



Agència Tributària  
Valenciana

# Política de Seguretat de la Informació

Agència Tributària Valenciana

## Índex

<b>1.</b>	<b>Introducció</b> .....	<b>3</b>
<b>2.</b>	<b>Missió i serveis prestats</b> .....	<b>4</b>
<b>3.</b>	<b>Principis bàsics</b> .....	<b>5</b>
<b>4.</b>	<b>Objectius de la Seguretat de la informació</b> .....	<b>6</b>
<b>5.</b>	<b>Abast</b> .....	<b>7</b>
<b>6.</b>	<b>Marc normatiu</b> .....	<b>7</b>
<b>7.</b>	<b>Organització de la Seguretat de la Informació</b> .....	<b>7</b>
7.1.	Criteris de la Seguretat de la Informació.....	7
7.2.	Definició de Rols i Responsabilitats associats a l'Esquema nacional de Seguretat.....	8
7.2.1.	Responsable de la Informació i dels Serveis.....	8
7.2.2.	Responsable de la Seguretat de la Informació .....	8
7.2.3.	Responsable del Sistema.....	9
7.3.	D'Assignació de Rols i Responsabilitats associats a l'Esquema nacional de Seguretat .....	10
7.4.	Comité de Seguretat de la Informació .....	10
7.4.1.	Atribucions del Comité de Seguretat de la Informació .....	11
7.4.2.	Periodicitat de les reunions i adopció d'acords .....	12
7.5.	Grup de Treball TIC.....	12
7.5.1.	Atribucions del Grup de Treball TIC.....	12
7.5.2.	Periodicitat de les reunions i adopció d'acords .....	13
7.6.	Procediment de designació.....	13
7.6.1.	Procediment de designació Comité de Seguretat de la Informació .	13
7.6.2.	Procediment de designació Grup de Treball TIC.....	13
<b>8.</b>	<b>Dades personals</b> .....	<b>14</b>
<b>9.</b>	<b>Obligacions del personal</b> .....	<b>14</b>
<b>10.</b>	<b>Gestió de riscos</b> .....	<b>14</b>
7.1.	Riscos que es deriven del tractament de dades personals .....	15
<b>11.</b>	<b>Documentació Complementària</b> .....	<b>15</b>
<b>12.</b>	<b>Terceres parts</b> .....	<b>15</b>
<b>13.</b>	<b>Millora contínua</b> .....	<b>16</b>
<b>14.</b>	<b>Aprovació i entrada en vigor</b> .....	<b>16</b>

# 1. Introducció

L'Agència Tributària Valenciana (d'ara en avant, l'Agència o "ATV"), depén dels sistemes TIC (Tecnologies de la Informació i les Telecomunicacions) per a 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 la seguretat de la informació tractada o els serveis prestats i estant sempre protegits contra les amenaces o els incidents amb potencial per a incidir en la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació tractada i els serveis prestats.

Per a fer front a aquestes amenaces, es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn per a garantir la prestació contínua dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), així com realitzar un seguiment continu dels nivells de prestació dels serveis, monitorar i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als ciberincidentes per a garantir la continuïtat dels serveis prestats.

D'aquesta manera, totes les unitats administratives de l'ATV tenen present que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seua concepció fins a la seua retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

Per tant, per a l'Agència Tributària Valenciana, l'objectiu de la Seguretat de la Informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària per a detectar qualsevol incident i reaccionant amb prestesa als incidents per a recuperar els serveis al més prompte possible, amb l'aplicació de les mesures.

## 2. Missió i serveis prestats

La missió de l'Agència Tributària Valenciana consisteix a coadjuvar a l'assoliment d'un grau satisfactori de suficiència financera, en aplicació del que es disposa en l'article 67 de l'Estatut d'Autonomia de la Comunitat Valenciana i en els articles 1 i 2 de la Llei orgànica 8/1980, de 22 de setembre, de Finançament de les Comunitats Autònomes, incrementar l'eficàcia per a reunir els recursos necessaris per al sosteniment de les despeses públiques, millorar la prestació del servei i la qualitat en l'atenció i assistència al contribuent, potenciar la col·laboració i cooperació interadministratives i afrontar adequadament la labor de control i lluita contra la defraudació fiscal en l'àmbit dels tributs gestionats per la Generalitat.

Des de la seua creació, l'ATV queda configurada com un organisme autònom adscrit a la Conselleria competent en matèria d'hisenda, amb personalitat jurídica pròpia, autonomia funcional i de gestió, i plena capacitat d'actuació en el desenvolupament de les funcions assumides. Li correspon l'aplicació dels tributs i l'exercici de la potestat sancionadora tant sobre els tributs propis de la Generalitat com sobre els tributs cedits per l'Estat, en el marc de la vigent Llei orgànica de finançament autonòmic.

L'ATV presta els següents serveis:

- Facilita informació, assistència i orientació general, sobre els seus serveis, oficines, i organització, en tots els seus centres gestors, en horari d'atenció al públic, en el servei telefònic d'informació tributària i en Internet.
- Facilita informació tributària, com puga ser:
  - a) Informació i assistència sobre el compliment de les obligacions tributàries derivades dels tributs la gestió dels quals se li encomana, prèvia cita, obtinguda per Internet
  - b) Informació genèrica sobre els tributs que gestiona la \*ATV, i sobre les taxes i altres ingressos de dret públic.
  - c) Informació sobre l'estat de tramitació dels expedients, prèvia cita, obtinguda per Internet.
  - d) Informació sobre normativa i doctrina tributària, novetats fiscals, convenis en vigor, estadístiques tributàries, informes del Ministeri, i beneficis fiscals aplicables.
- Posa a la disposició dels ciutadans diferents programes informàtics d'ajuda per a la confecció i presentació telemàtica de declaracions tributàries, així com ajuda en internet per al càlcul del valor real de béns immobles urbans i rústics, i del

valor fiscal de vehicles.

- Assisteix i informa en la Campanya de l'IRPF.
- Facilita als ciutadans el pagament de deutes mitjançant i) l'habilitació de diferents mitjans de pagament, ii) la concessió d'ajornaments i fraccionaments, i, iii) l'acord de compensacions de deutes i pagament en espècie
- Emet a petició dels interessats diferents documents, entre altres:
  - a) Certificat d'estar al corrent dels deutes tributaris amb la Generalitat.
  - b) Informe, quan les lleis o els reglaments propis de cada tribut així ho prevegen, sobre la valoració a efectes fiscals de rendes, productes, béns, despeses i altres elements determinants del deute tributari.
  - c) Certificats dels pagaments realitzats.
- Presta el servei de registre general.

### 3. Principis bàsics

Els principis bàsics són directrius fonamentals de seguretat que han de tindre sempre presents en qualsevol activitat relacionada amb l'ús dels actius d'informació. S'estableixen els següents:

- Seguretat com a procés integral.
- Gestió de la seguretat basada en els riscos.
- Prevenció, detecció, resposta i conservació.
- Existència de línies de defensa.
- Vigilància contínua.
- Revaluació periòdica.
- Diferenciació de responsabilitats.

I per això, i es desenvoluparà aplicant els següents requisits mínims:

- Organització i implantació del procés de seguretat
- Anàlisi i gestió dels riscos
- Gestió de personal
- Professionalitat

- Autorització i control dels accessos
- Protecció de les instal·lacions
- Adquisició de productes de seguretat i contractació de serveis seguretat
- Mínim privilegi
- Integritat i actualització del sistema
- de la informació emmagatzemada i en trànsit
- Prevenció davant altres sistemes d'informació interconnectats
- Registres de l'activitat i detecció de codi nociu
- Incidents de seguretat
- Continuitat de l'activitat
- Millora contínua del procés de seguretat

## 4. Objectius de la Seguretat de la informació

L'ATV, estableix com a objectius de la seguretat de la informació els següents:

- Garantir la qualitat i protecció de la informació.
- Aconseguir la plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Gestió d'actius d'informació: Els actius d'informació de la \*ATV es trobaran inventariats i categoritzats i estaran associats a un responsable.
- Seguretat lligada a les persones: S'implantaran els mecanismes necessaris perquè qualsevol persona que accedisca, o pugui accedir als actius d'informació, conega les seues responsabilitats i d'aquesta manera es reduïska el risc derivat d'un el seu ús indegut, aconseguint la plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Seguretat física: Els actius d'informació seran emplaçats en àrees segures, protegides per controls d'accés físics adequats al seu nivell de criticitat. Els sistemes i els actius d'informació que contenen aquestes àrees estaran prou protegits enfront d'amenaques físiques o ambientals.
- Seguretat en la gestió de comunicacions i operacions: S'establiran els procediments necessaris per a aconseguir una adequada gestió de la seguretat, operació i actualització de les TIC. La informació que es transmeta a través de xarxes de comunicacions haurà de ser adequadament protegida, tenint en compte el seu nivell de sensibilitat i de criticitat, mitjançant mecanismes que garantisquen la seua seguretat.
- Control d'accés: Es limitarà l'accés als actius d'informació per part d'usuaris, processos i altres sistemes d'informació mitjançant la implantació dels mecanismes d'identificació, autenticació i autorització concordes a la criticitat de

cada actiu. A més, quedarà registrada la utilització del sistema a fi d'assegurar la traçabilitat de l'accés i auditar el seu ús adequat, conforme a l'activitat de l'organització.

- Adquisició, desenvolupament i manteniment dels sistemes d'informació: Es contemplaran els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, garantint la seua seguretat per defecte.
- Gestió dels incidents de seguretat: S'implantarán els mecanismes apropiats per a la correcta identificació, registre i resolució dels incidents de seguretat.
- Garantir la prestació continuada dels serveis: S'implantarán els mecanismes apropiats per a assegurar la disponibilitat dels sistemes d'informació i mantindre la continuïtat dels seus processos de negoci, d'acord amb les necessitats de nivell de servei dels seus usuaris.
- Protecció de dades: S'adoptaran les mesures tècniques i organitzatives que corresponga implantar per a atendre els riscos generats pel tractament per a complir la legislació de seguretat i privacitat.
- Compliment: S'adoptaran les mesures tècniques, organitzatives i procedimentals necessàries per al compliment de la normativa legal vigent en matèria de seguretat de la informació.

## 5. Abast

Aquesta Política s'aplicarà als sistemes d'informació de l'ATV, relacionats amb l'exercici de les seues competències i a tots els usuaris amb accés autoritzat a aquests, siguen o no empleats públics i amb independència de la naturalesa de la seua relació jurídica amb l'ATV. Tots ells tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la seua Normativa de Seguretat derivada, sent responsabilitat del Comité de Seguretat TIC disposar els mitjans necessaris perquè la informació arribe al personal afectat.

## 6. Marc normatiu

El marc normatiu que aplica a l'ATV és aquell que està regit a través de totes aquelles normes que integren la seguretat de la informació en l'àmbit del servei que presta l'organització, especialment l'Esquema Nacional de Seguretat (ENS) i qualsevol norma que derive o estiga tractada en aquest.

Es mantindrà un Annex amb la identificació de la normativa aplicable.

## 7. Organització de la Seguretat de la Informació

### 7.1. Criteris de la Seguretat de la Informació

L'ATV tenint en compte els articles 11,12 i 13 de l'ENS (Reial decret 311/2022), estableix les següents accions per a organitzar la Seguretat de la Informació:

- i. Designarà rols de seguretat: Responsables unificats de Serveis i de la Informació, Responsable de la Seguretat, Responsable del Sistema i Delegat de Protecció de Dades.
- ii. Constituirà un òrgan consultiu i estratègic per a la presa de decisions en matèria de Seguretat de la Informació. Aquest òrgan es denominarà Comité de Seguretat de la Informació.

## **7.2. Definició de Rols i Responsabilitats associats a l'Esquema nacional de Seguretat**

### **7.2.1. Responsable de la Informació i dels Serveis**

Seràn funcions dels Responsables de la Informació i dels Serveis:

- Establir els requisits de seguretat aplicables a la Informació (nivells de seguretat de la Informació) i als Serveis (nivells de seguretat dels serveis), dins del marc establert en l'Annex I del RD ENS, podent recaptar una proposta al Responsable de Seguretat i tenint en compte l'opinió del Responsable del Sistema.
- Dictaminar respecte als drets d'accés a la informació i els serveis.
- Acceptar els nivells de risc residual que afecten la informació i els serveis.
- Posar en comunicació del Responsable de Seguretat qualsevol variació respecte a la Informació i els Serveis dels quals és responsable, especialment la incorporació de nous Serveis o Informació al seu càrrec. El qual donarà trasllat d'aquests canvis, al Comité de Seguretat de la Informació, en la seua pròxima reunió.
- Té la responsabilitat última de l'ús que es faça de determinats serveis i informació i, per tant, de la seua protecció.

### **7.2.2. Responsable de la Seguretat de la Informació**

Seràn funcions del Seguretat de la Informació (d'ara en avant, Responsable de Seguretat):

- Mantindre i verificar el nivell adequat de seguretat de la Informació manejada i dels Serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la Declaració d'Aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries i elaborar documentació del sistema.
- Aprovar la Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides conforme a l'Annex II de l'ENS.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable del Sistema i/o Comité de Seguretat TIC.



- Participar en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat, procedint a la seua validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comité de Seguretat l'aprovació de canvis i altres requisits del sistema.
- Aprovar els procediments de seguretat que formen part del Mapa Normatiu (i no són competència del Comité) i posar en coneixement al Comité de les modificacions que s'hagen realitzat al llarg del període en curs.
- Participarà en l'elaboració, en el marc del Comité de Seguretat de la Informació, la Política de Seguretat de la Informació, per a la seua aprovació per Direcció.
- Actuarà com a Secretari del Comité de Seguretat de la Informació, realitzant les següents funcions:
  - Convocar les reunions del Comité de Seguretat de la Informació.
  - Preparar els temes a tractar en les reunions del Comité, 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 Comité.

### **7.2.3. Responsable del Sistema**

Seràn funcions del Responsable del Sistema:

- Desenvolupar, operar i mantindre el sistema d'informació durant tot el seu cicle de vida, elaborant els procediments operatius necessaris.
- Definir la topologia i la gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en aquest.
- Detindre l'accés a informació o prestació de servei si té el coneixement que aquests presenten deficiències greus de seguretat.
- Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable de Seguretat i/o Comité de Seguretat de la Informació de la Informació.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat.
- Coordinar les funcions de l'administrador de la seguretat del sistema:
  - La gestió, configuració i actualització, en el seu cas, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
  - La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la seua correspondència amb l'autoritzat.
  - Aprovar els canvis en la configuració vigent del Sistema d'Informació.
  - Assegurar que els controls de seguretat establits són complits estrictament.
  - Assegurar que són aplicats els procediments aprovats per a manejar el Sistema d'Informació.

- Supervisar les instal·lacions de maquinari i programari, les seues modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.
- Informar el Responsable de Seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Col·laborar en la investigació i resolució d'incidents de seguretat, des de la seua detecció fins a la seua resolució.

### **7.3. D'Assignació de Rols i Responsabilitats associats a l'Esquema nacional de Seguretat**

- Responsable de Sistema: Prefectura de Servei de Tele administració.
- Responsable de Seguretat de la Informació: Prefectura de Departament d'Informàtica.
- Responsables del Servei i de la Informació: Prefectures d'àrea de l'ATV i Delegat/da d'Alacant i Castelló.

### **7.4. Comité de Seguretat de la Informació**

En l'ATV, s'ha creat el Comité de Seguretat de la Informació que estarà compost pels següents membres:

- Presidència: Subdirecció general
- Secretari: Responsable de Seguretat
- Vocals: Responsables de l Servei i Informació.

Aquests membres es classificaran en permanents o no permanents atenc l'obligatorietat de la participació del Comité de Seguretat de la Informació:

- Membres permanents:
  - Presidència
  - Responsable de Sistema
  - Responsable de Seguretat de la Informació
  - Assessors que es consideren oportuns per als temes en qüestió amb veu, però sense vot.
- Membres no permanents:
  - Responsables del Servei i de la Informació.
  - El Delegat de Protecció de dades.
  - Representants de l'ATV, especialistes externs dels sectors públic, privat, la presència del qual, per raó de la seua experiència o vinculació amb els assumptes tractats, siga necessària o aconsellable.

Els Responsables de la Informació i els Serveis seran convocats per la presidència en funció dels assumptes a tractar, en representació dels diferents àmbits o àrees de

seguretat TIC de l'ATV. Cada àrea estarà representada per un vocal amb vot, sense perjudici que acudisquen diversos representants d'aquesta.

El Delegat de Protecció de Dades participarà amb veu, però sense vot en les reunions del Comitè de seguretat de la informació quan en el mateix vagen a abordar-se qüestions relacionades amb el tractament de dades de caràcter personal, així com sempre que es requerisca la seua participació. En tot cas, si un assumpte se sotmetera a votació, es farà constar sempre en acta l'opinió del Delegat de Protecció de Dades.

El Secretari/a del Comitè realitzarà les convocatòries i alçarà actes de les reunions del Comitè de Seguretat. A les sessions del Comitè de Seguretat podran assistir en qualitat d'assessors les persones que en cada cas estime pertinents el seu President.

#### **7.4.1. Atribucions del Comitè de Seguretat de la Informació**

Seràn funcions del Comitè de Seguretat:

- Atendre les inquietuds de l'Alta Direcció i dels diferents departaments.
- Informar regularment de l'estat de la seguretat de la informació a l'Alta Direcció.
- Promoure la millora contínua del Sistema de Gestió de la Seguretat de la Informació.
- Elaborar l'estratègia d'evolució pel que fa a la 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 documentació de seguretat de la informació.
- Estar permanentment informat de la normativa que regula la Certificació de Conformitat amb l'ENS, incloent-hi les seues normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.
- Estar permanentment informat de la relació d'Entitats de Certificació acreditades i organitzacions, públiques i privades, certificades.
- Estar permanentment informat de la relació d'esquemes de certificació de la seguretat amb els quals l'Administració Pública té establits arranjaments o acords de reconeixement mutu de certificats.
- Proposar directrius i recomanacions, que seran recollides en les corresponents actes de les reunions del Comitè, a les quals el seu president, haurà de donar complida resposta.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que aquests siguen consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
- Atendre les inquietuds, en matèria de Seguretat de la Informació, de l'Administració i de les diferents àrees, informant regularment de l'estat de la seguretat de la informació a la Direcció.
- Resoldre els conflictes de responsabilitat que puguen aparéixer entre els diferents responsables i/o entre diferents Departaments, elevant aquells casos en els quals no tinga suficient autoritat per a decidir.
- Assessorar en matèria de seguretat de la informació, sempre que li siga requerit.
- Revisar la Política de Seguretat de la Informació prèvia aprovació per l'Òrgan Superior.

- Aprovar el Pla d'Adequació per a la implantació de l'ENS.

#### **7.4.2. Periodicitat de les reunions i adopció d'acords**

- El Comité de Seguretat de la Informació es reunirà, almenys, una vegada a l'any, sense perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, requerisca d'una major freqüència en les reunions.
- En qualsevol cas, les reunions es convocaran per la seua Presidència, a través del Secretari, a la seua iniciativa o per majoria dels seus membres permanents.
- Les decisions s'adoptaran per consens dels membres permanents.

#### **7.5. Grup de Treball TIC**

Dins de l'estructura de governança de la ciberseguretat es constitueix l'Oficina **de Seguretat TIC**, les competències de la qual estaran relacionades amb les següents àrees de treball: adequació a l'ENS, normativa i gestió de riscos, anàlisi i millora contínua, seguretat en les interconnexions i connectivitat i altres funcions connexes o concordants. Per a la seua **composició** es proposa:

- Responsable de Seguretat
- Responsable del Sistema
- Delegat /da de la Secretaria General
- Consultor/a extern expert en ENS com a membre no permanent
- Tots aquells administradors especialistes de seguretat (intern o externs a l'ATV) que el Responsable de Seguretat determine que siguen necessaris com a membre no permanents.

##### **7.5.1. Atribucions del Grup de Treball TIC**

Les **funcions del Grup de Treball TIC** seran, entre altres que els puguen ser encomanades pel Comité de Seguretat:

- Gestió i operativa de la seguretat del Projecte d'Adequació, Implantació i gestió de la Conformitat en l'ENS, anàlisi i gestió de riscos, explotació, normativa i manteniment.
- Redacció i presentació de propostes al Comité de Seguretat TIC. Elaborarà els aspectes relacionats amb la ciberseguretat i els debatrà en primera instància, per a ser traslladats al Comité.
- Promoure de la millora contínua del sistema de gestió de la Seguretat de la Informació. Per a això s'encarregarà de:
  - Elaborar (i revisar regularment) la Política de Seguretat de la Informació per al seu trasllat al Comité de Seguretat TIC per a la seua revisió i posterior aprovació de l'òrgan superior.
  - Elaborar la normativa de Seguretat de la Informació per a la seua aprovació pel Responsable de Seguretat, amb coneixement del Comité

- Verificar els procediments de seguretat de la informació i altra documentació per a la seua aprovació.
- Elaborar programes de formació destinats a formar i sensibilitzar al personal en matèria de seguretat de la informació i protecció de dades.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
- Proposar plans de millora de la seguretat de la informació, amb la seua dotació pressupostària corresponent, prioritzant les actuacions en matèria de seguretat quan els recursos siguen limitats.
- Realitzar un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions respecte d'ells.
- Promoure la realització de les auditories periòdiques ENS que permeten verificar el compliment de les obligacions de l'ATV en matèria de seguretat de la Informació i protecció de dades.

### **7.5.2. Periodicitat de les reunions i adopció d'acords**

- Es reunirà, almenys, una vegada al trimestre i sempre abans de les celebracions del Comitè de Seguretat TIC.
- Es recaptarà els acords aconseguits, dels quals donarà compte al Comitè de Seguretat TIC, per a la seua aprovació, en el seu cas.
- L'Oficina podrà desenvolupar les seues funcions en ple o en Grups de Treball per a l'anàlisi i realització de propostes específiques. Les propostes plantejades en l'Oficina de Seguretat TIC seran sotmeses a anàlisi, debat i aprovació, si escau, per part del Comitè de Seguretat TIC.

## **7.6. Procediment de designació**

### **7.6.1. Procediment de designació Comitè de Seguretat de la Informació**

- La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants i la designació dels Responsables identificats en aquesta Política, es realitzarà per la Direcció General de l'ATV, mitjançant la corresponent Instrucció.
- Els rols nomenats es renovaran anualment de manera automàtica. Les baixes o modificacions en els rols designats, es comunicaran al Comitè i se seguiran els llits establits per a la designació del nou responsable.

### **7.6.2. Procediment de designació Grup de Treball TIC**

- El nomenament formal del Grup de Treball TIC i dels seus integrants es formalitzarà a través d'una acta del Comitè de Seguretat de la Informació.

## 8. Dades personals

L'ATV, només recollirà i tractarà dades personals quan siguin adequats, pertinents i no excessius i aquests es troben en relació amb l'àmbit i les finalitats per als quals s'hagen obtingut. D'igual manera, adoptarà les mesures d'índole tècnica i organitzatives necessàries per al compliment de la s normatives de Protecció de Dades.

L'ATV, publicarà el seu Registre d'Activitats de Tractament i realitzarà la gestió de riscos a través d'Anàlisis de Riscos i EPID, en el cas que fora necessari en l'organització.

## 9. Obligacions del personal

Tot el personal de la \*ATV, tant extern com intern, que interactue amb el sistema d'informació haurà de complir amb la present política de seguretat de la informació.

## 10. Gestió de riscos

Tots els sistemes afectats per la present Política de Seguretat de la Informació estan subjectes a una anàlisi de riscos amb l'objectiu d'avaluar les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà:

- Almenys una vegada a l'any.
- Quan canvien la informació i/o els serveis manejats de manera significativa.
- Quan ocórrega un incident greu de seguretat o es detecten vulnerabilitats greus.

El Responsable de la Seguretat serà l'encarregat que es realitze l'anàlisi de riscos, així com d'identificar mancances i febleses i posar-les en coneixement del Comitè de Seguretat de la Informació.

El Comitè de Seguretat de la Informació dinamitzarà la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

El procés de gestió de riscos comprendrà les següents fases:

- Categorització dels sistemes.
- Anàlisi de riscos.
- El Comitè de Seguretat de la Informació procedirà a la selecció de mesures de seguretat a aplicar que hauran de ser proporcionals als riscos i estar justificades.

Les fases d'aquest procés es realitzaran segons el que es disposa en els Annexos I i II del Reial decret 311/2022, de 3 de maig, i seguint les normes, instruccions, Guies CCN-STIC i recomanacions per a l'aplicació del mateix elaborades pel Centre Criptològic Nacional.

En particular, per a realitzar l'anàlisi de riscos, com a norma general s'utilitzarà una metodologia reconeguda d'anàlisi i gestió de riscos.

### **7.1. Riscos que es deriven del tractament de dades personals**

En avaluar el risc en relació amb la seguretat de les dades, s'han de tindre en compte els riscos que es deriven del tractament de les dades personals, com la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservats o tractats d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades, susceptibles en particular d'ocasionar danys i perjudicis físics, materials o immaterials.

## **11. Documentació Complementària**

La present Política de Seguretat de la Informació serà complementada amb documents més precisos (normes, guies i procediments de seguretat) que ajuden a dur a terme el proposat.

El cos normatiu es desenvoluparà en tres nivells:

- a) Primer nivell normatiu: constituït per la present Política de Seguretat de la Informació.
- b) Segon nivell normatiu: constituït per les normes de seguretat derivades de les anteriors amb l'objectiu d'indicar l'ús correcte d'aspectes concrets del sistema de gestió de seguretat de la informació.
- c) Tercer nivell normatiu: constituït per procediments de seguretat, guies i instruccions tècniques. Són documents que, complint amb l'exposat en la Política de Seguretat de la Informació, determinen les accions o tasques a realitzar en l'acompliment d'un procés.

Correspon a la Direcció General de l'ATV, l'aprovació de la Política de Seguretat de la Informació i sent el Comité de Seguretat de la Informació l'òrgan responsable de l'aprovació i difusió dels restants documents propis de l'ATV. L'ATV complementarà el seu cos normatiu amb documents propis de la Direcció General de Tecnologies de la Informació i les Comunicacions (d'ara en avant DGTIC), a causa de les competències horitzontals que ostenta en Tecnologies de la Informació i la Comunicació (TIC) de la Generalitat.

## **12. Terceres parts**

Quan l'ATV, preste serveis a altres organismes o manege informació d'altres organismes, se'ls farà partícipe d'aquesta Política de Seguretat de la Informació. S'establiran canals per al reporte i la coordinació dels respectius Comitès de Seguretat de la Informació i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'ATV, utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícipe d'aquesta Política de Seguretat i de la normativa de seguretat que concernisca a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establides en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics de reporte i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que s'establí en aquesta Política de Seguretat.

Quan algun aspecte d'aquesta Política de Seguretat de la Informació no puga ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir avant.

### 13. Millora contínua

La gestió de la seguretat de la informació és un procés subjecte a permanent actualització. Els canvis en l'organització, les amenaces, les tecnologies i/o la legislació són un exemple en els quals és necessària una millora contínua dels sistemes.

Per això, és necessari implantar un procés permanent que comportarà, entre altres accions:

- a) Revisió de la Política de Seguretat de la Informació.
- b) Revisió dels serveis i informació i la seua categorització.
- c) Execució amb periodicitat anual de l'anàlisi de riscos.
- d) Realització d'auditories internes o, quan procedisquen, externes.
- e) Revisió de les mesures de seguretat.
- f) Revisió i actualització de les normes i procediments.

### 14. Aprovació i entrada en vigor

Aquesta Política de Seguretat de la Informació, serà efectiva des de la seua data d'aprovació i fins que siga reemplaçada per una nova Política.

La Política de Seguretat de la Informació serà revisada pel Comité de Seguretat de la Informació a intervals planificats, que no podran excedir l'any de duració, o sempre que es produïsquen canvis significatius, a fi d'assegurar que es mantinga la seua idoneïtat, adequació i eficàcia.

Els canvis sobre la Política de Seguretat de la Informació hauran de ser aprovats pel Consell Rector de l'Agència Tributària Valenciana, d'acord amb el que s'estableix en l'article 12 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.



Qualsevol canvi sobre la mateixa haurà de ser difós a totes les parts afectades.

El text ha sigut aprovat en el Consell Rector de l'Agència Tributària Valenciana el 31 de gener de 2023.