POLÍTICA DE SEGURETAT

AJUNTAMENT DE
SANT JOAN DESPÍ

AJUNTAMENT DE SANT JOAN DESPÍ

CONTROL DE VERSIONS

VERSIÓ	DESCRIPCIÓ DE CANVIS	PREPARAT	REVISAT	APROVAT
1.0	Primera versió del document	14/01/2025		

AJUNTAMENT DE SANT JOAN DESPÍ

ÍNDEX

AJUNTAMENT DE SANT JOAN DESPÍ

1 Aprovació i entrada en vigor

La Política de Seguretat de la Informació, d'ara endavant, PSI, serà validada pel Comitè de Seguretat de l'Ajuntament de Sant Joan Despí, i aprovada per l'Alcaldia-Presidència d'aquesta entitat o regidor/a delegat/da de Sistemes d'Informació.

Aquesta Política de Seguretat de la Informació és efectiva des de la data esmentada i fins que sigui reemplaçada per una nova política. En aquest sentit, es revisarà periòdicament, en intervals no superiors a 2 anys.

2 Introducció

L'Ajuntament de Sant Joan Despí depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per assolir els objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant de danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat de la informació tractada als 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 i reaccionant amb celeritat als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i els serveis a les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer un seguiment continu dels nivells de prestació dels serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

L'Ajuntament de Sant Joan Despí ha d'assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació.

L'Ajuntament de Sant Joan Despí ha d'estar preparat per prevenir, detectar, reaccionar, recuperar-se d'incidents i conservar la informació, d'acord amb l'article 5 del Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, en endavant (ENS).

3 Abast i missió de la Política de Seguretat de la Informació

Aquesta política té com a objectiu fonamental garantir la seguretat de la informació i la prestació continuada dels serveis que proporciona l'entitat. Aquesta política és aplicable i de compliment obligat per a tot el personal que, de manera permanent o eventual, presti els seus serveis a l'Ajuntament de Sant Joan Despí, especialment, els responsables dels serveis d'explotació dels

Sistemes d'Informació i els mateixos usuaris, com a actors tots dos, incloent-hi, si escau, el personal de proveïdors externs, quan sigui procedent i siguin usuaris dels Sistemes d'Informació.

A l'àmbit de la present Política, s'entén per usuari qualsevol empleat/empleada públic pertanyent o aliè a l'Ajuntament de Sant Joan Despí, així com personal d'organitzacions privades externes, entitats col·laboradores o qualsevol altre amb algun tipus de vinculació amb l'Ajuntament de Sant Joan Despí i que utilitzi o tingui accés als Sistemes d'Informació.

Això implica que les diferents àrees de l'Ajuntament de Sant Joan Despí han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos a la planificació, a la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

L'Ajuntament de Sant Joan Despí 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 les expectatives de la població i de tots els grups d'interès.

L'Ajuntament de Sant Joan Despí vol potenciar l'ús de les noves tecnologies tant internament com en les relacions amb la ciutadania.

Els principals objectius que es persegueixen són, entre d'altres, en aquest sentit, els següents:

- Millorar la qualitat dels serveis públics.
- Millorar la seguretat de la informació tractada per l'Ajuntament de Sant Joan Despí.
- Fomentar la relació electrònica de la ciutadania amb l'Ajuntament de Sant Joan Despí, creant la confiança necessària entre ciutadà i l'Ajuntament de Sant Joan Despí en aquesta relació.
- Fer transparent l´activitat de l´Ajuntament de Sant Joan Despí.
- Fomentar la participació i col·laboració.

4 Marc normatiu

Es pren com a referència bàsica en matèria de seguretat de la informació les normatives següents:

- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril del 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).
- 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 a l'àmbit de l'Administració Electrònica.

AJUNTAMENT DE SANT JOAN DESPÍ

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, de 1 d'octubre, de Règim Jurídic del Sector Públic.
- Llei 34/2002, de 11 de juny, de serveis de la societat de la informació i de comerç electrònic.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- Reial Decret Legislatiu 5/2015, del 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic.
- Reial Decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text Refós de la Llei de Propietat Intel·lectual.
- Reglament (UE) núm. 910/2014: relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior.
- Guia de Seguretat de les TIC CCN-STIC 801.
- Reglament (UE) 2016/679 del Parlament Europeo i del Consell. de 27 d' abril del 2016 (RGPD).
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals (LOPDGDD).

5 Principis bàsics

L'objecte últim de la seguretat de la informació és garantir que una organització podrà complir els seus objectius, desenvolupar les seves funcions i exercir-ne les competències utilitzant sistemes d'informació. Per això, en matèria de seguretat de la informació s'han de tenir en compte els principis bàsics següents:

a) Seguretat com a procés integral.

b) Gestió de la seguretat basada en els riscs.

c) Prevenció, detecció, resposta i conservació.

d) Existència de línies de defensa.

e) Continuar la vigilància.

f) Reavaluació periòdica.

g) Diferenciació de responsabilitats.

Aquests, desenvolupats al RD 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, seran de plena aplicació a l'entitat.

AJUNTAMENT DE SANT JOAN DESPÍ

6 Organització de la seguretat

La implantació de la Política de Seguretat a l'Ajuntament de Sant Joan Despí requereix que tots els membres de l'organització entenguin les obligacions i les responsabilitats en funció del lloc exercit. Com a part de la Política de Seguretat de la Informació, cada rol específic, personalitzat en usuaris concrets, ha d'entendre les implicacions de les seves accions i les responsabilitats que té atribuïdes, i queden identificades i detallades en aquesta secció, i que s'agrupen de la manera següent:

a) El Comitè de Seguretat de la Informació

b) Responsable de la Informació

c) Responsable del Servei

d) Responsable de Seguretat

e) Responsable de Sistemes

f) Administradors de sistemes

g) Delegat de Protecció de Dades

6.1 Comitè de Seguretat de la Informació

El Comitè de Seguretat de la Informació coordina la seguretat de la informació a l'Ajuntament de Sant Joan Despí.

- President: Alcalde/ssa o regidor/a delegat/da de Sistemes d'Informació.
- Secretari/a: Responsable de Seguretat de la Informació
- Vocals:
    - Assessor Jurídic
    - Responsable de Sistemes
    - Responsables de les unitats organitzatives municipals seran convocats pel president en funció dels temes a tractar (si afecten la seva àrea)
    - DPD (en aquest cas pot ser vocal sense dret a vot en ser personal extern)

Aquest Comitè està compost per cadascuna de les figures anteriorment esmentades.

El Comitè s'haurà de reunir amb caràcter ordinari cada tres mesos, sempre que sigui possible i, amb caràcter extraordinari per raons d'urgència i causa justificada o quan ho decideixi la seva Presidència.

El Comitè pot demanar del personal tècnic propi o extern la informació pertinent per a la presa de les seves decisions, així com convidar aquest personal a les reunions amb veu i sense vot.

El Comitè ajustarà el seu funcionament a les previsions contingudes al capítol II de la Llei 40/2015, de 1 d'octubre, de Règim Jurídic del Sector Públic.

El Responsable de la Seguretat, actuarà com a Secretari, amb veu i vot, i com a tal:

- Convoca les reunions del Comitè de Seguretat de la Informació.
- Aixecarà actes de les reunions del Comitè de Seguretat.
- Prepara els temes a tractar a les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- És responsable de l'execució directa o delegada de les decisions del Comitè.

Es convocarà la resta de persones amb responsabilitats als rols de l'ENS segons les necessitats del Comitè de Seguretat de la Informació.

Les funcions del Comitè de Seguretat de la Informació són les següents:

a) Elaborar els esborranys de modificació i actualització de la PSI.

b) Promoure la millora contínua del sistema de gestió de la seguretat de la informació.

c) Elaborar l'estratègia d'evolució de l'organització pel que fa a seguretat de la informació.

d) Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria i evitar duplicitats.

e) Aprovar les Normes de Seguretat TIC (documentació de segon nivell normatiu).

f) Assegurar la coordinació de les diferents àrees implicades en la gestió d'incidents de seguretat de la informació.

g) Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.

h) Aprovar plans de millora de la seguretat de la informació de l'Ajuntament de Sant Joan Despí. En particular, vetllarà per la coordinació de diferents plans que puguin realitzar-se en diferents àrees.

i) Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.

j) Vetllar perquè la seguretat de la informació es tingui en compte en tots els projectes TIC des de la seva especificació inicial fins a la posada en operació. En particular haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.

k) Impulsar el compliment i la difusió de la PSI, promovent les activitats de conscienciació i formació en matèria de seguretat per al personal de l'organització.

l) Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i entre diferents àrees de l'Ajuntament de Sant Joan Despí.

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

AJUNTAMENT DE SANT JOAN DESPÍ

Aquest assessorament es determinarà en cada cas, podent materialitzar-se de diferents formes i maneres:

- Grups de treball especialitzats interns, externs o mixtos.
- Assessoria interna i/o externa.
- Assistència a cursos o altres tipus d'entorns formatius o d'intercanvi d'experiències.

6.2 Responsable de la Informació (CSI)

Conformi als articles 11 i 41 del ENS, el Responsable de la Informació és la persona que estableix les necessitats de seguretat de la informació que es maneja i efectua les valoracions de l'impacte que tindria un incident que afectés la seva seguretat. Té, a més, la potestat de modificar el nivell de seguretat requerit per a aquesta (Annex II.5.7.2 de l'ENS).

La Disposició Addicional segona del RD 311/2022, de 3 de maig, estableix que entre d'altres, el CCN (Centre Criptològic Nacional), en l'exercici de les seves competències elaborarà i difondrà guies de seguretat d'obligat compliment.

D'acord al que es descriu al punt 5.1 de la Guia de Seguretat de les TIC CCN-STIC-801, els Responsables de la Informació, seran persones amb alt càrrec en la direcció de l'organització i pertanyents al comitè directiu del mateix. Aquest càrrec té la responsabilitat última de l'ús que es faci d'una certa informació i, per tant, de la seva protecció. Les seves funcions poden ser assignades a persones individuals, o bé ser assumides pel Comitè de Seguretat de la Informació.

A l'Ajuntament de Sant Joan Despí aquesta responsabilitat recaurà sobre l'alcalde/ssa o regidor/a delegat/da de Sistemes d'Informació.

La persona o òrgan que ho assumeixi haurà de ser identificada per a cada servei que presti l'organització.

Són funcions del Responsable de la Informació, dins del seu àmbit d'actuació, les següents:

a) Determinar els nivells de seguretat de la informació tractada, valorant els impactes dels incidents que afectin la seguretat de la informació (article 41 de l'ENS). Per fer-ho, podeu demanar l'assessorament del Responsable de Seguretat i del Responsable del Sistema.

b) És el responsable, juntament amb el Responsable del Servei, d'acceptar els riscos residuals calculats en l'anàlisi de riscos, i de fer-ne el seguiment i el control. Aquesta tasca podrà delegar-la, d'acord amb el Responsable del Servei, al Responsable de Seguretat i al Responsable del Sistema.

c) Adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a que estan exposats, ja provinguin de l'acció humana o del medi físic o natural.

d) Té la responsabilitat última de l'ús que es faci d'una certa informació i, per tant, de la seva protecció.

e) El Responsable de la Informació és el responsable últim de qualsevol error o negligència que porti a un incident de confidencialitat o integritat.

f) Estableix els requisits de la informació en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.

g) Encara que l'aprovació formal dels nivells correspongui al Responsable de la Informació, podrà demanar una proposta al Responsable de Seguretat i convé que escolti l'opinió del Responsable del Sistema.

Compatibilitat amb altres rols

Aquest rol podrà coincidir amb el del Responsable de Servei.

Aquest rol no podrà coincidir amb el de Responsable de Seguretat, excepte en organitzacions de reduïda dimensió que funcionin de manera autònoma.

Aquest rol no podrà coincidir amb el de Responsable de Sistema, ni tan sols quan es tracti d'organitzacions de reduïda dimensió que funcionin de forma autònoma.

6.3 Responsable del Servei (CSI)

D'acord amb l'article 13 de l'ENS, el responsable del servei és la persona que determina els requisits de seguretat del servei prestat.

Pel que fa al procés de gestió del risc, el Responsable del Servei és l'encarregat, juntament amb el Responsable de la Informació, d'acceptar els riscos residuals calculats en l'anàlisi de riscos, i de ferne el seguiment i el control. Aquesta tasca podrà delegar-la, d'acord amb el Responsable del Servei, al Responsable de Seguretat i al Responsable del Sistema.

El Responsable del Servei pot 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 poguessin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els Responsables de la Informació, Responsable de Seguretat i Responsable de Sistemes abans de ser executada.

D'acord al que es descriu al punt 5.2 de la Guia de Seguretat de les TIC CCN-STIC-801, els Responsables de la Informació, les seves funcions poden ser assignades a persones individuals, o bé ser assumides pel Comitè de Seguretat de la Informació.

A l'Ajuntament de Sant Joan Despí aquesta responsabilitat recaurà sobre l'alcalde/ssa o regidor/a delegat/da de Sistemes d'Informació.

La persona o òrgan que ho assumeixi haurà de ser identificada per a cada servei que presti l'organització.

Les seves funcions seran les següents:

AJUNTAMENT DE SANT JOAN DESPÍ

a) Estableix els requisits dels serveis en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.

b) Té la responsabilitat última de l'ús que es faci de determinats serveis i, per tant, de la protecció.

c) El Responsable del Servei és el responsable últim de qualsevol error o negligència que porti a un incident de disponibilitat dels serveis.

d) Determinarà els nivells de seguretat en cada dimensió del servei dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.

e) Encara que l'aprovació formal dels nivells correspongui al Responsable del Servei, podrà demanar una proposta al Responsable de la Seguretat i convé que escolti l'opinió del Responsable del Sistema.

f) La prestació d'un servei sempre ha d'atendre els requisits de seguretat de la informació que maneja, de manera que es poden heretar els requisits de seguretat d'aquesta, afegint-hi requisits de disponibilitat, així com altres com accessibilitat, interoperabilitat, etc.

Compatibilitat amb altres rols

Podrà coincidir en la mateixa persona o òrgan col·legiat el rol de Responsable de la Informació i del Responsable del Servei, encara que generalment no coincidiran quan:

- El servei gestioni informació de diferents procedències, no necessàriament de la mateixa unitat departamental que la que presta el servei.
- La prestació del servei no depengui de la unitat a què pertany el Responsable de la Informació.

Aquest rol no podrà coincidir amb el de Responsable de Seguretat, excepte en organitzacions de reduïda dimensió que funcionin de manera autònoma.

6.4 Responsable de Seguretat de la Informació

Aquest rol serà assumit per la persona Responsable Municipal d'Atenció a la Ciutadania qui podrà demanar ajut de suport tècnic segons les necessitats.

D'acord amb l'article 13 de l'ENS, el responsable de seguretat és la persona que determina les decisions per satisfer els requisits de seguretat de la informació i del servei.

Es nomenarà formalment com a tal, per part de l'òrgan de govern, una única persona a l'organització.

El rol no podrà ser desenvolupat per un òrgan col·legiat, ni hi podrà haver més d'una persona assumint el rol en l'organització, encara que pugui delegar part de les seves funcions en altres persones.

AJUNTAMENT DE SANT JOAN DESPÍ

Tal com es descriu a la Guia CCN-STIC-801: “La figura del “Responsable de la Seguretat” apareix a les dues normatives (ENS i LOPD) amb un paper molt similar com a persona que vetlla perquè els sistemes d'informació efectivament responguin a els requisits establerts. Les organitzacions faran bé de fer coincidir aquestes responsabilitats en una única figura, recopilant totes les funcions a la Política de Seguretat”.

Per tant, també es decideix que el Responsable de Seguretat exerceixi també de Responsable de Seguretat a l'efecte de compliment de la normativa en matèria de protecció de dades de caràcter personal.

Seran funcions del Responsable de Seguretat les següents:

a) Promoure la seguretat de la informació manejada i dels serveis electrònics prestats pels sistemes d'informació, amb la responsabilitat i l'autoritat per assegurar-se que el Sistema de Gestió de la Seguretat de la Informació compleix els requisits de l'Esquema Nacional de Seguretat.

b) Supervisar el compliment de la present Política, de les seves normes, procediments derivats i de la configuració de seguretat dels sistemes.

c) Establir les mesures de seguretat, adequades i eficaces per complir els requisits de seguretat establerts pels Responsables del Servei i de la Informació, seguint en tot moment el que exigeix l'Annex II de l'ENS, declarant l'aplicabilitat de les mesures esmentades.

d) Promoure les activitats de conscienciació i formació en matèria de seguretat al seu àmbit de responsabilitat.

e) Realitzar la coordinació i el seguiment de la implantació dels projectes d'adequació a l'Esquema Nacional de Seguretat, en col·laboració amb el Responsable de Sistemes.

f) Realitzar amb la col·laboració del Responsable del Sistema, les preceptives anàlisis de riscos, de seleccionar les salvaguardes a implantar i de revisar el procés de gestió del risc. Així mateix, juntament amb el Responsable del Sistema, podrà acceptar els riscos residuals calculats en l'anàlisi de riscos quan el Responsable de la Informació i el Responsable del Servei hi hagin delegat aquesta tasca.

g) Promoure auditories periòdiques per verificar el compliment de les obligacions en matèria de seguretat de la informació i analitzar els informes d'auditoria, elaborant les conclusions que cal presentar al Responsable del Sistema, als Responsables del Servei i als Responsables de la Informació perquè adoptin les mesures correctores adequades.

h) Coordinar el procés de Gestió de la Seguretat, en col·laboració amb el Responsable de Sistemes.

i) Signar la Declaració d'Aplicabilitat, que comprèn la relació de mesures de seguretat seleccionades per a un sistema (art. 28 i Annex II.2 de l'ENS).

j) Elaborar informes periòdics de seguretat que incloguin els incidents més rellevants a cada període, en coordinació amb el Responsable de Sistemes.

AJUNTAMENT DE SANT JOAN DESPÍ

k) Determinar la categoria del sistema segons el procediment descrit a l'Annex I de l'ENS i les mesures de seguretat que s'han d'aplicar d'acord amb allò previst a l'Annex II de l'ENS.

l) Verificar que les mesures de seguretat són adequades per a la protecció de la informació i els serveis.

m) Preparar els temes a tractar a les reunions del Comitè de Seguretat, en coordinació amb el Responsable del Sistema, aportant informació puntual per a la presa de decisions.

n) Responsable de l'execució directa o delegada de les decisions del Comitè de Seguretat.

o) Col·laborar estretament amb el Delegat de Protecció de Dades en relació amb les obligacions i disposicions del Reglament General de Protecció de Dades i la LOPDGDD.

p) Participar en l'elaboració de la Política de Seguretat de la Informació, en el marc del Comitè de Seguretat de la Informació, per aprovar-la per l'òrgan competent.

q) Facilitar periòdicament al Comitè 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 a què està exposat el sistema).

r) Elaborar, juntament amb el Responsable de Sistema, Plans de Millora de la Seguretat, per aprovar-lo pel Comitè de Seguretat de la Informació.

s) Validar els Plans de Continuïtat de Sistemes que elabori el Responsable de Sistemes, que hauran de ser aprovats pel Comitè de Seguretat de la Informació i provats periòdicament pel Responsable de Sistemes.

t) Aprovar les directrius proposades pel Responsable de Sistemes per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis.

En cas d'ocurrència d'incidents de seguretat de la informació:

- Analitzarà i proposarà salvaguardes que previnguin incidents semblants en un futur.

Compatibilitat amb altres Rols

Aquest rol només pot coincidir amb la del Responsable de Servei i el Responsable d'Informació en organitzacions de dimensions reduïdes que tinguin una estructura autònoma de funcionament.

Aquest rol no podrà coincidir amb el de Responsable de Sistema, encara que es tracti d'organitzacions de reduïdes dimensions que tinguin una estructura autònoma de funcionament.

Delegació de Funcions del Responsable de la Seguretat de la Informació

Per a determinats Sistemes d'Informació que, per la seva complexitat, distribució, separació física dels seus elements o nombre d'usuaris que es necessiti personal addicional per dur a terme les funcions de Responsable de la Seguretat, es podran designar els Responsables de Seguretat Delegats que es considerin necessaris.

La designació correspon al Responsable de la Seguretat. Per mitjà de la designació de delegats, es deleguen funcions.

Els Responsables de Seguretat Delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegui el Responsable de la Seguretat, i pot ser, per exemple, la seguretat de sistemes d'informació concrets o de sistemes d'informació horitzontals.

Cada Responsable de Seguretat Delegat tindrà una dependència funcional directa del Responsable de la Seguretat, que és qui reporten.

Pel que fa a la documentació, i recolzant-se en el Responsable del Sistema, són funcions del Responsable de Seguretat:

a) Proposar al Comitè de Seguretat per a la seva aprovació la documentació de seguretat de segon nivell (Normes de Seguretat TIC i Procediments Generals del Sistema de Gestió de la Seguretat de la Informació –SGSI–) i signar aquesta documentació.

b) Aprovar la documentació de seguretat de tercer nivell i signar aquesta documentació.

c) Mantenir la documentació organitzada i actualitzada, gestionant-ne els mecanismes d'accés.

Per al desenvolupament de qualsevol de les seves funcions, el Responsable de Seguretat podrà demanar la col·laboració del Responsable del Sistema.

6.5 Responsable del Sistema

Aquesta responsabilitat serà assumida pel Responsable del Departament de Sistemes d'Informació qui podrà demanar ajut de suport tècnic segons les necessitats. Aquest responsable no depèn jurídicament de la persona definida com a Responsable de Seguretat.

Seran funcions del Responsable del Sistema les següents:

a) Desenvolupar, operar i mantenir el sistema d'informació durant tot el cicle de vida, de les especificacions, instal·lació i verificació del funcionament correcte.

b) Definir la topologia i el sistema de gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en aquest.

c) Assegureu-vos que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.

d) Realitzar exercicis i proves sobre els procediments operatius de seguretat i els plans de continuïtat existents.

e) Seguiment del cicle de vida dels sistemes: especificació, arquitectura, desenvolupament, operació, canvis.

f) Implantar les mesures necessàries per garantir la seguretat del sistema durant tot el cicle de vida, d'acord amb el Responsable de Seguretat.

g) Aprovar qualsevol modificació substancial de la configuració de qualsevol element del sistema.

h) Suspendre el maneig d'una determinada informació o la prestació d'un servei electrònic si és informat de deficiències greus de seguretat, amb l'acord previ amb el Responsable d'aquesta informació o servei i amb el Responsable de Seguretat.

i) Realitzar amb la col·laboració del Responsable de Seguretat, les preceptives anàlisis de riscos, de seleccionar les salvaguardes a implantar i de revisar el procés de gestió del risc. Així mateix, juntament amb el Responsable de Seguretat, podrà acceptar els riscos residuals calculats en l'anàlisi de riscos quan el Responsable de la Informació i el Responsable del Servei hi hagin delegat aquesta tasca.

j) Elaborar en col·laboració amb el Responsable de Seguretat, la documentació de seguretat de tercer nivell.

k) Monitoritzar l'estat de la seguretat del Sistema d'Informació i reportar-lo periòdicament o davant d'incidents de seguretat rellevants al Responsable de Seguretat.

l) Elaborar els Plans de Continuïtat del Sistema perquè siguin validats pel Responsable de Seguretat i coordinats i aprovats pel Comitè de Seguretat de la Informació.

m) Realitzar exercicis i proves periòdiques dels Plans de Continuïtat del Sistema per mantenir-los actualitzats i verificar que són efectius.

n) Elaborar les directrius per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i els processos (especificació, arquitectura, desenvolupament, operació i canvis) i facilitar-les al Responsable de Seguretat per a la seva aprovació.

En cas d'ocurrència d'incidents de seguretat de la informació:

a) Planificar la implantació de les salvaguardes al sistema.

b) Executar el pla de seguretat aprovat.

Compatibilitat amb altres rols

Aquest rol no podrà coincidir amb el de Responsable d'Informació, amb el de Responsable de Servei ni amb el de Responsable de Seguretat.

6.6 Administrador de sistemes

Es designaran com a Administradors de la Seguretat del Sistema als tècnics informàtics amb aquesta funció, que podran recórrer a suport extern segons les necessitats per a la implementació de treballs a l'ENS, al qual, com a tal, li corresponen les funcions següents:

a) La implementació, la gestió i el manteniment de les mesures de seguretat aplicables al Sistema d'Informació.

b) Assegurar que els controls de seguretat establerts són estrictament complerts.

c) Assegurar que la traçabilitat, les pistes d'auditoria i altres registres de seguretat requerits estiguin habilitats i registrin amb la freqüència desitjada, d'acord amb la política de seguretat establerta per l'organització.

d) Aplicar als sistemes, usuaris i altres actius i recursos relacionats amb aquest, tant interns com externs, els procediments operatius de seguretat i els mecanismes i serveis de seguretat requerits.

e) Assegurar que són aplicats els procediments aprovats per manejar el sistema d'informació i els mecanismes i serveis de seguretat requerits.

f) La gestió, configuració i actualització, si escau, del maquinari i programari en què es basen els mecanismes i els serveis de seguretat del Sistema d'Informació.

g) Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa.

h) Aprovar els canvis a la configuració vigent del Sistema d'Informació, garantint que segueixin operatius els mecanismes i serveis de seguretat habilitats.

i) Informar els Responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.

j) Monitoritzar l'estat de seguretat del sistema.

k) En cas d'ocurrència d'incidents de seguretat de la informació:

- Dur a terme el registre, la comptabilitat i la gestió dels incidents de seguretat en els sistemes sota la seva responsabilitat.
- Executar el pla de seguretat aprovat.
- Aïllar l'incident per evitar la propagació a elements aliens a la situació de risc.
- Prendre decisions a curt termini si la informació s'ha vist compromesa de manera que pogués tenir conseqüències greus (aquestes actuacions haurien d'estar reflectides en un procediment documentat per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Assegurar la integritat dels elements crítics del Sistema si se n'ha vist afectada la disponibilitat (aquestes actuacions haurien d'estar reflectides en un procediment documentat per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Mantenir i recuperar la informació emmagatzemada pel sistema i els seus serveis associats.
- Investigar l'incident: determinar la manera, els mitjans, els motius i l'origen de l'incident.

6.7 Delegat de Protecció de Dades

Seguint el que indica el RGPD i la LOPDGDD, el Delegat de Protecció de Dades tindrà com a mínim les funcions següents:

AJUNTAMENT DE SANT JOAN DESPÍ

a) Assessorar i supervisar el compliment de principis relatius al tractament, com ara els de limitació de finalitat, minimització o exactitud de les dades.

b) Assessorar i supervisar que s'han definit terminis de conservació per a les dades i que hi ha i s'apliquen procediments correctes per a la seva destrucció quan correspongui.

c) Supervisar que els tractaments disposen de bases jurídiques o legitimació

d) Assessorar sobre la compatibilitat de finalitats diferents de les que van originar la recollida inicial de les dades.

e) Assessorar sobre l'existència de normativa sectorial que pugui determinar condicions de tractament específiques diferents de les establertes per la normativa general de protecció de dades.

f) Assessorar i supervisar el disseny i la implantació de mesures d'informació als afectats pels tractaments de dades (clàusules).

g) Assessorar i supervisar que hi ha mecanismes de recepció i gestió de les sol·licituds d'exercici de drets per part dels interessats.

h) Supervisar les sol·licituds d'exercici de drets per part dels interessats.

i) Supervisar la diligència en la contractació d'encarregats de tractament, inclòs el contingut dels contractes o actes jurídics que regulin la relació responsable-encarregat.

j) Assessorar i supervisar sobre els instruments de transferència internacional de dades adequades a les necessitats i característiques de l'organització i de les raons que justifiquin la transferència.

k) Assessorar i supervisar el disseny i la implantació de polítiques de protecció de dades.

l) Revisar els controls i auditories de seguretat i protecció de dades i reportar conclusions a la direcció.

m) Supervisar la primera versió dels registres d'activitats de tractament, així com els canvis que s'hi facin.

n) Assessorar i supervisar els supòsits de necessitat de realització d'avaluacions d'impacte sobre la protecció de dades.

o) Assessorar, revisar i validar les anàlisis de risc i les avaluacions d'impacte fetes.
p) Assessorar i supervisar la implantació de les mesures de protecció de dades des del disseny i protecció de dades per defecte adequades als riscos i naturalesa dels tractaments.

q) Assessorar i supervisar en la implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments.

r) Supervisar els procediments de gestió de violacions de seguretat de les dades, inclosa l'avaluació del risc per als drets i les llibertats dels afectats i els procediments de notificació a les autoritats de supervisió i als afectats.

s) Comunicar les violacions de seguretat a les autoritats i interessats quan calgui.

t) Assessorar i supervisar els supòsits de necessitat de realització d'avaluacions d'impacte sobre la protecció de dades.

u) Supervisar les avaluacions d'impacte sobre la protecció de dades.

v) Mantenir les relacions amb les autoritats de supervisió.

w) Mantenir el contacte amb els interessats.

x) Assessorar i supervisar en el disseny de programes de formació, conscienciació i sensibilització d'usuaris.

y) Reportar periòdicament a la Junta de Govern sobre l'estat de compliment en la matèria i les accions que calgui emprendre, així com reportar davant d'incidències i circumstàncies que es produeixin puntualment.

El delegat de protecció de dades està nomenat formalment i comunicat a l'Agència Espanyola de Protecció de Dades, i els ciutadans poden comunicar-se al correu **dpd@sjdespi.net**.

7 Procediments de designació

La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants i la designació del Responsable de Seguretat i del Responsable del Sistemes seran proposats i aprovats per l'alcalde/ssa o regidor/a delegat/da de Sistemes d'Informació de l'Ajuntament de Sant Joan Despí.

El nomenament es revisarà cada 2 anys o quan el lloc quedi vacant.

Es designen les següents responsabilitats:

- **Responsable d'informació:** L'Alcalde/ssa o regidor/a delegat/da de Sistemes d'Informació.
- **Responsables del Servei:** L'Alcalde/ssa o regidor/a delegat/da de Sistemes d'Informació.
- **Responsable de Seguretat**: Responsable Municipal d'Atenció a la Ciutadania
- **Responsable del Sistema**: Responsable del dept. de Sistemes d'Informació
- **Administrador del Sistema:** Tècnics informàtics amb aquesta funció
- **Delegat de Protecció de dades**: Figura designada com a tal

- **Assessor Jurídic**: Tècnic jurídic que se li assigni aquesta funció.

8 Revisió de la política de seguretat de la informació

Serà missió del Comitè de Seguretat de la Informació (CSI) la revisió biennal d'aquesta Política de Seguretat de la Informació i la proposta de modificació o manteniment de la mateixa. La Política serà validada per aquest, aprovada per l'òrgan competent i difosa perquè la coneguin totes les parts afectades.

Aquesta Política es desenvoluparà per mitjà de normativa de seguretat que tracti aspectes específics.

La normativa de seguretat estarà disponible a la intranet de l'organisme.

9 Dades de caràcter personal

Per a la prestació dels serveis previstos cal tractar dades de caràcter personal. El Registre d'Activitats del Tractament detalla els tractaments afectats i els responsables corresponents, així com les mesures adoptades derivades de les avaluacions d'impacte realitzades sobre els tractaments.

Tots els sistemes d'informació s'ajustaran als nivells de seguretat requerits per la normativa per la naturalesa i finalitat de les dades de caràcter personal recollides a l'esmentat Registre d'Activitats del Tractament.

En tot cas, caldrà atendre als principis regulats a l'article 5 RGPD, que es consideren autèntiques obligacions per a aquesta entitat.

9.1 Figures vinculades a la protecció de dades de caràcter personal

9.1.1 Responsable del Tractament

El Responsable del Tractament és la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideix sobre la finalitat, contingut i ús del tractament.

A aquests efectes s'ha atribuït la condició de Responsable de Tractament a la persona juridicopública, és a dir, al mateix Ajuntament de Sant Joan Despí. De manera que, s'ha entès que l'Ajuntament de Sant Joan Despí és responsable del tractament de les dades de caràcter personal que obren als seus sistemes d'informació, i que deriven de la prestació dels serveis públics atribuïts a nivell de competències. Val a dir que la consideració de Responsable de Tractament no ha de ser associada a persona física representant de l'Ajuntament de Sant Joan Despí, en qualitat del càrrec o lloc (com, per exemple, l'Alcalde/ssa o Secretari/a).

Les funcions del Responsable del Tractament són, principalment:

AJUNTAMENT DE SANT JOAN DESPÍ

a) Adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat.

b) Informar als titulars de les dades els drets que els assisteixen i en els termes en què els poden exercir.

c) Excloure del tractament les dades relatives a l'afectat que s'oposi al tractament.

d) Cessar en la utilització o cessió il·lícita de les dades quan així ho requereixi l'interessat.

e) Obligació de fer efectiu el dret de rectificació o supressió de l'interessat en el termini màxim d'un mes.

f) Notificar les rectificacions o cancel·lacions efectuades a les dades personals a qui s'hagi comunicat aquestes dades, en el cas que es mantingui el tractament per aquest últim, que també haurà de procedir a la cancel·lació.

9.1.2 Delegat de Protecció de dades

El Delegat de Protecció de Dades (DPD) pot ser intern o extern a l'organització, i també pot revestir la forma d'un òrgan col·legiat (Comitè Delegat de Protecció de Dades), vetllant sempre per evitar conflicte d'interessos en qualsevol dels seus membres. A més d'això, es pot designar un únic DPD per a diverses autoritats o organismes públics, tenint en consideració la seva estructura i mida.

El Delegat de Protecció de Dades a l'entitat serà una persona externa a l'organització i designada per l'empresa que resulti adjudicatària del servei de conformitat amb el procediment de contractació pública segons la legislació vigent.

Per a qualsevol comunicació es realitzarà mitjançant el correu electrònic:**dpd@sjdespi.net**

Les funcions associades són:

a) Informar i assessorar al responsable o l'encarregat del tractament i els empleats que s'ocupin del tractament de les obligacions que els incumbeixen en virtut del present Reglament i d'altres disposicions de protecció de dades de la Unió o dels Estats membres.

b) Supervisar el compliment del que disposa aquest Reglament, d'altres disposicions de protecció de dades de la Unió o dels Estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats , la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.

c) Oferir l'assessorament que se us demani sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació de conformitat amb l'article 35.

d) Cooperar amb l'autoritat de control.

AJUNTAMENT DE SANT JOAN DESPÍ

e) Actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia a què fa referència l'article 36, i fer consultes, si escau, sobre qualsevol altre assumpte.

El delegat de protecció de dades exerceix les seves funcions prestant la deguda atenció als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i els fins del tractament. Per això **haurà de ser capaç** de:

a) Recollir informació per determinar les activitats de tractament.

b) Analitzar i comprovar la conformitat de les activitats de tractament.

c) Informar, assessorar i emetre recomanacions al responsable o encarregat del tractament.

d) Recollir informació per supervisar el registre de les operacions de tractament.

e) Assessorar en l'aplicació del principi de la protecció de dades per disseny i per defecte.

f) Assessorar sobre:

- Si heu de dur a terme o no una avaluació d'impacte de la protecció de dades.
- Quina metodologia s'ha de seguir en fer una avaluació d'impacte de la protecció de dades.
- Si cal dur a terme l'avaluació d'impacte de la protecció de dades amb recursos propis o amb contractació externa.
- Quines salvaguardes (incloses les mesures tècniques i organitzatives) aplicar per mitigar qualsevol risc per als drets d'interessos dels afectats.
- Si heu dut a terme correctament o no l'avaluació d'impacte de la protecció de dades.
- Si les vostres conclusions (si seguir endavant o no amb el tractament i quines salvaguardes aplicar) són conformes al Reglament.

g) Prioritzar les seves activitats i centrar els seus esforços en aquelles qüestions que presentin més riscos relacionats amb la protecció de dades.

h) Assessorar el responsable del tractament sobre:

- Que metodologia emprar en dur a terme una avaluació d'impacte de la protecció de dades.
- Quines àrees s'han de sotmetre a auditoria de protecció de dades interna o externa.
- Quines activitats de formació internes proporcionar al personal o als directors responsables de les activitats de tractament de dades i a què operacions de tractament dedicar més temps i recursos.

AJUNTAMENT DE SANT JOAN DESPÍ

El DPD haurà de reunir coneixements especialitzats del dret i la pràctica en matèria de protecció de dades. S'han identificat, en conseqüència, aquells **coneixements, habilitats o destreses** necessàries que ha de saber o posseir el Delegat de Protecció de Dades per dur a terme una de les funcions pròpies del seu lloc.

Aquestes funcions genèriques del DPD es poden concretar en tasques d'assessorament i supervisió, entre d'altres, a les àrees següents:

a) Compliment de principis relatius al tractament, com ara els de limitació de finalitat, minimització o exactitud de les dades.

b) Identificació de les bases jurídiques dels tractaments.

c) Valoració de compatibilitat de finalitats diferents de les que van originar la recollida inicial de les dades.

d) Determinació de l'existència de normativa sectorial que pugui determinar condicions de tractament específiques diferents de les establertes per la normativa general de protecció de dades.

e) Disseny i implantació de mesures d'informació als afectats pels tractaments de dades.

f) Establiment de mecanismes de recepció i gestió de les sol·licituds d'exercici de drets per part dels interessats.

g) Valoració de les sol·licituds d'exercici de drets per part dels interessats.

h) Contractació d'encarregats de tractament, inclòs el contingut dels contractes o actes jurídics que regulin la relació responsable-encarregat.

i) Identificació dels instruments de transferència internacional de dades adequades a les necessitats i les característiques de l'organització i de les raons que justifiquin la transferència.

j) Disseny i implantació de polítiques de protecció de dades.

k) Auditoria de protecció de dades.

l) Establiment i gestió dels registres d'activitats de tractament.

m) Anàlisi de riscos dels tractaments realitzats.

n) Implantació de les mesures de protecció de dades des del disseny i protecció de dades per defecte adequades als riscos i naturalesa dels tractaments.

o) Implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments.

p) Establiment de procediments de gestió de violacions de seguretat de les dades, inclosa l'avaluació del risc per als drets i les llibertats dels afectats i els procediments de notificació a les autoritats de supervisió i als afectats.

q) Determinació de la necessitat de fer avaluacions d'impacte sobre la protecció de dades.

r) Realització d'avaluacions d'impacte sobre la protecció de dades.

s) Relacions amb les autoritats de supervisió.

t) Implantació de programes de formació i sensibilització del personal en matèria de protecció de dades.

9.1.3 Funcions i obligacions d'usuaris amb accés a dades

Tots els empleats de l'entitat estan subjectes a funcions i obligacions que es defineixin en aquest sentit.

Tot el personal de l'entitat que disposi d'accés a les dades de caràcter personal ha de complir les obligacions generals següents:

a) No es permet la difusió de dades de caràcter personal ni confidencial pertanyent a l'entitat, estant obligat a guardar secret de la informació fins i tot acabada la relació laboral.

b) L'usuari es responsabilitzarà de notificar tota incidència segons el procediment de gestió d'incidències. No notificar una incidència serà considerada una omissió del deure del treballador.

c) L'usuari es responsabilitzarà de tots els accessos que es facin sota el vostre identificador i contrasenya, per tant, no haureu de revelar la contrasenya.

d) No es permet la còpia de dades de caràcter personal, en suports, sense l'autorització expressa del delegat de protecció de dades.

e) De totes maneres, conforme referit, cada usuari dels sistemes d'informació de l'entitat haurà de respectar les normatives que estiguin vigents i aprovades a cada moment.

9.1.4 Funcions i obligacions de l'encarregat del tractament

El **apartat 8 de l'article 4 del RGPD** defineix l'Encarregat de Tractament com a <<*la persona física o jurídica, autoritat pública, servei o un altre organisme que tracti dades personals per compte del responsable del tractament*>>.

L'encarregat del tractament ha d'aplicar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat.

Igualment, haurà d'implementar les mesures de seguretat a què es refereix el paràgraf anterior i que apareixeran estipulades al contracte amb el Responsable del Tractament.

En concret, les seves funcions són les de:

a) Tractar les dades del tractament.

b) Realitzar el control de tractament, qualitat i seguretat de les dades.

c) Controlar la forma i els requisits per procedir a les addicions i cancel·lacions.

AJUNTAMENT DE SANT JOAN DESPÍ

d) Controlar els suports de seguretat.

e) Control i accés de contrasenyes.

f) Manteniment del registre d'incidències.

g) Crear una llista per a les situacions en què un afectat no vulgui que les dades personals s'emmagatzemin en el tractament.

h) Traslladar al responsable del tractament d'aquelles sol· licituds d'exercici de dret que es rebin per part dels interessats.

En conseqüència, l'Ajuntament de Sant Joan Despí haurà de dur a terme un document actualitzat on s'identificaran els Encarregats de Tractament que estan prestant serveis a l'entitat, així com la indicació de la formalització del contracte pertinent amb aquests prestadors de serveis amb accés a dades .

10 Gestió de riscos

Per a tots els sistemes subjectes a aquesta Política de Seguretat de la Informació s'ha de fer periòdicament una avaluació dels riscos a què estan exposats. Aquesta anàlisi es repetirà:

- Regularment almenys una vegada a l'any.
- Quan canvieu la informació gestionada.
- Quan canviïn els serveis prestats.
- Quan es produeixi un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

La gestió de riscos s'ha de fer de manera contínua sobre els sistemes d'informació, d'acord amb els principis de gestió de la seguretat basada en els riscos (article 7 de l'ENS) i la reavaluació periòdica (article 10 de l'ENS).

El Responsable de Seguretat juntament amb el Responsable de Sistemes, són els encarregats de realitzar les preceptives anàlisis de riscos, i de seleccionar les salvaguardes a implantar.

El Responsable de la Informació i el del Servei són els responsables dels riscos sobre la informació i sobre el servei, respectivament, i per tant d'acceptar els riscos residuals calculats en l'anàlisi i de fer-ne el seguiment i control sense perjudici de la possibilitat de delegar aquesta tasca.

El procés de gestió de riscos, que comprèn les fases de categorització dels sistemes, anàlisis de riscos i selecció de mesures de seguretat a aplicar, que hauran de ser proporcionals als riscos i estar justificades, s'haurà de revisar cada any per part del Responsable de Seguretat amb la col·laboració del Responsable del Sistema, que elevaran un informe al Comitè Seguretat de la Informació.

AJUNTAMENT DE SANT JOAN DESPÍ

11 Desenvolupament de la política de seguretat de la informació. Documentació de Seguretat

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

Les normes i procediments contemplaran, almenys, els aspectes següents:

a) Protecció de dades de caràcter personal: s'han d'implantar mesures tècniques i organitzatives que permetin complir els requisits normatius en aquesta matèria.

b) Gestió d'actius d'informació: els actius d'informació estaran inventariats, categoritzats i estaran associats a un responsable.

c) Seguretat lligada als recursos humans: la seguretat lligada al personal és fonamental per reduir els riscos d'errors humans, robatoris, fraus o mal ús de les instal·lacions i serveis, per a la qual cosa s'implantaran els mecanismes que permetin als usuaris conèixer les seves responsabilitats i com complir-les.

d) Seguretat física: les instal·lacions de l'Ajuntament de Sant Joan Despí mantindran una seguretat física correcta per evitar els accessos no autoritzats així com qualsevol altre tipus de dany o interferència externa.

e) Seguretat lògica: s'estableixen mesures organitzatives i tècniques per al control d'accessos, la protecció davant de codis nocius, la seguretat de les comunicacions, la realització de còpies de seguretat, etc.

f) Gestió d'incidents de seguretat: s'establiran responsabilitats i procediments de gestió d'incidències per assegurar una resposta ràpida, eficaç i endreçada als esdeveniments en matèria de seguretat.

El cos normatiu sobre seguretat de la informació serà de compliment obligat i es desenvoluparà en quatre nivells segons l'àmbit d'aplicació i nivell de detall tècnic, de manera que cada norma d'un determinat nivell de desenvolupament es fonamenti en les normes de nivell superior. Aquests nivells de desenvolupament normatiu són els següents:

a) Primer nivell normatiu: Política de seguretat de la informació de l'Ajuntament de Sant Joan Despí. Document de compliment obligat per tot el personal, intern i extern, recollit en aquest document.

b) Segon nivell normatiu: Polítiques Específiques de Seguretat de la Informació i Normes de Seguretat TIC, que desenvolupen amb més grau de detall la PSI dins d'un àmbit determinat. Les Normes donen resposta, sense entrar en detalls d'implementació ni tecnològics, a què es pot fer i què no en relació amb un cert tema des del punt de vista de la seguretat: què es considera un ús apropiat o inapropiat, les conseqüències derivades del incompliment, entre altres aspectes.

AJUNTAMENT DE SANT JOAN DESPÍ

També pertanyen a aquest nivell la documentació de Procediments Generals del Sistema de Gestió de la Seguretat de la Informació (SGSI) que implementa, manté i millora de manera continuada el SGSI. Els documents relatius a aquest segon nivell normatiu seran aprovats per Comitè de Seguretat a proposta del Responsable de Seguretat.

c) Tercer nivell normatiu: Procediments Operatius i Instruccions Tècniques. Són documents que donen resposta, incloent detalls d'implementació i tecnològics, a com es pot realitzar una determinada tasca respectant els principis de seguretat de l'organització, i els processos interns que s'hi estableixen. Procediments STIC i Instruccions Tècniques STIC seran aprovats pel Responsable de Seguretat i amb la participació en la seva elaboració del Responsable del Sistema.

d) Quart Nivell: Informes, registres i evidències electròniques. Documents de caràcter tècnic que poden estar suportats en formats normalitzats que arrepleguen el resultat i les conclusions d'un estudi, una activitat o una valoració; documents de caràcter tècnic que recullen amenaces i vulnerabilitats dels sistemes d'informació, així com també evidències electròniques generades durant totes les fases del cicle de vida del sistema d'informació. La responsabilitat que hi hagi aquest tipus de documents és del Responsable del Sistema.

A banda dels documents sol·licitats al punt anterior, la documentació de seguretat del sistema podrà comptar, sota criteri del Responsable de Seguretat, amb altres documents de caràcter no vinculant: recomanacions, bones pràctiques, informes, etc.

El Responsable de Seguretat i el Responsable del Sistema seran responsables de mantenir la documentació de seguretat actualitzada i organitzada i de gestionar-ne els mecanismes d'accés, així com de garantir que tots els usuaris interns del sistema d'informació la coneixen.

12 Formació i conscienciació

Tots els membres de l'Ajuntament de Sant Joan Despí tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, i és responsabilitat del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi als afectats.

Tots els membres de l'Ajuntament de Sant Joan Despí assistiran a una sessió de conscienciació en matèria de seguretat com a mínim una vegada a l'any. S'establirà un programa de conscienciació continuada per atendre tots els membres de l'Ajuntament de Sant Joan Despí, en particular 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 que la necessitin per fer la feina. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

AJUNTAMENT DE SANT JOAN DESPÍ

13 Incompliment

L'incompliment de la present Política de Seguretat de la Informació pot comportar l'inici de les mesures disciplinàries que siguin procedents, sense perjudici de les responsabilitats legals corresponents.

14 Terceres parts

Les empreses i organitzacions externes que, en ocasió de la col·laboració amb l'Ajuntament de Sant Joan Despí per a la prestació d'un servei, accedeixin o gestionin actius d'informació de l'Ajuntament de Sant Joan Despí o dels seus usuaris, directament o indirectament (en sistemes propis o aliens), comparteixen la responsabilitat de mantenir la seguretat dels sistemes i actius de l'Ajuntament de Sant Joan Despí, per la qual cosa hauran d'assumir les obligacions següents:

a) No difondre cap informació relativa als serveis proporcionats a l'Ajuntament de Sant Joan Despí sense autorització expressa.

b) Informar i difondre al personal les obligacions establertes en aquesta Política.

c) Aplicar les mesures estipulades per RGPD al tractament de les dades personals responsabilitat de l'Ajuntament de Sant Joan Despí que tractin per raó de la prestació del servei.

d) Aplicar els procediments per a la gestió de seguretat relacionats amb els serveis proporcionats a l'Ajuntament de Sant Joan Despí. Especialment s'han d'aplicar els procediments relacionats amb la gestió d'usuaris, com ara notificacions d'altes i baixes, identificació dels usuaris, gestió de contrasenyes, etc., en el sentit descrit en aquesta política i normativa reguladora que sigui aplicable.

e) Notificar qualsevol incidència o sospita d'amenaça a la seguretat d'algun sistema o actiu de l'Ajuntament de Sant Joan Despí a través dels mecanismes que es determinin, col·laborant en la resolució relacionada amb els sistemes, serveis o personal de la pròpia entitat.

f) Implantar mesures als seus propis sistemes i xarxes per prevenir la difusió de virus i/o codi maliciós als sistemes de l'Ajuntament de Sant Joan Despí. Específicament qualsevol equip connectat a la xarxa corporativa de l'Ajuntament de Sant Joan Despí ha de disposar d'un antivirus actualitzat preferiblement de forma automàtica.

g) Implantar mesures als seus propis sistemes i xarxes per prevenir l'accés no autoritzat als sistemes de l'Ajuntament de Sant Joan Despí des d'altres xarxes. Entre altres, s'han d'aplicar les actualitzacions de seguretat als seus sistemes i s'ha de mantenir un sistema tallafoc per protegir les connexions des d'Internet i altres xarxes no fiables.

L'Ajuntament de Sant Joan Despí es reserva el dret de revisar la relació amb l'entitat externa en cas d'incompliment de les obligacions anteriors.

L'Ajuntament de Sant Joan Despí s'encarregarà de posar a disposició d'aquests la Política de Seguretat de l'entitat, així com les normes o procediments que els afectin, enviant-los aquesta informació als contactes que constin als proveïdors.

AJUNTAMENT DE
SANT JOAN DESPÍ