REGLAMENT DE SEGURETAT DE LA INFORMACIÓ DE L'AJUNTAMENT DE PICANYA (TIC02)

Aprovació 19-7-2018
Publicació: BOP núm 212 de 5-11-2018
Entrada en vigor 5-11-2018

Exposició de motius

L'Ajuntament de Picanya va esdevenir en una Administració Electrònica a l'any 2008 a la empara de normes que promovien dita transformació, que posteriorment es va disposar com a preceptiva, de tal manera que l'actualment vigent Llei 39/2015, d'1 d'octubre, de Procediment Administratiu Comú de les Administracions Públiques no preveu altra cosa que un procediment i una documentació electròniques.

Això suposa el reconeixement del caràcter estratègic de la informació i els sistemes que la suporten, de la necessitat d'un marc de gestió de la seua seguretat.

Ja la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics va establir la necessitat de l'Esquema Nacional de Seguretat que, aprovat mitjançant Reial Decret 3/2010, de 8 de gener, té per objecte determinar la política de seguretat en la utilització de mitjans electrònics en el seu àmbit d'aplicació i estarà constituït pels principis bàsics i requisits mínims que permeten una protecció adequada de la informació. Posteriorment, la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic, arreplega l'Esquema Nacional de Seguretat en el seu article 156 apartat 2 en similars termes.

En 2015 es va publicar la modificació de l'Esquema Nacional de Seguretat (ENS), aprovada pel Reial Decret 951/2015, de 23 d'octubre, en resposta a l'evolució de l'entorn normatiu, especialment de la Unió Europea, de les tecnologies de la informació i de l'experiència de la implantació de l'Esquema.

Per a la seua aplicació cal una específica organització, amb uns concrets objectius, que son el objecte del present Reglament, arrel per al preceptiu desenvolupament en forma de Polítiques de Seguretat.

Per altre costat, encara sense transposició legislativa estatal, ha entrat en aplicació el passat 25 de maig de 2018, el Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques respecte al tractament de dades personals i a la lliure circulació d'eixes dades, que deroga la Directiva 95/46/CE (Reglament General de Protecció de Dades).

El Reglament de referència disposa la necessitat de comptar amb un Delegat de Protecció de Dades, que s'ha d'inserir dins d'eixa organització de l'ENS. La normativa de protecció de dades s'haurà d'implementar des de l'entramat organitzatiu i procedimental de l'ENS, com una especialitat material d'unes determinades dades.

Per tot allò, exercint la potestat d'autoregulació de l'Administració Municipal, es dicta el present Reglament de Seguretat de la Informació:

Article 1. Objecte i àmbit d'aplicació

1. Constitueix l'objecte del present Reglament de Seguretat de la Informació, d'ara endavant RSI, l'articulació de les condicions generals de seguretat en l'àmbit de l'Ajuntament de

Picanya, així com del marc organitzatiu i tecnològic de la mateixa, amb la finalitat d'asseure les bases per a establir els mecanismes normatius i procedimentals necessaris per a fer de la gestió de la seguretat una activitat continuada, al mateix nivell que les altres activitats que constitueixen el normal funcionament de l'Ajuntament, i com a base per a una execució fiable d'aquestes, tant a nivell intern com per a la ciutadania.

2. El RSI serà d'obligat compliment per a tots els òrgans administratius de l'Ajuntament de Picanya, qualssevol organismes públics i entitats de dret públic vinculats al mateix o dependents d'ell i les entitats de dret privat vinculades a aquest o dependents del mateix, que quedaran subjectes al que es disposa en les normes del RSI que específicament es referisquen a elles, i, en tot cas, quan exercisquen potestats administratives, sent aplicable als actius emprats per l'Ajuntament en la prestació dels serveis de l'Administració Electrònica.

3. El RSI serà d'obligat compliment per a tot el personal que accedisca tant als sistemes d'informació com a la pròpia informació que siga gestionada per l'Ajuntament i les seues entitats vinculades o dependents, amb independència de quin siga la seua destinació, adscripció o relació amb el mateix.

Article 2. Marc legal i regulador.

El marc normatiu en què es desenvolupen les activitats de l'Ajuntament de Picanya i les seues entitats vinculades o dependents en l'àmbit de la prestació dels serveis electrònics als ciutadans, sense perjudici de la legislació específica, així com de la normativa que en un moment donat pot substituir a la que seguidament es detalla, es compon de:

a) Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, especialment per:
   a. Art. 17.3: els mitjans o suports en què s'emmagatzemen documents hauran de comptar amb les mesures de seguretat que estableix l'Esquema Nacional de Seguretat, que garantisquen una sèrie de principis com a integritat, autenticitat, confidencialitat, qualitat, protecció i conservació dels documents emmagatzemats.
   b. Art. 27.3: les Administracions Públiques hauran de complir amb l'Esquema Nacional de Seguretat per a garantir la identitat i contingut de les còpies electròniques o en paper, és a dir, el caràcter de còpies autèntiques.
   c. Disposició Addicional segona: les Comunitats Autònomes, com les Entitats Locals, hauran de garantir la seua compatibilitat informàtica i interconnexió, així com la transmissió telemàtica de les sol·licituds, escrits i comunicacions que es realitzen en els seus corresponents registres i plataformes mitjançant el compliment, igualment, de l'Esquema Nacional de Seguretat.

b) La Llei 5/2013, de 23 de desembre, de Mesures Fiscals, de Gestió Administrativa i Financera, i d'Organització de la Generalitat. [2013/12400], que deroga la Llei 3/2010, de 5 de maig, de la Generalitat, d'Administració Electrònica de la Comunitat Valenciana, que estableix en el seu art. 117.2.2.p) la prestació de serveis de seguretat tècnics i administratius, en les comunicacions a través de tècniques electròniques, informàtiques i telemàtiques de l'Institut Valencià de Finances.

c) Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en a l'àmbit de l'Administració Electrònica.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org |

d) Reial Decret 951/2015, de 23 d'octubre, de modificació del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.

e) Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en a l'àmbit de l'Administració Electrònica.

f) Llei Orgànica 15/1999 de desembre, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

g) Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

h) Llei 59/2003, de 19 de desembre, de signatura electrònica.

i) Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.

j) Llei 40/2015, d'1 d'octubre, del Règim Jurídic del Sector Públic.

k) 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).

De la mateixa manera, formen part del marc regulador les normes aplicables a l'Administració Electrònica de l'Ajuntament de Picanya que desenvolupen o complementen les anteriors en l'ús de la seua potestat d'autoregulació i que es troben dins de l'àmbit d'aplicació del la RSI, tal com es defineixen en l'article 13 del mateix; així com la normativa comunitària en la matèria.

Article 3. Principis de la seguretat de la informació.

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

   a) Abast estratègic: La seguretat de la informació ha de comptar amb el compromís i suport de tots els nivells amb capacitat de presa de decisions, de manera que puga estar coordinada i integrada amb la resta d'iniciatives estratègiques de l'Ajuntament per a conformar un tot coherent i eficaç.
   b) Responsabilitat diferenciada: En els sistemes d'informació es diferenciarà el Responsable de la Informació, que proposa els requisits de seguretat de la informació tractada; els Responsables del Servei, que compleixen i fan complir els requisits de seguretat en els sistemes i serveis de la seua competència; els Responsables del Sistema, que tenen la responsabilitat sobre la seguretat física i lògica i la prestació dels serveis en els àmbits de competència que es determinen en el present RSI; i el Responsable de Seguretat, que determina les decisions per a satisfer els requisits de seguretat. El Comitè de Seguretat de la Informació serveix de vincle entre tots ells, amb les funcions que es codifiquen en el present RSI.
   c) Seguretat integral: La seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb el sistema, evitant, excepte casos d'urgència o necessitat, qualsevol actuació puntual o tractament

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

d) Gestió de riscos: L'anàlisi i gestió de riscos serà part essencial del procés de seguretat. La gestió de riscos permetrà el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells es realitzarà mitjançant el desplegament de mesures de seguretat, que establirà un equilibri entre la naturalesa de les dades i els tractaments, l'impacte i la probabilitat dels riscos als quals estiguen exposats i l'eficàcia i el cost de les mesures de seguretat.
e) Proporcionalitat: L'establiment de mesures de protecció, detecció i recuperació haurà de ser proporcional als potencials riscos i a la criticitat i el valor de la informació i dels serveis afectats.
f) Millora contínua: Les mesures de seguretat es revaluaran i actualitzaran periòdicament per a adequar la seua eficàcia a la constant evolució dels riscos i sistemes de protecció. La seguretat de la informació serà atesa, revisada i auditada per personal qualificat, instruït i dedicat, amb la periodicitat que determine el Comitè de Seguretat de la Informació (d'ara endavant CSI).
g) Seguretat per defecte: Els sistemes han de dissenyar-se i configurar-se de manera que garantisquen un grau suficient de seguretat per defecte, atenent a l'Esquema Nacional de Seguretat (d'ara endavant ENS).

2. Les directrius fonamentals de seguretat es concreten en un conjunt de principis particulars i responsabilitats específiques, que es configuren com a objectius instrumentals que garanteixen el compliment dels principis bàsics del RSI i que inspiren les actuacions de l'Ajuntament de Picanya en aquesta matèria. S'estableixen els següents:

a) Protecció de dades de caràcter personal: S'adoptaran les mesures tècniques i organitzatives destinades a garantir el nivell de seguretat exigit per la normativa vigent en relació amb el tractament de les dades de caràcter personal, de manera coherent amb el Document de Seguretat exigit per l'article 88 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
b) Gestió d'actius d'informació: Els actius d'informació de l'Ajuntament es trobaran inventariats i categoritzats i estaran associats almenys a un responsable tècnic.
c) Seguretat lligada a les persones: S'implantaran els mecanismes necessaris perquè qualsevol persona que accedisca, o puga accedir als actius d'informació, conega les seues responsabilitats i d'aquesta manera es reduïsca el risc derivat d'un ús indegut de dites actives.
d) Seguretat física: Els actius d'informació seran emplaçats en àrees segures, protegides per controls d'accés físics adequats al seu nivell de criticitat. Els sistemes i els actius d'informació que contenen aquestes àrees estaran suficientment protegits enfront d'amenaces físiques o ambientals. En el supòsit de fer ús de sistemes o serveis en modalitat Cloud, haurà d'existir un acord de nivell de servei (SLA) que establisca idèntic grau de seguretat física i atenga a les recomanacions del Centre Criptològic Nacional en les seues Guies CCN-STIC.
e) Seguretat en la gestió de comunicacions i operacions: S'establiran els procediments necessaris per a aconseguir una adequada gestió de la seguretat, operació i actualització de les tecnologies de la informació i de les comunicacions. La informació que es transmeta a través de xarxes de comunicacions haurà de ser adequadament protegida, tenint en compte el seu nivell de sensibilitat i de criticitat, mitjançant mecanismes que garantisquen la seua seguretat. Les tècniques de xifrat o encriptació han de ser prou fiables com per a garantir la seguretat en les comunicacions i operacions, però de cap manera comprometre la usabilitat futura dels actius d'informació.
f) Control d'accés: Es limitarà l'accés als actius d'informació per part d'usuaris, processos i altres sistemes d'informació mitjançant la implantació dels mecanismes d'identificació,

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

g) Adquisició, desenvolupament i manteniment dels sistemes d'informació: Es contemplaran els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, garantint la seua seguretat per defecte. Per això s'estarà al que es disposa en la restant normativa municipal reguladora de tots els aspectes associats a l'Administració Electrònica, en particular a les disposicions de l'Ordenança Municipal d'Administració Electrònica i la seua normativa de desenvolupament.
h) Gestió dels incidents de seguretat: S'implantaran els mecanismes apropiats per a la correcta identificació, registre i resolució dels incidents de seguretat. En tot cas, es proporcionarà informació a, i s'atendran les recomanacions de, els Sistemes d'Alerta Primerenca del Centre Criptològic Nacional.
i) Gestió de la continuïtat: S'implantaran els mecanismes apropiats per a assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels processos de l'Ajuntament i les seues entitats vinculades o dependents, d'acord amb les necessitats de nivell de servei dels seus usuaris.
j) Compliment: S'adoptaran les mesures tècniques, organitzatives i procedimentals necessàries per al compliment de la normativa legal vigent en matèria de seguretat de la informació.

Article 4. Estructura organitzativa.

L'estructura organitzativa per a la gestió de la seguretat de la informació en l'àmbit descrit pel RSI de l'Ajuntament de Picanya i de les seues entitats vinculades o depenents està composta pels següents agents:

a) Responsable de la Informació.
b) Responsable del Servei.
c) Delegat de Protecció de Dades.
d) Responsable de Seguretat de la Informació.
e) Responsable del Sistema.
f) Administrador de la Seguretat del Sistema.
g) Responsable de Seguretat Física.
h) Responsable de Gestió de Personal.
i) Comitè de Seguretat de la Informació.

Article 5. Responsable de la Informació.

El Responsable de la Informació és el responsable últim de qualsevol error o negligència que porte a un incident de confidencialitat o d'integritat. Té la responsabilitat última de l'ús que es faça d'una certa informació i, per tant, de la seua protecció.

Es designa Responsable de la Informació a l'Alcaldia-Presidència o òrgan en qui delegue, a qui li correspon les següents funcions:

a) Adoptar les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat dels tractaments de 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 provinguen de l'acció humana o del mitjà físic o natural.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org |

b) Establir els requisits de la informació en matèria de seguretat mitjançant l'aprovació formal dels nivells de seguretat de la informació, a proposta del Responsable de la Seguretat i previ informe del Responsable del Sistema.

c) Determinar els nivells de seguretat en cada dimensió dins del marc establert en l'Annex I de l'Esquema Nacional de Seguretat.

Article 6. Responsable del Servei.

El Responsable del Servei és el responsable últim de qualsevol error o negligència que porte a un incident de disponibilitat dels serveis. Té la responsabilitat última de l'ús que es faça de determinats serveis i, per tant, de la seua protecció.

Es designen responsables del servei a cadascun dels responsables d'unitats funcionals amb serveis en la seu electrònica (Caps d'àrea i de servei), als qui els correspon les següents funcions:

a) Ser el Gestor de Fitxers Concrets, en terminologia de protecció de dades de caràcter personal, quan se li encomana el desenvolupament de les tasques relacionades amb la gestió dels fitxers i tractaments de dades personals que es realitzen en la seua àrea en concret, per delegació del Responsable del tractament, d'acord amb el RGPD.
b) Establir 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.

c) Determinar els nivells de seguretat en cada dimensió del servei dins del marc establert en l'Annex I de l'Esquema Nacional de Seguretat, a proposta del Responsable de la Seguretat i previ informe del Responsable del Sistema.
La prestació d'un servei sempre ha d'atendre als requisits de seguretat de la informació que utilitza, de manera que poden heretar-se els requisits de seguretat de la mateixa, afegint requisits de disponibilitat, així com uns altres com a accessibilitat, interoperabilitat, etc.

Article 7. Delegat de protecció de Dades.

El rol del Delegat en Protecció de Dades, és una figura requerida en la secció 4 del RGPD, i segons l'article 39 del RGPD les seues funcions són les següents:

1. Informar i assessorar al responsable, a l'encarregat i empleats.

2. Supervisar el compliment incloent assignació de responsabilitats, conscienciació i formació personal.

3. Assessorar sobre l'avaluació d'impacte i supervisar la seua aplicació.

4. Cooperar amb l'autoritat de control.

5. Actuar com a punt de contacte en qüestions relatives al tractament de les dades, incloent les consultes prèvies.

Les anteriors funcions, han sigut concretades per l'Agència Espanyola de Protecció de Dades, tant en relació amb les Administracions Públiques, com en general, en l'Esquema de Certificació i es detallen a continuació:

a) Complir els principis relatius al tractament, com els de limitació de finalitat, minimització o exactitud de les dades.
b) Identificar les bases jurídiques dels tractaments.

c) Valorar la compatibilitat de finalitats diferents de les quals van originar la recollida inicial de les dades.
d) Complir l'eventual normativa sectorial que puga determinar condicions de tractament específiques, diferents de les establides per la normativa general de protecció de dades.
e) Dissenyar i implantar mesures d'informació als afectats pels tractaments de dades.
f) Establir mecanismes de recepció i gestió de les sol·licituds d'exercici de drets per part dels interessats.
g) Valorar les sol·licituds d'exercici de drets per part dels interessats.
h) Regular la relació entre el responsable de tractament i eventuals encarregats de tractament.

i) Identificar els instruments de transferència internacional de dades adequades a les necessitats i característiques de l'organització i de les raons que justifiquen la transferència.
j) Dissenyar i implantar polítiques de protecció de dades.
k) Auditar la protecció de dades.
l) Establir i gestionar els registres d'activitats de tractament.
m) Analitzar el risc dels tractaments realitzats.
n) Implantar les mesures de protecció de dades des del disseny i protecció de dades per defecte, adequades als riscos i naturalesa dels tractaments.
o) Implantar les mesures de seguretat adequades als riscos i naturalesa dels tractaments.
p) Establir procediments de gestió de violacions de seguretat de les dades, inclosa l'avaluació del risc per als drets i llibertats dels afectats i els procediments de notificació a les autoritats de supervisió i als afectats.
q) Determinar la necessitat de realització d'avaluacions d'impacte sobre la protecció de dades.
r) Realitzar avaluacions d'impacte sobre la protecció de dades.
s) Ser l'interlocutor en les relacions amb les autoritats de supervisió.
t) Implantar programes de formació i sensibilització del personal en matèria de protecció de dades.

El seu nomenament es farà d'acord amb la seua normativa segons siga més convenient en cada moment.

Article 8. Responsable de Seguretat de la Informació.

Es designa com a Responsable de Seguretat de la Informació a la Prefectura del Servei Municipal d'Informàtica, a qui li correspondran les següents funcions:

a) Coordinar i controlar les mesures definides en el Registre d'activitats del tractament i, en general, encarregar-se del compliment de les mesures de seguretat que detalla l'informe d'avaluació d'impacte en la protecció de dades.

b) Reportar directament al Comitè de Seguretat de la Informació.

c) Actuar com a Secretari del Comitè de Seguretat de la Informació. Per la Secretaria del Comitè de Seguretat de la Informació li correspon:

   a. Convocar les reunions del Comitè de Seguretat de la Informació.
   b. Preparar els temes a tractar en les reunions del Comitè, aportant informació puntual per a la presa de decisions.
   c. Elaborar l'acta de les reunions.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org | APP mòbils

d. Executar, directament o per delegació, les decisions del Comitè.

d) Mantenir la seguretat de la informació utilitzada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb la Política de Seguretat de l'Organització.

e) Promoure la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.

f) Recopilar els requisits de seguretat dels Responsables d'Informació i Servei i determinarà la categoria del Sistema.

g) Realitzar l'Anàlisi de Riscos.

h) Elaborar una Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides conforme a l'Annex II de l'ENS i del resultat de l'Anàlisi de Riscos.

i) Facilitar als Responsable 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'ENS.

j) Coordinar l'elaboració de la Documentació de Seguretat del Sistema.

k) Participar en l'elaboració, en el marc del Comitè de Seguretat de la Informació, de la Política de Seguretat de la Informació.

l) Participar en l'elaboració i aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de Seguretat de la Informació.

m) Elaborar i aprovar els Procediments Operatius de Seguretat de la Informació.

n) 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 al que està exposat el sistema.

o) Elaborar, al costat dels Responsables de Sistemes, Plans de Millora de la Seguretat, per a la seua aprovació pel Comitè de Seguretat de la Informació.

p) Elaborar els Plans de Formació i Conscienciació del personal en Seguretat de la Informació, que hauran de ser aprovats pel Comitè de Seguretat de la Informació.

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

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

Article 9. Responsable del Sistema.

Es designa com a responsable del Sistema al Tècnic Informàtic Municipal de Sistemes, al que li corresponen les següents funcions:

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

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

c) Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.

d) Acordar eventualment la suspensió de l'ús d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que pogueren afectar a la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els Responsables de la Informació afectada, del Servei afectat i amb el Responsable de la Seguretat abans de ser executada.

e) Aplicar els procediments operatius de seguretat elaborats i aprovats pel Responsable de Seguretat.

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

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

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

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

Article 10. Administrador de la Seguretat del Sistema.

Es designa com a Administrador de la Seguretat del Sistema al Tècnic Informàtic Municipal de Sistemes, al que, com a tal, li corresponen les següents funcions:

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

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

c) Assegurar que la traçabilitat, pistes d'auditoria i altres registres de seguretat requerits es troben habilitats i registren amb la freqüència desitjada, d'acord amb la política de seguretat establida per l'Organització.

d) Aplicar als Sistemes, usuaris i altres actius i recursos relacionats amb el mateix, tant interns com a externs, els Procediments Operatius de Seguretat i els mecanismes i serveis de seguretat requerits.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org | APP mòbils

e) Assegurar que són aplicats els procediments aprovats per a 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 els quals es basen els mecanismes i serveis de seguretat del Sistema d'Informació.

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

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

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

j) Monitoritzar l'estat de la seguretat del sistema.

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

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

Article 11. Responsable de Seguretat Física.

Es designa com a Responsable de Seguretat Física a la Direcció d'Àrea de Seguretat Ciutadana i Protecció Civil, al que li correspondrà implantar les mesures de seguretat de la seua competència, dins de les determinades pel responsable de la Seguretat de la Informació, i informarà a aquest del seu grau d'implantació, eficàcia i incidents.

Article 12. Responsable de Gestió de Personal.

Es designa com a responsable de Gestió de Personal a la Sotssecretària, a la que li correspon implantar les mesures de seguretat de la seua competència dins de les determinades pel Responsable de Seguretat de la Informació, i informarà a aquest del seu grau d'implantació, eficàcia i incidents.

Article 13. Comitè de Seguretat de la Informació.

Es crea el Comitè de Seguretat de la Informació que estarà compost pels següents membres:

PRESIDENT: Alcalde o regidor en qui delegue.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org | APP mòbils

SECRETARI: Cap de l'Àrea de Sistemes de la informació com a Responsable de Seguretat del Sistema.

VOCALS:

- Responsable del Sistema i Administrador de la Seguretat del Sistema.
- La persona titular de la Secretaria General o funcionari en qui delegue.
- La persona titular de la Direcció d'Àrea de Serveis a les Persones o funcionari en qui delegue.
- La persona titular de la Direcció d'Àrea de Serveis Econòmics i Financers o funcionari en qui delegue.
- La persona titular de la Direcció d'Àrea de Seguretat Ciutadana i Protecció Civil o funcionari en qui delegue.
- Responsable de Gestió de Personal.

Podran acudir a requeriment del Comitè qualssevol altres Caps de Servei o Àrea i responsables la intervenció de les quals siga precisa per ser afectats per l'Esquema Nacional de Seguretat i pel RGPD.

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

a) Atendre les inquietuds de l'Alta Direcció i dels diferents departaments.
b) Informar regularment de l'estat de la seguretat de la informació a l'Alta Direcció.
c) Promoure la millora contínua del Sistema de Gestió de la Seguretat de la Informació.
d) Elaborar l'estratègia d'evolució de l'Ajuntament pel que fa a la seguretat de la informació.
e) 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.
f) Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè siga aprovada per la Direcció.
g) Aprovar la normativa de seguretat de la informació.
h) Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
i) Monitoritzar els principals riscos residuals assumits per l'Ajuntament i recomanar possibles actuacions respecte d'ells.
j) Monitoritzar 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.
k) Promoure la realització de les auditories periòdiques que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
l) Aprovar plans de millora de la seguretat de la informació de l'Ajuntament. En particular, vetlarà per la coordinació de diferents plans que puguen realitzar-se en diferents àrees.
m) 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 recolzen un funcionament homogeni de tots els sistemes TIC.
n) Resoldre els conflictes de responsabilitat que puguen aparèixer entre els diferents responsables i/o entre diferents àrees de l'Organització, elevant aquells casos en els quals no tinga suficient autoritat per a decidir.
o) Recaptarà regularment del personal tècnic propi o extern, la informació pertinent per a prendre decisions.
p) S'assessorarà dels temes que haja de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, podent materialitzar-se de diferents formes i maneres:

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

q) Aprovar, en cas d'ocurrència d'incidents de seguretat de la informació, el Pla de Millora de la Seguretat, amb la seua dotació pressupostària corresponent.

Article 13. Grups de treball.

El CSI podrà articular la creació de grups de treball per a la realització d'activitats tals com a estudis, treballs i informes, que s'estimen convenients.

Article 14. Gestió dels riscos.

1. La gestió de riscos ha de realitzar-se de manera contínua sobre els sistemes d'informació i contemplar una anàlisi de riscos avançat que avalue els riscos residuals i propose tractaments adequats.

2. El CSI s'encarregarà d'adoptar les mesures oportunes per a analitzar i avaluar els riscos de funcionament dels serveis a fi d'establir les corresponents mesures preventives.

3. Per a la realització de l'anàlisi de riscos es tindran en compte les recomanacions publicades per a l'àmbit de l'Administració Pública i especialment les guies elaborades pel Centre Criptològic Nacional, així com metodologies reconegudes en ús a nivell nacional i internacional.

Article 15. Estructura normativa.

El cos normatiu sobre seguretat de la informació és d'obligat compliment i s'estructura en els següents nivells relacionats jeràrquicament:

a) Primer nivell normatiu: El present RSI i les directrius generals de seguretat aplicables als òrgans de l'Ajuntament i a les seues entitats vinculades o dependents als quals siga aplicable el present RSI

b) Segon nivell normatiu: Les normes de seguretat desenvolupades pel Responsable de Seguretat. Aquestes normes de seguretat hauran de:
    1. Limitar-se única i exclusivament a l'àmbit específic de les competències de l'Ajuntament i de les seues entitats vinculades o depenents. Aquest àmbit vindrà determinat pels sistemes d'informació i serveis de tecnologies de la informació i de les comunicacions que siguen prestats i gestionats directament per cada òrgan o entitat vinculada o depenent.

    2. Complir estrictament amb l'indicat en l'ENS i amb el primer nivell normatiu enunciat en el present article.

    3. Ser informades pel CSI i aprovades mitjançant acord de la Junta de Govern Local.

c) Tercer nivell normatiu: Procediments, guies i instruccions tècniques. Són documents que, complint amb l'exposat en el RSI, determinen les accions o tasques a realitzar en l'acompliment d'un procés. Aquest tercer nivell normatiu haurà de:

1. Limitar-se única i exclusivament a l'àmbit específic de les competències de l'Ajuntament i de les seues entitats vinculades o depenents. Aquest àmbit vindrà determinat pels sistemes d'informació i serveis de tecnologies de la informació i de les comunicacions que siguen prestats i gestionats directament per cada òrgan o entitat vinculada o depenent.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org | APP mòbils

2. Complir estrictament amb l'indicat en l'ENS i amb el primer i segon nivell normatius enunciats en el present article.

3. Ser informat pel CSI i aprovat mitjançant acord de la Junta de Govern Local.

A més de la normativa enunciada en el present article, l'estructura normativa podrà disposar, a criteri dels òrgans competents de l'Ajuntament, i sempre dins de l'àmbit de les seues competències i responsabilitats, altres documents normatius, en virtut de la potestat autoreguladora de l'Administració Municipal, i previ informe del CSI i aprovació mitjançant acord de la Junta de Govern Local. En qualsevol cas, sempre haurà de disposar-se, de conformitat amb el previst en l'article 88 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, de Document de Seguretat permanentment actualitzat.

D'acord amb l'ENS i a les Guies CCN-STIC del Centre Criptològic Nacional que el desenvolupen, el CSI determinarà les normes de diferent nivell a ser aprovades i l'ordre i prioritat de les mateixes.

El personal de cadascun dels òrgans de l'Ajuntament i les seues entitats vinculades o dependents tindrà l'obligació de conèixer i complir, a més del present RSI, i als nivells en què resulte de la seua responsabilitat, totes les directrius generals, normes i procediments de seguretat de la informació que puguen afectar a les seues funcions.

Article 16. Protecció de dades de caràcter personal.

Per a la prestació dels serveis previstos han de ser tractats 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 a la naturalesa i finalitat de les dades de caràcter personal recollits en l'esmentat Registre d'Activitats del Tractament.

El règim jurídic aplicable es composa de les següents normes o les eventuals substitutes:

a) Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

b) Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

c) Annex II del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.

d) El Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques 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).

Article 17. Formació i conscienciació.

1. El Responsable de Seguretat de la Informació desenvoluparà un pla bianual d'activitts formatives específiques orientades a la conscienciació i formació dels empleats públics de l'Ajuntament i de les seues entitats vinculades i dependents, així com a la difusió entre els mateixos del RSI i del seu desenvolupament normatiu.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org |

2. El Responsable de Seguretat de la Informació, en cooperació amb el Responsable de Gestió de Personal, s'encarregarà de promoure les activitats de formació i conscienciació en matèria de seguretat.

Article 16. Tercers.

Quan l'Ajuntament de Picanya utilitze serveis o informació de tercers, els farà partícips d'aquesta Política de Seguretat de la Informació. El Comité de Seguretat de la Informació establirà canals per a reporte i coordinació dels diferents serveis i establirà procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'Ajuntament de Picanya preste serveis a altres organismes, o informació a tercers, els farà partícips d'aquesta Política de Seguretat de la Informació i de les Instruccions i Procediments propis d'aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establides en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics de reporte i resolució d'incidències. S'exigirà que el personal de tercers estiga adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en la Política de Seguretat de la Informació municipal.

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 Responsable de Seguretat que precise els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir avant.

Disposició addicional única. Deure col·laboració en la implantació del RSI.

Tots els òrgans i unitats de l'Ajuntament i les seues entitats vinculades o dependents prestaran la seua col·laboració en les actuacions d'implantació del RSI.

Disposició final única. Modificació i publicitat del RSI i entrada en vigor.

1. El present RSI serà objecte d'aprovació i publicació d'acord amb els tràmits legals oortuns.

2. El present RSI es publicarà en la seu electrònica de l'Ajuntament i en el seu portal de transparència.

3. El present RSI entrarà en vigor en el termini de l'article 70.2 i 65 de la Llei 7/1985, de 2 d'abril, reguladora de les Bases del Règim Local, a partir de la seua publicació en el Butlletí Oficial.

Pl. Espanya,1 - 46210 | tel. 961 594 460 | www.picanya.org | ajuntament@picanya.org |