aprovat el dia **8 de gener de 2026** en sessió del Comitè de Seguretat de la Informació de l'Agència Tributària de les Illes Balears (ATIB).

Aquesta Política de Seguretat de la Informació, d'ara endavant la Política, serà efectiva des d'aquesta data i romandrà vigent fins que sigui substituïda per una nova.

Les modificacions que suposen millores o adaptacions seran realitzades pel Comitè de Seguretat de la Informació, que haurà de revisar-la com a mínim anualment.

En cas que els canvis impliquen modificacions substancials en principis o responsabilitats, aquests hauran de ser aprovats per l'òrgan competent.

La substitució de la Política serà impulsada pel Comitè de Seguretat i ratificada per l'òrgan competent, informant-se adequadament pels canals habituals.

2. INTRODUCCIÓ

L'Agència Tributària de les Illes Balears (ATIB) depèn en gran mesura dels sistemes de Tecnologies d'Informació i Comunicacions (TIC) per a aconseguir els seus objectius operatius.

Donada aquesta dependència crítica, és imperatiu administrar aquests sistemes amb la màxima diligència, implementant mesures efectives per a salvaguardar-los contra possibles danys, tant accidentals com intencionats, que pogueren comprometre la disponibilitat, integritat, autenticitat, traçabilitat i confidencialitat de la informació manejada i els serveis proporcionats.

El propòsit fonamental de la política de seguretat de la informació és assegurar la qualitat de la informació i la continuïtat sense interrupcions en la prestació de serveis.

Això s'aconsegueix a través d'una combinació d'enfocaments preventius, supervisió constant de les activitats diàries i una resposta àgil davant qualsevol incident que pugi sorgir.

Donada la naturalesa dinàmica i en constant evolució de les amenaces als sistemes TIC, és essencial adoptar una estratègia proactiva que s'adapti als canvis en l'entorn de seguretat.

Això implica la implementació de mesures mínimes de seguretat establides per l'Esquema Nacional de Seguretat, així com la vigilància contínua dels nivells de servei, l'anàlisi de vulnerabilitats reportades i la preparació de plans de resposta a incidents eficaços per a garantir la continuïtat dels serveis.

Cada departament dins de l'organització ha d'assegurar-se que la seguretat de les TIC sigui una consideració integral en totes les etapes del cicle de vida dels sistemes, des de la seua concepció i desenvolupament fins a la seua retirada.

Els requisits de seguretat i les necessitats financeres han de ser identificats i abordats en totes les fases de planificació, adquisició i operació de projectes relacionats amb les TIC.

És fonamental que els departaments estiguin preparats per a prevenir, detectar, respondre i recuperar-se d'incidents de seguretat, conforme al que s'estableix en l'Article 7 de l'Esquema Nacional de Seguretat.

Això garantirà la capacitat de l'ATIB per a mantenir la integritat i la continuïtat de les seues operacions en un entorn cada vegada més desafiador en termes de seguretat de la informació.

2.1. Prevenció

Els departaments han d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per a garantir el compliment de la política, els departaments han de:

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

2.2. Detecció

Donat que els serveis es poden degradar ràpidament degut a incidents, que van des d'una simple desacceleració fins a la seua detenció, els serveis han de monitoritzar l'operació de manera contínua per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que s'estableix en l'Article 8 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 arriben als responsables regularment i quan es produeixi una desviació significativa dels paràmetres que s'hagen preestablert com a normals.

2.3. Resposta

Per a garantir la disponibilitat dels serveis crítics, els departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

3. PRINCIPIS RECTORS DE LA POLÍTICA

- Abast estratègic: la seguretat de la informació ha de comptar amb el compromís i suport de tots els nivells de l'entitat i haurà de coordinar-se i integrar-se amb la resta de les iniciatives estratègiques de manera coherent
- Seguretat integral: la seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes de la informació, procurant evitar qualsevol actuació puntual o

tractament conjuntural. La seguretat de la informació ha de considerar-se com a part de l'operativa habitual, estant present i aplicant-se des del disseny inicial dels sistemes TIC

- Gestió de la seguretat basada en el risc: la gestió de la seguretat basada en els riscos identificats permetrà el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. Les mesures de seguretat s'establiran en funció dels riscos als quals estigui subjecta la informació i els seus sistemes, i seran proporcionals al risc que tracten, havent d'estar justificades. També es tindran en compte els riscos identificats en el tractament de dades personals
- Prevenció, detecció, resposta i conservació amb la implementació d'accions preventives d'incidents, minimitzant les vulnerabilitats detectades, evitant la materialització de les amenaces i, quan aquestes es produeixin, donant una resposta àgil per a restaurar la informació o serveis prestats, garantint una conservació segura de la informació
- Existència de línies de defensa, l'estratègia de seguretat de l'entitat es dissenya i implementa en capes de seguretat
- Vigilància contínua i reavaluació periòdica: l'entitat implementa mitjans la detecció i resposta a activitats o comportaments anòmals. A més, d'altres que permeten una avaluació continuada de l'estat de seguretat dels actius. Existirà, també, un procés de millora contínua per a la revisió i actualització de les mesures de seguretat, de manera periòdica, conforme a la seua eficàcia i l'evolució dels riscos i sistemes de protecció
- Seguretat per defecte i des del disseny: els sistemes han d'estar dissenyats i configurats per a garantir la seguretat per defecte. Els sistemes proporcionaran la funcionalitat mínima necessària per a prestar el servei per al qual van ser dissenyats
- Diferenciació de responsabilitats, en aplicació d'aquest principi les funcions del Responsable de la Seguretat i del Responsable del Sistema estaran diferenciades

4. ABAST

Aquesta Política s'aplicarà als sistemes d'informació de l'Agència Tributària de les Illes Balears, que estan relacionats amb l'exercici de drets i el compliment de deures per mitjans electrònics, o amb l'accés a la informació o al procediment administratiu i que es troben dins de l'abast de l'Esquema Nacional de Seguretat (ENS).

Tots els empleats públics i càrrecs de l'Agència Tributària de les Illes Balears, així com el personal de tercers relacionats amb aquesta, que es troben afectats per l'abast de l'ENS, tenen l'obligació de conèixer i complir aquesta "Política de Seguretat de la Informació" i la normativa de seguretat, sent responsabilitat del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi al personal afectat.

5. MISSIÓ

L'Agència Tributària de les Illes Balears (ATIB), 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 expectatives de la població i de tots els grups d'interès.

L'Agència Tributària de les Illes Balears (ATIB) desitja potenciar l'ús de les noves tecnologies tant internament com en les seues relacions amb la ciutadania.

Els principals objectius que es persegueixen són, entre altres, els següents:

- Millorar la qualitat dels serveis públics
- Fomentar la relació electrònica de la ciutadania amb l'entitat, creant la confiança necessària entre el ciutadà i l'agència en aquesta relació
- Reduir els temps de tramitació
- Reduir les càrregues administratives
- Fer transparent l'activitat de l'Agència Tributària
- Fomentar la participació y col·laboració.

6. MARC NORMATIU

L'Agència Tributària de les Illes Balears (ATIB) desenvolupa les seues activitats en l'àmbit de l'administració electrònica i de la seguretat de la informació de conformitat amb el marc normatiu vigent que resulte d'aplicació en cada moment, incloent, entre altres, la normativa en matèria de procediment administratiu, règim jurídic del sector públic, protecció de dades personals, seguretat nacional, serveis electrònics de confiança i, de manera específica, l'Esquema Nacional de Seguretat (ENS).

Amb la finalitat de garantir la vigència, actualització i control del compliment normatiu, el detall del marc legislatiu i reglamentari aplicable no es recull de manera exhaustiva en la present Política, sinó que es manté actualitzat en el Procediment i Registre de Legislació Aplicable, on s'identifiquen:

- Les normes legals y reglamentàries d'aplicació.
- Les Instruccions Tècniques de Seguretat (ITS) de compliment obligatori.
- El perfil de compliment específic establert conforme a l'article 30 del Reial decret 311/2022.
- Les guies i recomanacions del Centre Criptològic Nacional (CCN) que resulten aplicables per a reforçar el compliment de l'ENS.

Aquest procediment i registre constitueixen el repositori oficial de referència normativa, sent objecte de revisió periòdica per a incorporar modificacions legislatives, noves disposicions o actualitzacions rellevants, sense que això impliqui la necessitat de modificar ni tornar a aprovar la present Política de Seguretat de la Informació.

La responsabilitat del manteniment, revisió i actualització del marc normatiu aplicable correspon a l'Agència Tributària de les Illes Balears (ATIB), d'acord amb els rols i responsabilitats definits en el Sistema de Gestió de la Seguretat de la Informació i en compliment dels principis establis per l'Esquema Nacional de Seguretat.

7. ORGANITZACIÓ DE LA SEGURETAT

7.1. Comitès: Funcions y Responsabilitats.

El Comitè de Seguretat de la Informació coordina la seguretat de la informació. Procurarà estar format per representants de les àrees afectades per l'ENS (es detalla en el Document PR-01 Organització de la seguretat).

La Comissió de Seguretat TIC reportarà a la Direcció de ATIB y tindrà las següents funcions:

- Establir els mecanismes de cooperació i coordinació amb les diverses àrees de l'Agència Tributària de les Illes Balears en matèria de seguretat de la informació.
- Establir els mecanismes de cooperació i coordinació amb les diverses àrees de l'Agència Tributària de les Illes Balears en matèria de seguretat de la informació.
- Informar regularment de l'estat de la seguretat de la informació a la Direcció.
- Promoure la millora contínua de la gestió de la seguretat de la informació.
- Elaborar l'estratègia d'evolució de la Direcció pel que fa a seguretat de la informació.
- 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.
- Elaborar (i revisar regularment) la Política de Seguretat de la Informació perquè siga aprovada per l'òrgan municipal competent.
- Aprovar la normativa de seguretat de la informació.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
- Monitoritzar els principals riscos residuals assumits i recomanar possibles actuacions respecte d'ells.
- Monitoritzar el rendiment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'ells. En particular, vetlar 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 que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Aprovar plans de millora de la seguretat de la informació. En particular vetlarà per la coordinació de diferents plans que puguin realitzar-se en diferents àrees.
- Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.
- Vetlar 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 operació. En particular haurà de vetlar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donen suport a un funcionament homogeni de tots els sistemes TIC..

- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables, elevant aquells casos en els quals no tingui suficient autoritat per decidir.

El Comitè de Seguretat TIC estarà format per:

- **Responsable de Seguretat** Externalitzat segons licitació
- **Responsable de Sistemes**: Responsable del Departament d'Informàtica
- **Responsable d'Informació:** Director ATIB.
- **Responsable de Serveis:** Responsable Àrea d'Auditoria
- **DPD:** Externalitzat segons licitació

7.2. Rols: Funcions i Responsabilitats.

L'ENS es regeix pel Reial decret 311/2022 i estableix 4 rols en 2 nivells segons el seu article 11. Els quals també estan detallats en la Guia 801 del Centre Criptològic Nacional.

	ROLS	
NIVELL DE GOVERN	RESPONSABLE DE LA INFORMACIÓ Determinar els nivells de seguretat de la informació	RESPONSABLE DEL SERVEI Determinar els nivells de seguretat dels serveis
NIVELL OPERATIU	RESPONSABLE DE LA SEGURETAT Atén la seguretat de la informació	RESPONSABLE DEL SISTEMA Explotació de la Tecnologia

A nivell de Govern podem trobar:

El responsable de la informació: Determina els requisits de seguretat de la informació tractada segons els paràmetres de l'annex I de l'ENS. Pot tractar-se d'una persona o d'un òrgan col·legiat.

El responsable del servei: Determina els requisits de seguretat dels serveis prestats segons els paràmetres de l'annex I de l'ENS. Pot tractar-se d'una persona física singular o d'un òrgan col·legiat, formant part del que es denomina Comitè de Seguretat de la Informació.

Ha d'incloure les especificacions de seguretat en el cicle de vida dels serveis i sistemes, acompanyades dels corresponents procediments de control.

A nivell Operatiu podem trobar:

El responsable de Seguretat (o CISO): Determina les decisions de seguretat pertinents per a satisfer els requisits establerts pel responsable de la informació i dels serveis. Haurà de ser una persona física jeràrquicament independent del responsable del sistema. En cas de serveis externalitzats, la responsabilitat última la té sempre l'entitat.

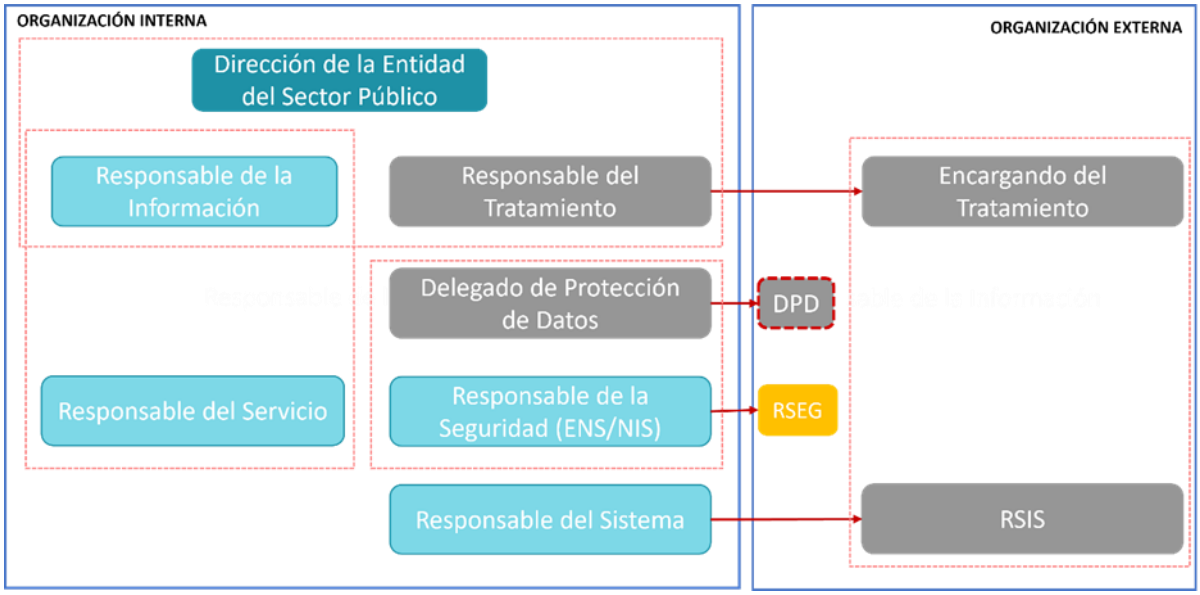
Funcions:

- Elaborar Plans amb Mesures per a gestionar els riscos detectats.
- Supervisar i desenvolupar les polítiques de seguretat, normatives i procediments, la seua efectivitat fent controls periòdics.
- Elaborar el document de Declaració d'Aplicabilitat de mesures de seguretat.
- Promoure i formar sobre "bones pràctiques" de l'organització en matèria de ciberseguretat
- Remetre a l'autoritat competent les notificacions d'incidències amb efectes adversos.
- Rebre, interpretar i supervisar l'aplicació d'instruccions i guies de l'autoritat competent
- Recopilar i subministrar informació o documentació a l'autoritat competent.

El responsable del sistema: S'encarrega de l'operació del Sistema d'informació atenent a les mesures de seguretat determinades pel responsable de la seguretat. La seua responsabilitat pot estar situada dins de l'organització o estar compartimentada. Els informes d'autoavaluació i els informes d'auditoria seran analitzats pel responsable de la seguretat competent, que avaluarà les conclusions del responsable del Sistema perquè adopti les mesures correctives adequades.

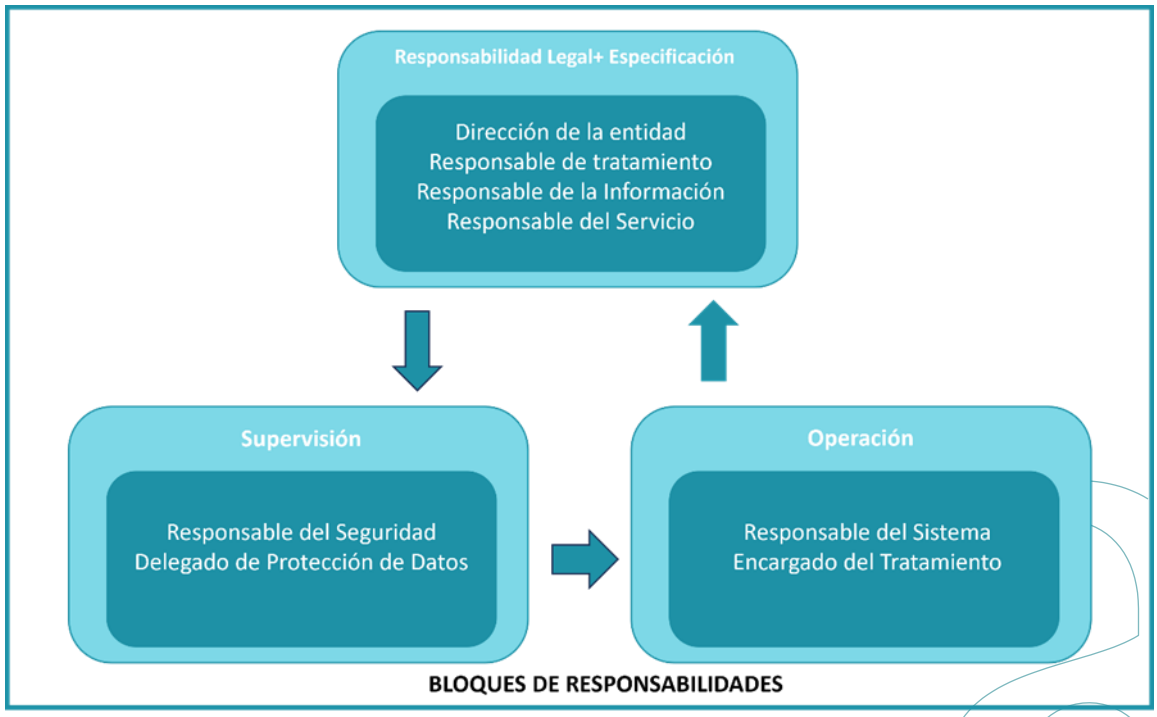
Funcions:

- Desenvolupar, operar i mantenir el sistema.
- Definir la tipologia i política de gestió del sistema
- La connexió/desconnexió d'equips/usuari
- Aprovar els canvis operatius que afecten el sistema
- Decidir les mesures de seguretat que aplicaran els proveïdors de components.
- Implantar, controlar i integrar mesures específiques de seguretat
- La configuració autoritzada i aprovació de modificacions substancials del maquinari i programari.
- Mantenir actualitzat l'Anàlisi de Riscos en el sistema
- Determinar la Categoria del Sistema (procés en Annex I ENS) i les mesures de seguretat que han d'aplicar-se (Annex II ENS)
- Elaborar i aprovar la documentació del sistema i determinar les responsabilitats dels involucrats en el manteniment, explotació, implantació i supervisió del sistema.
- Ha d'investigar Incidents de Seguretat i comunicar-ho a qui correspongui si escau
- Establir Plans de Contingència o Emergència i dur a terme exercicis calendaritzats
- Acordar l'ús de determinada informació o prestació de servei si hi ha vulnerabilitats greus en el sistema, decisió acordada amb el responsable de Seguretat prèviament.



En **l'Article 11 del Reial Decret 311/2022**, pel qual es regula l'Esquema Nacional de Seguretat, també estableix que:

- "En els sistemes d'informació es **diferenciarà el responsable de la informació, el responsable del servei, el responsable de la seguretat i el responsable del sistema"**
- **"La responsabilitat de la seguretat** dels sistemes d'informació estarà diferenciada de **la responsabilitat sobre l'explotació dels sistemes d'informació."**
- "La política de seguretat de la informació detalla les **atribucions de cada responsable i els mecanismes de coordinació i resolució de conflictes".**



El Marc Operacional del Reial Decret 311/2022 comenta la importància de la "Segregació de Funcions y tasques" on trobem **els requisits que han de complir-se**.

En concret, descriu "El sistema de control d'accessos s'organitza de manera que se s'exigissin la concurrència de 2 o més persones per a realitzar tasques crítiques…". El que implica que:

- Les capacitats **de desenvolupament i operació no recauran en la mateixa persona**.
- Les **persones que autoritzen y controlen l'ús de la informació** seran distintes.
- La mateixa persona **no conjuminarà funcions de configuració i manteniment** del sistema.
- La mateixa **persona no pot conjuminar funciones d'auditoria o supervisió amb qualsevol altra funció**.

Una vegada establerts els rols a diferents persones de l'organisme, i després de diferenciar bé les funcions i responsabilitats de cadascuna d'elles, es disposarà del Comitè de Seguretat de la Informació.

7.3. Procediment de Designació

Els membres del Comitè de Seguretat de la Informació seran designats per Direcció d'ATIB.

El responsable de Seguretat de la Informació serà nomenat i proposat pel Comitè de Seguretat TIC. El nomenament es revisarà cada 2 anys o quan el lloc quedi vacant.

El responsable de la Informació serà designat a proposta del Comitè de Seguretat.

El Departament responsable d'un servei que es preste electrònicament d'acord amb la Llei 11/2007 designarà al responsable del Sistema, precisant les seues funcions i responsabilitats dins del marc establert per aquesta Política.

7.4. Política de Seguretat de la Informació.

Serà missió del Comitè de Seguretat TIC **la revisió anual** d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment d'aquesta. La Política serà aprovada per l'Agència Tributària de les Illes Balears i difosa perquè la coneguin totes les parts afectades.

7.5. Resolució de Conflictes

El Comitè de Seguretat de la Informació s'encarregarà de la resolució dels conflictes i/o diferències d'opinions que puguin sorgir entre els rols de seguretat.

8. DADES DE CARÀCTER PERSONAL

L'Agència Tributària de les Illes Balears (ATIB) només recollirà dades de caràcter personal quan siguin adequades, pertinents i no excessives i aquestes es troben en relació amb l'àmbit i les finalitats per als quals s'hagen obtingut.

L'Agència Tributària de les Illes Balears (ATIB) realitza tractaments en els quals fa ús de dades de caràcter personal sotmesos al que es disposa pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Política de Protecció de Dades:

L'Agència Tributària de les Illes Balears (ATIB) es compromet a garantir la protecció de les dades personals conforme al que s'estableix pel Reglament General de Protecció de Dades (RGPD) i la Llei Orgànica de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD). Tots els tractaments de dades realitzats per ATIB compliran amb els principis de licitud, lleialtat i transparència en el tractament de dades personals, així com amb el principi de minimització de dades, assegurant que únicament es recullen les dades estrictament necessàries per a la finalitat del tractament. Així mateix, s'adoptaran les mesures tècniques i organitzatives necessàries per a garantir la seguretat i confidencialitat de les dades personals, evitant la seua alteració, pèrdua, tractament o accés no autoritzat. El Delegat de Protecció de Dades de l'Agència Tributària de les Illes Balears (ATIB) supervisarà el compliment d'aquestes polítiques i normatives en matèria de protecció de dades. Véase el document **(SGPD_02 - POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES)**

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 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

A més, es disposa d'un RAT (Registre d'Activitats del Tractament) on s'indexen els distints tractaments de dades afectats per la normativa.

Tots els sistemes d'informació de l'Agència Tributària de les Illes Balears (ATIB) s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal. El Delegat de Protecció de Dades de l'Agència Tributària de les Illes Balears (ATIB) vetlarà pel compliment del RGPD i de la LOPDGDD.

Es pot consultar el Registre d'Activitats de Tractament en els següents enllaços:

Agència Tributària de les Illes Balears - A.T.I.B. 759 (atib.es)

9. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Aquest anàlisi es repetirà:

- regularment, almenys una vegada a l'any
- quan canviï la informació manejada
- quan canvien els serveis prestats
- quan ocorri un incident greu de seguretat
- quan es reporten vulnerabilitats greus
- quan es produeixin modificacions en l'anàlisi de riscos de protecció de dades o en les avaluacions d'impacte

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat TIC establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats. El Comitè de Seguretat TIC dinamitzarà la disponibilitat de recursos per a atendre a les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

Es tindran en compte els riscos en protecció de dades, comptant amb l'opinió del Delegat de Protecció de Dades, a més es coordinaran els plans del tractament del risc.

10. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El Comitè de Seguretat de la Informació ha aprovat el desenvolupament d'un sistema de gestió, que serà establert, implementat, mantingut i millorat, conforme als estàndards de seguretat. Aquest sistema s'adequarà i servirà de gestió dels controls de l'Esquema Nacional de Seguretat. El sistema serà documentat i permetrà generar evidències dels controls i del compliment dels objectius marcats pel Comitè. Existirà un procediment de gestió documental que establirà les directrius per a l'estructuració de la documentació de seguretat del sistema, la seua gestió i accés.

Correspon al Comitè de Seguretat de la Informació la revisió anual de la present Política proposant, en cas que sigui necessari millores d'aquesta, per a la seua aprovació per part de la Direcció de l'Agència Tributària de les Illes Balears (ATIB).

Aquesta Política es desenvoluparà per mitjà de normativa de seguretat que abordi aspectes específics. La normativa de seguretat estarà a disposició de tots els membres d'ATIB que necessiten conèixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible per diversos mitjans a disposició dels usuaris en els repositoris interns de l'agència.

11. DIRECTRIUS PER A L'ESTRUCTURACIÓ DE LA DOCUMENTACIÓ DE SEGURETAT DEL SISTEMA, GESTIÓ I ACCÉS.

Tots els documents que formen part del sistema de gestió inclouran una ressenya indicant qui els ha revisat i qui els ha aprovat. Preferiblement, els documents hauran de ser revisats pel Responsable de Seguretat i aprovats pel Comitè de Seguretat.

El sistema col·laboratiu que allotgi tota la documentació de seguretat haurà de permetre la gestió de versions dels documents, així com el seguiment de les activitats realitzades en aquesta documentació.

12. OBLIGACIONS DEL PERSONAL

Tots els membres de l'Agència Tributària de les Illes Balears, tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribi als afectats.

Tots els membres de l'Agència Tributària de les Illes Balears assistiran a una sessió de conscienciació en matèria de seguretat TIC almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per a atendre a tots els membres de l'agència, en particular als de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessiten per a realitzar el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seua primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

13. TERCERES PARTS / PRESTADORS DE SERVEIS / PROVEÏDORS DE SOLUCIONS

Quan l'ATIB preste serveis a altres entitats o manegi informació d'altres, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, sense perjudici de respectar les obligacions de la normativa de protecció de dades si actua com a encarregat del tractament en la prestació dels citats serveis, i s'establiran canals per al report i coordinació dels respectius Comitès de Seguretat i procediments d'actuació per a la reacció davant incidents de seguretat. A més, el Responsable de Seguretat (o persona en qui delegui) serà el Punt de Contacte (POC).

Quan ATIB utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que afecte aquests serveis o informació, sense perjudici del compliment d'altres obligacions en matèria de protecció de dades. En la contractació de prestadors de serveis o adquisició de productes es tindrà en compte l'obligació de l'adjudicatari de complir amb l'ENS.

En l'adquisició de drets d'ús d'actius en el núvol es tindrà en compte els requisits establerts en les mesures de seguretat de l'Annex II i les Guies de desenvolupament.

Aquesta tercera part quedarà subjecta a les obligacions establides en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la, de manera que l'entitat pugui supervisar-los o sol·licitar evidències del compliment d'aquests, inclús auditories de segona o tercera part. Es establiran procediments específics de report i resolució d'incidències que hauran de ser canalitzades pel POC dels tercers implicats i, a més, quan s'afecti a dades personals pel Delegat de Protecció de Dades. Els tercers garantiran que el seu personal està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política o el que específicament es pugui exigir en el contracte.

Quan algun aspecte de la Política no pugui ser satisfet per un tercer segons es requereix en els paràgrafs anteriors, el Responsable de la Seguretat emetrà un informe que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de l'inici de la contractació o, si escau, de l'adjudicació. L'informe es traslladarà al representant de l'entitat que haurà d'autoritzar la continuació amb la tramitació de contractació del tercer, assumint els riscos detectats.

Quan l'entitat adquireixi, desenvolupi o implanti un sistema d'Intel·ligència Artificial, a més de complir amb el que s'estableix en la normativa vigent en la matèria, haurà de comptar amb l'informe del Responsable de la Seguretat, que consultarà al Responsable de la Informació i del Servei i, quan sigui necessari, al del Sistema, havent també el Delegat de Protecció de Dades d'emetre el seu parer.

14. GESTIÓ D'INCIDENTS DE SEGURETAT

ATIB disposa d'un procediment per a la gestió àgil dels esdeveniments i incidents de seguretat que suposen una amenaça per a la informació i els serveis.

Aquest procediment s'integrarà amb altres relacionats amb els incidents de seguretat d'altres normes sectorials com la de protecció de dades personals o una altra que afecte l'organisme per a coordinar la resposta des dels diferents enfocaments i comunicar als diferents organismes de control sense dilacions indegudes i, quan sigui necessari, a les Forces i Cossos de Seguretat de l'Estat o als jutjats.