

Anunci Política de Seguretat de la Informació de l'Ajuntament de Castelló de la Plana

En virtut de l'acord adoptat per la Junta de Govern Local de l'Ajuntament de Castelló de la Plana, en sessió de 24 d'abril de 2025, es deixa sense efecte el document de Política de Seguretat que va ser aprovat mitjançant acord de la Junta de Govern Local de l'Ajuntament de Castelló de la Plana, en data 31 de març de 2022, s'aprova la Política de Seguretat de la Informació de l'Ajuntament de Castelló de la Plana, en compliment del que s'estableix en el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, i altra normativa concordant, com a document en el qual es reflecteixen les directrius que regeixen la forma en què l'Ajuntament de Castelló de la Plana i els seus organismes dependents han de gestionar i protegir la informació i els serveis, i es designa als càrrecs unipersonals o òrgans col·legiats indicats en el document de la Política de Seguretat, per a ocupar els diferents rols de seguretat.

En compliment del citat acord, es publica el text íntegre del document de Política de Seguretat de la Informació:

«POLÍTICA DE SEGURETAT DE LA INFORMACIÓ AJUNTAMENT DE CASTELLÓ DE LA PLANA»



CONTROL DE VERSIONS

DATA	VERSIÓ	CANVIS REALITZATS
07/12/2021	01	Edició inicial del document
11/10/2023	02	Actualització al Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
02/11/2023	03	Homogeneïtzació
12/11/2024	04	Revisió i actualització



Sumario

1.INTRODUCCIÓ.....	4
1.1.Missió i valors de l'entitat.....	4
2.Justificació de la Política de Seguretat de la Informació.....	4
2.1.Necessitat de seguretat en els sistemes.....	4
2.2.REQUISITS DE SEGURETAT EN ELS DEPARTAMENTS.....	5
3.MARC NORMATIU.....	6
4.ORGANITZACIÓ DE LA SEGURETAT.....	6
4.1.DEFINICIÓ DE ROLS.....	6
4.2.RESPONSABLE DE LA INFORMACIÓ.....	7
4.3.Responsable del servei.....	8
4.4.RESPONSABLE DE SEGURETAT DE LA INFORMACIÓ.....	16
4.5.RESPONSABLE DEL SISTEMA.....	19
4.6.ADMINISTRADOR/A DE LA SEGURETAT DEL SISTEMA.....	20
4.7.RESPONSABLE DE SEGURETAT FÍSICA.....	21
4.8.RESPONSABLE DE GESTIÓ DEL PERSONAL.....	22
4.9.COMITÉ DE SEGURETAT DE LA INFORMACIÓ.....	22
4.9.1.Jerarquia en el procés de decisions i mecanismes de coordinació.....	24
4.9.2.Procediments de designació de persones.....	26
5.Gestió de riscos.....	26
5.1.Justificació.....	26
5.2.Criteris d'avaluació de riscos.....	27
5.3.Directrius de tractament.....	27
5.4.Procés d'acceptació del risc residual.....	27
5.5.Necessitat de realitzar o actualitzar les avaluacions de riscos.....	28
6.Gestió d'incidents de seguretat.....	28
6.1.Prevenició d'incidents.....	28



6.2.Monitoratge i detecció d'incidents.....	29
6.3.Resposta davant incidents.....	29
6.4.Recuperació davant incidents i plans de continuïtat.....	30
7.Obligacions del personal.....	30
8.TercerEs parts.....	30
9.Estructura normativa i desenvolupament de la Política de Seguretat.....	31
10.Revisió i aprovació de la política de seguretat.....	32
11.anNex. glossari de termes.....	33

1. INTRODUCCIÓ

1.1. Missió i valors de l'entitat

La missió de l'Ajuntament de Castelló de la Plana és prestar els serveis públics municipals en l'àmbit de les seues competències, sota atributs de qualitat, eficaces, eficients, fiables i segurs, amb una gestió transparent, mitjançant l'ús de les noves tecnologies i l'Administració electrònica, impulsant la participació i col·laboració de la ciutadania, i així facilitar que Castelló de la Plana siga una ciutat moderna, innovadora, emprenedora, oberta, dinàmica i cohesionada territorialment.

Els valors de l'Ajuntament de Castelló de la Plana (d'ara en avant, l'Ajuntament) és convertir la Ciutat de Castelló de la Plana en un referent i model de ciutat que promoga l'economia basada en la sostenibilitat, creativitat i innovació, i l'Ajuntament en una administració innovadora, eficient en la utilització dels recursos i responsable, subjecta als principis de participació, col·laboració i transparència, que millore el nivell de qualitat i eficiència del servei prestat per a una major satisfacció de ciutadans i empreses.

2. JUSTIFICACIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

2.1. Necessitat de seguretat en els sistemes

Per a dur a terme la missió, prestar els serveis i complir amb els objectius, l'Ajuntament, depén dels sistemes TIC (tecnologies de la informació i comunicacions).

Aquests sistemes han de ser administrats amb diligència, adoptant les mesures adequades per a protegir-los davant de danys accidentals o deliberats que puguin



afectar la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de la informació tractada o dels serveis prestats.

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, previndre els incidents i reaccionar amb prestesa si és el cas.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per a incidir en la confidencialitat, integritat, disponibilitat, autenticitat, traçabilitat, ús previst i valor de la informació i els serveis. Per a defensar-se d'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.

És per això que el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (d'ara en avant, Esquema Nacional de Seguretat), estableix en el seu article 12 que tots els òrgans superiors de les Administracions públiques hauran de disposar formalment de la seua política de seguretat, que serà aprovada pel titular de l'òrgan superior corresponent. Aquesta política de seguretat s'establirà d'acord amb els principis bàsics recollits en el seu article 5, i es desenvoluparà aplicant els requisits mínims enumerats en l'article 12.1 de la citada norma.

2.2. REQUISITS DE SEGURETAT EN ELS DEPARTAMENTS

Tots els departaments de l'ajuntament han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

Els diferents departaments han de cerciorar-se 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.

Els departaments han d'estar preparats per a previndre, detectar, reaccionar i recuperar-se d'incidentes, d'acord amb l'article 8 de l'Esquema Nacional de Seguretat.



3. MARC NORMATIU

- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Llei 39/2015 d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica.
- 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 lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.
- Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
- Reial decret 43/2021, de 26 de gener, pel qual es desenvolupa el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.

4. ORGANITZACIÓ DE LA SEGURETAT

4.1. DEFINICIÓ DE ROLS

Tal com indica l'article 13 de l'Esquema Nacional de Seguretat, la seguretat haurà de comprometre a tots els membres de l'ajuntament.

La política de seguretat, segons detalla l'Annex II de l'ENS, en la seua secció 3.1, ha d'identificar els responsables de vetlar pel seu compliment i ser coneguda per tots els membres de l'ajuntament.

La responsabilitat de l'èxit de l'Ajuntament, en última instància, en la seua direcció, com a responsable d'organitzar les funcions i responsabilitats, la política de seguretat



de l'ajuntament, i de facilitar els recursos adequats per a aconseguir els objectius proposats.

L'estructura organitzativa de seguretat, i jerarquia en el procés de decisions la componen:

Rol	Funcions
Direcció	Òrgans col·legiats o unipersonals que decideixen la missió i els objectius de l'Ajuntament.
Comité de Seguretat	Òrgans col·legiats o unipersonals que prenen decisions que concreten com aconseguir els objectius marcats pels òrgans de govern.
Responsable de la informació	A nivell de govern. Té la responsabilitat última sobre quina seguretat requereix una certa informació manejada per de l'Ajuntament.
Responsable de servei	A nivell de govern o, a vegades baixa a nivell executiu. Té la responsabilitat última de determinar els nivells de servei acceptables per de l'Ajuntament.
Responsable de seguretat	A nivell executiu. Funciona com a supervisor de l'operació del sistema i vehicle de reporte al Comité de Seguretat de la Informació.
Responsable del sistema	A nivell operacional. Pren decisions operatives: arquitectura del sistema, adquisicions, instal·lacions i operació del dia a dia.

4.2. RESPONSABLE DE LA INFORMACIÓ

El responsable de la informació ha de ser una persona que ocupe un alt càrrec en la direcció de l'Ajuntament.

Compatibilitats. Aquest rol únicament podrà coincidir amb el de responsable de servei i el responsable d'informació en organitzacions de reduïdes dimensions que tinguen una estructura autònoma de funcionament.

Incompatibilitats. Aquest rol no podrà coincidir amb el de responsable del sistema i el d'administrador de seguretat del sistema, encara que es tracte d'organitzacions de reduïdes dimensions que tinguen una estructura autònoma de funcionament.

S'ha designat responsable de la informació l'alcalde/essa de l'Ajuntament o regidor/a en qui delegue.



Al responsable de la informació corresponen les següents funcions:

Funció	Detall
Establir requisits de seguretat sobre la informació	Estableix els requisits de la informació en matèria de seguretat. En el marc de l'Esquema Nacional de Seguretat, equival a la potestat de determinar els nivells de seguretat de la informació.
Determinar nivells de seguretat en cada dimensió	Determinar els nivells de seguretat en cada dimensió (confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat) dins del marc establert en l'Annex I de l'Esquema Nacional de Seguretat. Encara que l'aprovació formal dels nivells corresponga al responsable de la informació, podrà recaptar una proposta del responsable de la seguretat i convé que escolte l'opinió del responsable del sistema.
Adoptar mesures sobre les dades personals	Adoptar les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat de les dades de caràcter personal i eviten la seua alteració, pèrdua, tractament o accés no autoritzat, tenint en compte de l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos al fet que estan exposats, ja provenen de l'acció humana o del medi físic o natural.
Respondre de l'ús	Té la responsabilitat última de l'ús que es faça d'una certa informació i, per tant, de la seua protecció.

4.3. Responsable del servei

El responsable del servei pot ser una persona concreta o pot ser un òrgan corporatiu, que revestirà la forma d'òrgan col·legiat d'acord amb la normativa administrativa.

Compatibilitats.

És possible que coincidisquen en la mateixa persona o òrgan les responsabilitats de la informació i del servei. La diferenciació té sentit:

- Quan el servei maneja informació de diferents procedències, no necessàriament de la mateixa unitat departamental que la que presta el servei.
- Quan la prestació del servei no depén de la unitat que és responsable de la informació.



Incompatibilitats.

Aquest rol no podrà coincidir amb el de responsable de seguretat, excepte en organitzacions de reduïda dimensió que funcionen de manera autònoma.

Aquest rol no podrà coincidir amb el de responsable de sistema ni amb el d'administrador de la seguretat del sistema, ni tan sols quan es tracte d'organitzacions de reduïda dimensió que funcionen de manera autònoma.

S'ha designat com a responsables de servei a les persones que ostenten el lloc de major responsabilitat administrativa/operativa en cada servei. Aquests llocs figuren en la RLT anual i es mantenen actualitzats via canvis en la denominació del càrrec o en la mateixa RLT.

Els Serveis són els següents:

Nom del servei
Alcaldia
Grups polítics
Secretaria General
Intervenció General Municipal
Assessoria Jurídica
Planificació i Projecció Econòmica
Gestió Pressupostària i Comptabilitat
Tresoreria
Gestió Tributaria
Recursos Humans
Contractació
Estadística i Padró
Atenció Integrada i Registro General
Gestió Cadastral
Polícia Local
Servei d'Extinció d'Incendis i Protecció Civil
Benestar Social
Vivenda
Educació
Cultura





Arxiu
Participació Ciutadana
Joventut
Igualtat
Comerç i Mercats
Urbanisme
Medi Ambient
Aigües, sanejament i recollida de residus
Manteniment, infraestructures i comunicacions
Mobilitat
Festes
Esports
Agència de Desenvolupament Local
Turisme
Informàtica
Consum
Serveis funeraris
Família i Infància
Sanitat
Modernització i Qualitat dels Serveis
Gent Gran
Pacte Local per l'Ocupació

Les funcions i informació manejades per aquests serveis són els següents:

Nom del servei	Descripció
Alcaldia	Gestió de les agendes i l'activitat d'alcaldia.
Grups polítics	Gestió de les agendes i l'activitat dels grups polítics



Nom del servei	Descripció
Secretaria General	Gestió, seguiment i control sobre els actes municipals i els membres de la corporació local. Gestió d'expedients relacionats amb l'activitat municipal
Intervenció General Municipal	Control i fiscalització interna de la gestió econòmica, financera i pressupostària.
Assessoria Jurídica	Defensa jurídica
Planificació i Projecció Econòmica	Identificació, sol·licitud, gestió i justificació de línies d'ajuda i subvencions públiques que puguin ser d'interés municipal.
Gestió Pressupostària i Comptabilitat	Gestió econòmica i comptable de l'Ajuntament. Realització de pagaments corresponents, gestió de la facturació, control pressupostari i gestió fiscal.
Tresoreria	Gestió dels recursos financers, incloent-hi diners, valors o crèdits per operacions pressupostàries o extra pressupostàries.
Gestió Tributària	Gestió d'inspecció i tràmits relacionats amb tributs i altres ingressos de dret públic.
Recursos Humans	Gestió del personal intern (vacances, baixes, consultes, etc.). Prevenció de riscos laborals i accidents de treball. Gestió i publicació d'ofertes d'ocupació pública de personal de l'entitat local.
Contractació	Gestió dels procediments de contractació pública, així com el seguiment i control dels adjudicataris. Gestió patrimonial.



Nom del servei	Descripció
Estadística i Padró	Gestió del Padró municipal.
Atenció Integrada i Registre General	Gestió de l'entrada d'escrits o comunicacions presentats a l'Ajuntament, així com l'eixida dels escrits i comunicacions oficials dirigides a altres òrgans o particulars
Gestió Cadastral	Gestió de la informació cadastral en el marc del conveni amb cadastre.
Polícia Local	Serveis de Policia Local incloent la seguretat ciutadana, seguretat de les instal·lacions municipals i la regulació del trànsit, gestió de l'estacionament de vehicles i el servei de grua i depòsit municipal.
Servei d'Extinció d'Incendis i Protecció Civil	Serveis d'extinció d'incendis i protecció civil.
Benestar Social	Serveis d'avaluació i orientació per a persones en situacions de necessitat social, així com l'atenció immediata a persones en situació o risc d'exclusió social. Gestió de les prestacions i actuacions socials a persones i col·lectius vulnerables incloent les relacionades amb l'atenció a la dependència i la cooperació al desenvolupament.
Vivenda	Cooperació amb les administracions amb competències en vivenda.
Educació	Cooperació amb les administracions amb competències en educació.
Cultura	Promoció de la cultura i equipaments culturals. Gestió de la biblioteca municipal. Gestió de museus municipals.
Arxiu	Organització i localització d'expedients, documents o



Nom del servei	Descripció
	registres de l'Ajuntament que han passat a l'Arxiu Municipal. Gestió de les consultes, còpies i préstecs de documents de l'Arxiu Municipal. Conservació i consulta dels documents rebuts i produïts per l'entitat local.
Participació Ciutadana	Processos participatius. Gestió d'entitats ciutadanes i voluntariat del municipi. Publicitat activa i dret d'accés a la informació. Gestió de sol·licituds d'informació, queixes, reclamacions i iniciatives rebudes a l'Ajuntament.
Joventut	Assessorament i informació a la població jove del municipi, així com la realització d'activitats i esdeveniments enfocats a aquest col·lectiu.
Igualtat	Promoció de la igualtat entre homes i dones, així com contra la violència de gènere.
Comerç i Mercats	Fires, proveïments, mercats, llotges i comerç ambulant.
Urbanisme	Tramitació i resolució de sol·licituds, autoritzacions i llicències d'obres. Gestió de desenvolupaments urbanístic i obres públiques.
Medi Ambient	Manteniment de parcs i jardins públics. Gestió de la neteja viària. Promoció, prevenció i inspeccions relacionades amb la contaminació acústica, lumínica i atmosfèrica.
Aigües, sanejament i recollida de residus	Gestió i control dels serveis municipals d'aigües i sanejament i recollida d'escombraries.
Manteniment, infraestructures i comunicacions	Manteniment de la via pública i instal·lacions municipals.



Nom del servei	Descripció
Mobilitat	Gestió del trànsit, estacionament de vehicles i mobilitat. Transport col·lectiu urbà.
Festes	Promoure, fomentar organitzar les festes de la ciutat de Castelló de la Plana l'organització de les quals corresponguen a l'Excm. Ajuntament de Castelló de la Plana i col·laborar i assessorar en la celebració d'altres festes que s'organitzen a la ciutat per associacions, entitats, carrers i barris etc., sempre que aquestes festes tinguin caràcter públic.
Esports	Gestió d'instal·lacions esportives i promoció de l'esport en l'entitat local.
Agència de Desenvolupament Local	Orientació laboral. Subvencions d'ocupació. Emprenedoria.
Turisme	Promoció de l'entitat local mitjançant l'organització de diverses activitats, així com la promoció del turisme.
Informàtica	Gestió i control dels sistemes informàtics i de comunicacions de l'Ajuntament, així com la gestió de la seguretat d'aquests. WIFI públic. Gestió de les obligacions en matèria de protecció de dades.
Consum	Serveis de mediació en matèria de consum.
Serveis funeraris	Gestió del cementeri municipal i dels serveis funeraris.
Família i Infància	Atenció preventiva i integral de menors i les seues famílies. En aquesta línia, el Negociat de Família i Infància s'orienta a la gestió dels serveis, recursos i projectes municipals dirigits al suport a famílies i destinats a la prevenció i abordatge de situacions de



Nom del servei	Descripció
	risc social i a la promoció de la convivència familiar.
Sanitat	Informació de sanitat. Gestió de la tinència d'animals.
Modernització i qualitat dels serveis	Gestió i millora de la qualitat en els serveis municipals.
Gent Gran	Assessorament i informació a la gent gran del municipi, així com la realització d'activitats i esdeveniments enfocats a aquest col·lectiu.
Pacte Local	Formació, intermediació i observatori socioeconòmic en matèria d'ocupació.

Les funcions dels i de les responsables del servei són les següents:

Funció	Detall
Responsabilitat	Té la responsabilitat última de l'ús que es faça de determinats serveis i, per tant, de la seua protecció.
Establir els requisits de seguretat del servei	Té la potestat d'establir els requisits del servei en matèria de seguretat o, en terminologia de l'Esquema Nacional de Seguretat, la potestat de determinar els nivells de seguretat dels serveis. Encara que l'aprovació formal dels nivells corresponga al responsable del servei, es pot demanar una proposta al responsable de la seguretat i convé que s'escolte l'opinió del responsable del sistema.
Riscos	Aprovar el risc residual (el resultant una vegada aplicats els controls de seguretat).
Gestionar els registres d'activitat dels	Per delegació del responsable de tractament s'encarrega al responsable del servei el desenvolupament de les tasques relacionades amb la gestió dels tractaments de dades



tractaments del RGPD	personals que es realitzen en la seua àrea en concret.
-----------------------------	--

Consideracions. El responsable del servei haurà de tindre en compte les següents consideracions:

- La determinació dels nivells de seguretat en cada dimensió de seguretat ha de realitzar-se dins del marc establert en l'Annex I de l'Esquema Nacional de Seguretat. Es recomana que els criteris de valoració estiguen recolzats per la política de seguretat en la mesura en què siguen sistemàtics, sense perjudici que puguin donar-se criteris particulars en casos singulars.
- La prestació d'un servei sempre ha d'atendre els requisits de seguretat de la informació que maneja, de manera que poden heretar-se els requisits de seguretat d'aquesta, afegint requisits de disponibilitat, així com uns altres com a accessibilitat, interoperabilitat, etc.
- Continua sent vàlid el/la responsable de cada servei encara que la seua nomenclatura no coincidisca exactament amb la indicada en aquesta taula-relació, sempre que les seues funcions, rols i responsabilitats no hagen variat.

4.4. RESPONSABLE DE SEGURETAT DE LA INFORMACIÓ

El responsable de seguretat de la informació és una figura clau, ja que li correspon dinamitzar i gestionar el dia a dia de tot el procés de seguretat de la informació.

S'ha designat com a responsable de seguretat de la informació el o la cap de la Secció d'Innovació i Desenvolupament Tecnològic (SIDT).

Les funcions del responsable de seguretat són les següents:

Funció	Detall
Política, normativa i procediments	• Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, de la política i normativa de seguretat de la informació, per a la seua aprovació per direcció. • Elaborarà i sotmetrà a l'aprovació del Comitè els procediments operatius de seguretat de la informació.
Document de seguretat	• Coordinarà i controlarà les mesures definides en el document de seguretat i en general s'encarregarà del compliment de les mesures de seguretat que detalla el reglament de desenvolupament de la LOPD.



	• Coordinarà l'elaboració de la documentació de seguretat del sistema.
Formació i conscienciació	• Promourà la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat. • Elaborarà els plans de formació i conscienciació del personal en seguretat de la informació, que hauran de ser aprovats pel Comité de Seguretat de la Informació.
Gestió de la seguretat	• Mantindrà la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb el que s'estableix en la política de seguretat de l'Ajuntament. • Recopilarà els requisits de seguretat dels responsables d'informació i servei i determinarà la categoria del sistema. • Realitzarà l'anàlisi de riscos. • Facilitarà als responsables d'Informació i als responsables de servei informació sobre el nivell de risc residual esperat després d'implementar les opcions de tractament seleccionades en l'anàlisi de riscos i les mesures de seguretat requerides per l'Esquema Nacional de Seguretat. • Elaborarà una declaració d'aplicabilitat a partir de les mesures de seguretat requerides d'acord amb l'Annex II de l'Esquema Nacional de Seguretat i del resultat de l'anàlisi de riscos. • Elaborarà, al costat del o la responsable del sistema, el Pla de millora de la seguretat, per a la seua aprovació pel Comité de Seguretat de la Informació. • Validarà els plans de continuïtat de sistemes que elabore el o la responsable del sistema, que hauran de ser aprovats pel Comité de Seguretat de la Informació i provats periòdicament pel o la responsable del sistema. • Aprovarà les directrius proposades pel o la responsable del sistema per a considerar la seguretat de la informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis. • Elaborar la memòria anual sobre l'estat de la seguretat de la informació, amb el progrés dels projectes dels plans de millora, resum de les actuacions en matèria de seguretat, dels incidents relatius a seguretat de la



	informació, de l'estat de la seguretat del sistema, i en particular del nivell de risc residual al qual està exposat el sistema.
Monitorar	• Monitorarà els principals riscos residuals assumits per l'organització i recomanarà possibles actuacions contra aquests. • Monitorarà l'acompliment dels processos de gestió d'incidents de seguretat i recomanarà possibles actuacions respecte d'ells. En particular, vetlarà per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.
Assessorament	• Assessorarà a altres responsables en la determinació de les mesures de seguretat necessàries a partir dels requisits de seguretat establits pel context intern i extern de l'àmbit de l'Ajuntament.
Comité de Seguretat.	• Facilitarà periòdicament al Comité de Seguretat un resum d'actuacions en matèria de seguretat, d'incidents relatius a seguretat de la informació i de l'estat de la seguretat del sistema (en particular del nivell de risc residual al qual està exposat el sistema).

Delegació de funcions

En cas que, per la seua complexitat, distribució, separació física dels seus elements o nombre d'usuaris es necessite de personal addicional per a dur a terme les funcions de responsable de la seguretat, es podrà designar els nombre de responsables de seguretat delegats que es considere necessari.

La designació correspon al o la responsable de la seguretat. Per mitjà de la designació de delegats, es deleguen funcions. La responsabilitat final continua recaient sobre el o la responsable de la seguretat.

Els delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegue el o la responsable de la seguretat. És habitual que s'encarreguen de la seguretat de sistemes d'informació concrets o de sistemes d'informació horitzontals.

Cada delegat tindrà una dependència funcional directa del o la responsable de la seguretat, que és a qui reporten.



4.5. RESPONSABLE DEL SISTEMA

El o la responsable del sistema és la persona que pren les decisions operatives: arquitectura del sistema, adquisicions, instal·lacions i operació del dia a dia.

Compatibilitats. Aquest rol podrà coincidir amb el d'administrador de seguretat del sistema en organitzacions d'una dimensió reduïda o intermèdia que tinguin una estructura autònoma de funcionament.

Incompatibilitats. Aquest rol no podrà coincidir amb el de responsable d'informació, amb el de responsable de servei ni amb el de responsable de seguretat corporativa o de la informació.

S'ha designat com a responsable del sistema el o la cap del Negociat de Sistemes i Seguretat Informàtica.

Les funcions del o la responsable del sistema són les següents:

Funció	Detall
Gestionar el sistema	- Desenvolupar, operar i mantindre el sistema d'informació durant tot el seu cicle de vida, de les seues especificacions, instal·lació i verificació del seu correcte funcionament. - Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat. - Acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que pogueren afectar la satisfacció dels requisits establits. Aquesta decisió ha de ser acordada amb els i les responsables de la informació afectada, del servei afectat i amb el o la responsable de la seguretat abans de ser executada.
Establir directrius i mesures	- Definir la topologia i sistema de gestió del sistema d'informació establint els criteris d'ús i els serveis disponibles en aquest. - Definir la política de connexió o desconnexió d'equips i usuaris nous en el sistema. - Decidir les mesures de seguretat que aplicaran els subministradors de components del sistema durant les etapes de desenvolupament, instal·lació i prova d'aquest. - Determinar la configuració autoritzada de maquinari i programari a utilitzar en el sistema. - Delimitar les responsabilitats de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del sistema.
Elaborar	- Elaborar procediments operatius de seguretat. - Establir plans de contingència i emergència, duent a terme freqüents exercicis perquè el personal s'hi familiaritze.



Aprovar	• Aprovar els canvis que afecten la seguretat del mode d'operació del sistema. • Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.
Monitorar	• Monitorar l'estat de la seguretat del sistema d'informació i reportar-lo periòdicament o davant incidents de seguretat rellevants al o la responsable de seguretat de la informació.

Delegació de funcions.

En cas que, per la seua complexitat, distribució, separació física dels seus elements o nombre d'usuaris es necessite de personal addicional per a dur a terme les funcions de responsable del sistema, es podrà designar el nombre de responsables del sistema delegats que es considere necessari.

La designació correspon al o la responsable del sistema. Per mitjà de la designació de delegats, es deleguen funcions. La responsabilitat final continua recaient sobre el o la responsable del sistema.

Els delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegue el o la responsable del sistema relacionades amb l'operació, manteniment, instal·lació i verificació del correcte funcionament del sistema d'informació. És habitual que s'encarreguen de subsistemes d'informació d'una certa envergadura o de sistemes d'informació que presten serveis horitzontals.

4.6. ADMINISTRADOR/A DE LA SEGURETAT DEL SISTEMA.

L'administrador/a de seguretat és la persona encarregada d'executar les accions diàries d'operació del sistema segons les indicacions rebudes dels seus superiors jeràrquics.

S'han designat com a administrador/s de la seguretat del sistema les o els tècnics del Negociat de Sistemes i Seguretat Informàtica juntament amb la o el tècnic en Seguretat de la Informació.

Les funcions de l'administrador/a de la seguretat del sistema són les següents:



Funció	Detall
Implementar, gestionar i mantindre la seguretat	• La implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació. • Assegurar que els controls de seguretat establits són complits estrictament. • Informar els i les responsables de la seguretat i del sistema 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.
Gestió, configuració i actualització	• La gestió, configuració i actualització, si és el cas, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat del sistema d'informació. • Aprovar els canvis en la configuració vigent del 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.
Gestió de les autoritzacions	• La gestió de les autoritzacions concedides a les persones usuàries del sistema, en particular els privilegis concedits, incloent-hi el monitoratge que l'activitat desenvolupada en el sistema s'ajusta a l'autoritzat.
Aplicar els procediments	• L'aplicació dels procediments operatius de seguretat. • Assegurar que són aplicats els procediments aprovats per a manejar el sistema d'informació.
Monitorar la seguretat	• Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica implementats en el sistema.

4.7. RESPONSABLE DE SEGURETAT FÍSICA

Quan la seguretat física (de les instal·lacions) estiga segregada de la seguretat lògica, aquesta s'ajustarà al que s'estableix per l'Esquema Nacional de Seguretat en matèria de protecció física de manera anàloga al que s'estableix en els punts anteriors.

El o la responsable de la seguretat física implantarà les mesures de seguretat que li competisquen dins de les determinades pel o la responsable de la seguretat de la informació, i li informarà del seu grau d'implantació, eficàcia i incidents.



S'ha designat com a responsable de seguretat física e o la comissària principal cap de la Policia Local

4.8. RESPONSABLE DE GESTIÓ DEL PERSONAL

S'ha designat com a responsable de gestió de personal el o la cap de la Secció de Gestió i Desenvolupament de RRHH. a qui correspon implantar les mesures de seguretat que li competisquen dins de les determinades per l'Esquema Nacional de Seguretat col·laborant-hi en la seua implantació, eficàcia i resolució d'incidents.

4.9. COMITÉ DE SEGURETAT DE LA INFORMACIÓ

S'ha creat el Comité de Seguretat de la Informació que estarà format pels següents membres:

PRESIDENTA: alcaldessa (qui actuarà com a responsable d'informació o regidor/a en qui delegue)

SECRETARI/ÀRIA: responsable de seguretat de la informació.

VOCALS PERMANENTS:

- Secretari General de l'Administració Municipal.
- Titular d'Assessoria Jurídica.
- Responsable del sistema
- Responsable de seguretat de la informació (actuarà com a secretari/ària del Comité)
- Responsable de seguretat física.
- Delegat/ada de protecció de dades.
- Cap del Servei de Manteniment, Infraestructures i Comunicacions.

ALTRES VOCALS:

- Responsables de servei (seran convocats segons ho requerisquen els temes a tractar).

Funcions del secretari/ària. Correspon al secretari/ària del Comité de Seguretat de la Informació:



- Convocar les reunions del Comité de Seguretat de la informació
- Preparar els temes a tractar en les reunions del comité aportant informació concreta per a la presa de decisions.
- Elaborar l'acta de les reunions.
- La responsabilitat de l'execució directa o delegada de les decisions del comité.

Funcions dels vocals. Correspon als i les vocals del Comité de Seguretat de la Informació:

- Participar en les reunions.
- Contribuir amb idees i suggeriments per al bon desenvolupament de les reunions.

Totes i tots els membres del comité actuaran amb veu i vot i els seus acords requeriran, com a mínim, el vot de la majoria simple dels seus membres.

Funcions del comité. Correspon al Comité de Seguretat de la Informació:

Funció	Detall
Informar	• Atendre les inquietuds de direcció de l'Ajuntament i dels diferents departaments/àrees. • Informar regularment de l'estat de la seguretat de la informació a la direcció de l'Ajuntament.
Promoure	• Promoure la millora contínua del sistema de gestió de la seguretat de la informació. • Promoure la realització de les auditories periòdiques que permeten verificar el compliment de les obligacions de l'Ajuntament en matèria de seguretat.
Coordinar	• Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats. • Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables o entre diferents àrees de l'Ajuntament, i elevar aquells casos en els quals no tinga suficient autoritat per a decidir.
Elaborar	• Elaborar (i revisar regularment) la política de seguretat de la informació perquè siga aprovada per la direcció. • Elaborar l'estratègia d'evolució de l'Ajuntament pel que fa



	a la seguretat de la informació.
Aprovar	• 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 • Aprovar plans de millora de la seguretat de la informació de l'Ajuntament. En particular, vetlarà per la coordinació de diferents plans que puguin realitzar-se en diferents àrees.
Controlar	• Monitorar l'acompliment 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. • Vetlar perquè la seguretat de la informació es tinga 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 reduïsquen duplicitats i donen suport a un funcionament homogeni de tots els sistemes TIC.

Per a dotar de major agilitat el comitè, es crearà una comissió operativa de caràcter tècnic, que exercirà les funcions executives. Aquesta comissió estarà formada pel o per la responsable de seguretat de la informació i per dos administradors/es de seguretat i mantindrà reunions de caràcter mensual. A aquestes reunions podran acudir personal assessor extern convidat per la comissió.

4.9.1. Jerarquia en el procés de decisions i mecanismes de coordinació

Els diferents rols de seguretat de la informació (autoritat principal i possibles delegades) es limiten a una jerarquia simple: el Comitè de Seguretat de la Informació dona instruccions al o la responsable de la seguretat de la informació que s'encarrega de dur-la a terme i supervisar quins administradors i operadors implementen les mesures de seguretat segons el que s'estableix en la política de seguretat aprovada per l'Ajuntament.

El o la responsable de la seguretat:



- Informa el o la responsable de la informació de les decisions i incidents en matèria de seguretat que afecten la informació que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.
- Informa el o la responsable del servei de les decisions i incidents en matèria de seguretat que afecten el servei que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.
- Dona compte al Comité de Seguretat de la Informació, com a secretari/ària:
 - Resum consolidat d'actuacions en matèria de seguretat.
 - Resum consolidat d'incidentes relatius a la seguretat de la informació.
 - Estat de la seguretat del sistema, en particular del risc residual al qual el sistema està exposat.
- Dona compte a la Junta de Govern Local, segons els acords en el Comité de Seguretat de la Informació.
 - Resum consolidat d'actuacions en matèria de seguretat.
 - Resum consolidat d'incidentes relatius a la seguretat de la informació.
 - Estat de la seguretat del sistema, en particular del risc residual al qual el sistema està exposat.

El o la responsable del sistema:

- Informa el o la responsable de la informació de les incidències funcionals relatives a la informació que li competeix.
- Informa el o la responsable del servei de les incidències funcionals relatives al servei que li competeix.
- Dona compte al o a la responsable de la seguretat:
 - Actuacions en matèria de seguretat, en particular quant a decisions d'arquitectura del sistema.
 - Resum consolidat dels incidents de seguretat.
 - Mesures de l'eficàcia de les mesures de protecció que s'han d'implantar.



4.9.2. Procediments de designació de persones

La direcció de l'Ajuntament nomenarà formalment mitjançant la seua publicació en el butlletí oficial corresponent:

- el o la responsable de la informació; pot ser un càrrec unipersonal o un òrgan col·legiat (típicament, el Comitè de Seguretat de la Informació).
- el o la responsable del servei; pot ser el mateix que el o la responsable de la informació; pot ser un càrrec unipersonal o un òrgan col·legiat (típicament, el Comitè de Seguretat de la Informació).
- el o la responsable de la seguretat, que ha de reportar directament a la direcció o, quan existisquen, als comitès de seguretat de la informació i seguretat corporativa.
- el o la responsable del sistema, que ha de reportar directament a la direcció o, quan existisquen, als comitès de seguretat de la informació i seguretat corporativa.

La direcció de l'organització designa la persona responsable del sistema:

- A proposta del o de la responsable de la informació tractada, quan el sistema d'informació tracte una única informació.
- A proposta del o de la responsable del servei prestat, quan el sistema d'informació preste un únic servei.
- Directament, quan el sistema d'informació tracta diferents informacions o presta diferents serveis, sentits els responsables de les informacions i els serveis afectats.

La direcció de l'Ajuntament designa l'administrador/a de seguretat del sistema a proposta del o de la responsable del sistema.

5. GESTIÓ DE RISCOS

5.1. Justificació

Tots els sistemes subjectes a aquesta política hauran de realitzar una anàlisi de riscos avaluant les amenaces i els riscos als quals estan exposats.

L'anàlisi de riscos serà la base per a determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establits per l'Esquema Nacional de Seguretat, segons el que es preveu en l'article 7.



5.2. Criteris d'avaluació de riscos

Per a l'harmonització de les anàlisis de riscos, el Comité de Seguretat de la Informació establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

Els criteris d'avaluació de riscos detallats s'especificaran en la metodologia d'avaluació de riscos que elaborarà l'organització, basant-se en estàndards i bones pràctiques reconegudes.

Hauran de tractar-se, com a mínim, tots els riscos que puguin impedir la prestació dels serveis o el compliment de la missió de l'organització de manera greu.

Es prioritzaran especialment els riscos que impliquen un cessament en la prestació de serveis als ciutadans.

5.3. Directrius de tractament

El Comité de Seguretat de la Informació dinamitzarà la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes i promourà inversions de caràcter horitzontal.

5.4. Procés d'acceptació del risc residual

Els riscos residuals seran avaluats pel o per la responsable de seguretat de la informació.

Els nivells de risc residual esperats sobre cada informació després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II de l'Esquema Nacional de Seguretat) hauran de ser acceptats prèviament per la persona responsable d'aquesta informació.

Els nivells de risc residual esperats sobre cada servei després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II de l'Esquema Nacional de Seguretat) hauran de ser acceptats prèviament per la persona responsable d'aquest servei.

Els nivells de risc residuals seran presentats pel o la responsable de seguretat de la informació al Comité de Seguretat de la Informació, perquè aquest procedisca, si és el cas, a avaluar, aprovar o rectificar les opcions de tractament proposades.



5.5. Necessitat de realitzar o actualitzar les avaluacions de riscos

L'anàlisi dels riscos i el seu tractament han de ser una activitat repetida regularment, segons el que s'estableix en l'article 10 de l'Esquema Nacional de Seguretat. Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada a l'any.
- Quan es produïsquen canvis significatius en la informació manejada.
- Quan es produïsquen canvis significatius en els serveis prestats.
- Quan es produïsquen canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.
- Quan ocorrega un incident greu de seguretat.
- Quan es reporten vulnerabilitats greus.

6. GESTIÓ D'INCIDENTS DE SEGURETAT

6.1. Prevenció d'incidents

Els departaments de l'Ajuntament han de previndre que la informació o els serveis es vegen perjudicats per incidents de seguretat.

L'Esquema Nacional de Seguretat estableix la que els sistemes han de dissenyar-se i configurar-se de manera que garantisquen la seguretat per defecte. D'igual forma, l'article 18 de l'Esquema Nacional de Seguretat defineix que els sistemes s'instal·laran en àrees separades, dotades d'un procediment de control d'accés.

Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'Esquema Nacional de Seguretat, així com qualsevol control addicional identificat a través d'una avaluació d'amenaques 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 deuen:

- Establir àrees segures per als sistemes d'informació crítica o confidencial.



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

6.2. Monitoratge i detecció d'incidents

Atés que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seua detenció, els serveis han de monitorar 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 10 de l'Esquema Nacional de Seguretat.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 9 de l'Esquema Nacional de Seguretat. S'establiran mecanismes de detecció, anàlisi i reporte que arriben a les persones responsables regularment i quan es produïska una desviació significativa dels paràmetres que s'hagen preestablit com a normals.

Els sistemes de detecció d'intrusos compleixen fonamentalment amb una labor de supervisió i auditoria sobre els recursos de l'Ajuntament i verificar que la política de seguretat no és violada i intentant identificar qualsevol tipus d'activitat maliciosa d'una forma primerenca i eficaç.

S'hauran d'establir, en funció de les necessitats, les següents classificacions:

- Sistemes de detecció d'intrusos a nivell de xarxa.
- Sistemes de detecció d'intrusos a nivell sistema.
- Sistemes de detecció d'intrusos a nivell físic

6.3. Resposta davant incidents

Els departaments de l'Ajuntament han de:

- Establir mecanismes per a respondre eficaçment als incidents de seguretat.
- Designar punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes.



- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els equips de resposta a emergències (CERT).

6.4. Recuperació davant incidents i plans de continuïtat

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.

7. OBLIGACIONS DEL PERSONAL

El personal treballador de l'Ajuntament té 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 a les i als afectats.

El personal treballador de l'Ajuntament atindrà una sessió de conscienciació en matèria de seguretat TIC almenys una vegada cada dos anys. S'establirà un programa de conscienciació contínua per a atendre les i els membres de l'organització, en particular les i els 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 en què la necessiten per a fer el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seua primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

El compliment de la present política de seguretat és obligatori per part de tot el personal intern o extern que intervinga en els processos l'organització, i constituirà el seu incompliment infracció greu a efectes laborals.

8. TERCERES PARTS

Quan es prestin serveis o es gestione informació d'altres organitzacions, se'ls farà partícip d'aquesta política de seguretat de la informació, s'establiran canals per a reportar i coordinació dels respectius comitès de seguretat de la informació i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.



Quan s'utilitzen serveis de tercers o cedisca informació a tercers, se'ls farà partícips 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 i podrà 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 l'establitz en aquesta política.

Quan algun aspecte de la política no puga ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del o la responsable de seguretat que precise els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe per les persones responsables de la informació i els serveis afectats abans de seguir avant.

9. ESTRUCTURA NORMATIVA I DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT

La estructura jeràrquica de la documentació de seguretat és la següent:

Document	Detall
Política	• Defineix les metes i expectatives de seguretat. • Descriu quin tipus de gestió de la seguretat es pretén aconseguir i quins són els objectius perseguits. • Ha de ser elaborada pel Comité de Seguretat i ser aprovada per la direcció.
Normativa	• Estableix el que s'ha de fer i uniformitza l'ús d'aspectes concrets del sistema. • És de caràcter obligatori. • Ha de ser escrita per persones expertes en la matèria o pel o la responsable de seguretat i aprovada pel Comité de Seguretat.
Procediment	• Un procediment ha de ser clar, senzill d'interpretar i no ambigu en la seua execució. No té per què ser extens, atés que la intenció del document és indicar les accions a desenvolupar. • Un procediment pot secundar-se en altres documents per a especificar, amb el nivell de detall que es desitge, les



	diferents tasques. Per a això, pot relacionar-se amb altres procediments o amb instruccions tècniques de seguretat. • Ha de ser elaborat pel o la responsable del sistema i aprovat pel o la responsable de seguretat.
Instruccions tècniques	• Determina les accions o tasques necessàries per a completar una activitat o procés d'un procediment concret sobre una part concreta del sistema d'informació (maquinari, sistema operatiu, aplicació, dades, usuari, etc.). • Igual que un procediment, són l'especificació detallada dels passos a executar. • Una instrucció tècnica ha de ser clara i senzilla d'interpretar. • Ha de documentar els aspectes tècnics necessaris perquè la persona que executa la instrucció tècnica no haja de prendre decisions respecte a l'execució d'aquesta. A major nivell de detall, major precisió i garantia de la seua correcta execució. • Poden ser elaborats pel o la responsable del sistema o administrador/a del sistema i han de ser aprovats pel o la responsable de seguretat.
Guies	• Tenen un caràcter formatiu i busquen ajudar les i els usuaris a aplicar correctament les mesures de seguretat proporcionant raonaments on no existeixen procediments precisos. Per exemple, sol haver-hi una guia sobre com escriure procediments de seguretat. • Les guies ajuden a previndre que es passen per alt aspectes importants de seguretat que poden materialitzar-se de diverses formes. • Han de ser aprovades pel o la responsable de seguretat.

10. REVISIÓ I APROVACIÓ DE LA POLÍTICA DE SEGURETAT

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 per la Junta de Govern Local, d'acord amb l'article 12 de l'Esquema Nacional de Seguretat.



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

11. ANNEX. GLOSSARI DE TERMES

Anàlisi de riscos

Utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos.

Dades de caràcter personal

Qualsevol informació concernent a persones físiques identificades o identificables.

Gestió d'incidents

Pla d'acció per a atendre les incidències que es donen. A més de resoldre-les ha d'incorporar mesures d'acompliment que permeten conèixer la qualitat del sistema de protecció i detectar tendències abans que es convertisquen en grans problemes.

Gestió de riscos

Activitats coordinades per a dirigir i controlar una organització respecte als riscos.

Incident de seguretat

Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació.

Política de seguretat

Conjunt de directrius plasmades en document escrit, que regeixen la forma en què una organització gestiona i protegeix la informació i els serveis que consideren crítics.

Principis bàsics de seguretat

Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis.

Responsable de la informació

Persona que té la potestat d'establir els requisits d'una informació en matèria de seguretat.

Responsable de la seguretat



El responsable de seguretat determinarà les decisions per a 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 exercida per alguna entitat oficial destinada a cuidar interessos o satisfer necessitats de la ciutadania.

Sistema d'informació

Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantindre, usar, compartir, distribuir, posar a disposició.»

Castelló de la Plana
El Cap de Secció d'Innovació i Desenvolupament Tecnològic,
David López López
(Document signat electrònicament)

