Secció III. Altres disposicions i actes administratius

CONSELL INSULAR DE MALLORCA
PLE, COMISSIÓ DE GOVERN, CONSELL EXECUTIU I PRESIDÈNCIA

10837 ***Aprovació del document de Política de Seguretat de la Informació***

El Consell Executiu del Consell Insular de Mallorca, dia 26 de setembre de 2018, ha aprovat el document de Política de Seguretat de la Informació que seguidament es transcriu:

«**Política de Seguretat de la Informació del Consell Insular de Mallorca**

Índex

1. Aprovació i entrada en vigor

Text aprovat el 26 de setembre de 2018 pel Consell Executiu del Consell Insular de Mallorca.

Aquesta política de seguretat de la informació és efectiva des de la data esmentada i fins que sigui reemplaçada per una política nova.

2. Introducció

El Consell Insular de Mallorca, en endavant el Consell, depèn dels sistemes de les tecnologies de la informació i la comunicació (TIC) per assolir els seus objectius.

Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los de danys accidentals o deliberats que puguin afectar la disponibilitat, la integritat o la confidencialitat de la informació tractada o els 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 rapidesa als incidents.

Els sistemes de les TIC han d'estar protegits contra amenaces d'evolució ràpida amb potencial per incidir en la confidencialitat, en la integritat, en la disponibilitat, en l'ús previst i en el valor de la informació i en els serveis. Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que els agents implicats 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 diferents agents implicats han de garantir que la seguretat de les TIC és una part integral de cada etapa del cicle de vida del sistema, des de la concepció del servei fins a la retirada, passant per les decisions de desenvolupament o d'adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament s'han d'identificar i incloure en la planificació i execució dels projectes de les TIC, tant si es fan amb recursos propis com externs.

La Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, estableix que les administracions públiques s'han de relacionar entre si i amb els seus òrgans, organismes públics i entitats vinculades o dependents a través de mitjans electrònics. Aquests mitjans han d'assegurar la interoperativitat i seguretat dels sistemes i de les solucions adoptades, han de garantir la protecció de les dades de caràcter personal i han de facilitar preferentment la prestació conjunta de serveis a les persones interessades. En aquest sentit, l'article 156 de l'esmentada Llei 40/2015, d'1 d'octubre, regula l'Esquema Nacional de Seguretat.

Per altra banda, la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, en l'article 13 reconeix una sèrie de drets de les persones en les seves relacions amb les administracions públiques. Entre aquests drets, es reconeix el dret relatiu a la protecció de dades de caràcter personal i, en particular, a la seguretat i confidencialitat de les dades que figurin en els fitxers, en els sistemes i en les aplicacions de les administracions públiques.

El Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, modificat parcialment pel Reial decret 951/2015, de 23 d'octubre, té per objecte determinar la política de seguretat en la utilització de mitjans electrònics en l'àmbit d'aplicació, els principis bàsics i els requisits mínims que permetin una protecció adequada de la informació.

L'article 11 de l'esmentat Reial decret 3/2010, de 8 de gener, exigeix que tots els òrgans superiors de les administracions públiques disposin formalment de la seva política de seguretat, que ha d'aprovar el titular de l'òrgan superior corresponent. Aquesta política de seguretat s'ha d'establir sobre la base dels principis bàsics recollits en el capítol II de la mateixa norma (seguretat integral, gestió de riscos, prevenció, reacció i recuperació, línies de defensa, reavaluació periòdica i funció diferenciada) i ha de desplegar una sèrie de requisits mínims consignats en l'article 11.1, que ja hem esmentat.

Els principis bàsics són directrius fonamentals de seguretat que s'han de tenir 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 directius, de manera que pugui estar coordinada i integrada amb la resta d'iniciatives estratègiques de l'organisme per conformar un tot coherent i eficaç.

b. Responsabilitat diferenciada: en els sistemes d'informació s'ha de diferenciar la persona responsable de la informació, que determina els requisits de seguretat de la informació tractada; la persona responsable del servei, que determina els requisits de seguretat dels serveis prestats; la persona responsable del sistema, que té la responsabilitat sobre la prestació dels serveis i la persona responsable de la seguretat, que determina les decisions per satisfer els requisits de seguretat.

c. Seguretat integral: la seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius relacionats amb el sistema, per evitar, llevat dels casos d'urgència o de necessitat, qualsevol actuació puntual o tractament conjuntural. La seguretat de la informació s'ha de considerar una part de l'operativa habitual, ha d'estar present i s'ha d'aplicar des del disseny inicial dels sistemes d'informació.

d. Gestió de riscos: l'anàlisi i la gestió de riscos és una part essencial del procés de seguretat. La gestió de riscos permet mantenir un entorn controlat i minimitzar els riscos fins a nivells acceptables. La reducció d'aquests nivells es fa mitjançant el desplegament de mesures de seguretat i s'estableix un equilibri entre la naturalesa de les dades i els tractaments, l'impacte i la probabilitat dels riscos a

què estiguin exposats i l'eficàcia i el cost de les mesures de seguretat. En avaluar el risc en relació amb la seguretat de les dades, s'han de tenir en compte els riscos que es deriven del tractament de les dades personals.

e. Proporcionalitat: l'establiment de mesures de protecció, detecció i recuperació ha de ser proporcional als riscos potencials, a la criticitat i al valor de la informació i dels serveis afectats.

f. Millora contínua: les mesures de seguretat s'han de reavaluar i actualitzar periòdicament per adequar-ne l'eficàcia a l'evolució constant dels riscos i dels sistemes de protecció. La seguretat de la informació ha de ser atesa, revisada i auditada per personal qualificat, instruït i dedicat.

g. Seguretat per defecte: els sistemes s'han de dissenyar i configurar de manera que garanteixin un grau suficient de seguretat per defecte.

3. Àmbit d'aplicació

Aquesta política de seguretat s'ha d'aplicar a tota la informació del Consell Insular de Mallorca.

4. Missió i objectius

El Consell reconeix com a actius estratègics la informació i els sistemes que la gestionen.

Un dels objectius fonamentals de la implantació d'aquesta política de seguretat és establir les bases perquè tant els empleats públics com la ciutadania puguin accedir als serveis públics en un entorn segur i de confiança.

La política de seguretat de la informació defineix el marc global per gestionar la seguretat de la informació, protegir tots els actius d'informació i garantir la continuïtat en el funcionament dels sistemes. Es pretén així minimitzar els riscos derivats d'una possible fallada en la seguretat i assegurar el compliment dels objectius del Consell davant un hipotètic incident de seguretat de la informació.

Per a això, s'estableixen els objectius generals en matèria de seguretat de la informació:

a. Contribuir des de la gestió de la seguretat a complir la missió i els objectius del Consell.

b. Disposar de les mesures de control necessàries per garantir que es compleixen els requisits legals que siguin aplicables com a conseqüència de l'activitat desenvolupada, especialment pel que fa a la protecció de dades de caràcter personal i a la prestació de serveis a través de mitjans electrònics o telemàtics.

c. Garantir la implantació de les mesures i dels mecanismes de seguretat apropiats per protegir els serveis prestats, els sistemes d'informació emprats per prestar-los i la informació processada, emmagatzemada o transmesa per aquests, de manera coherent amb els riscos afrontats.

d. Garantir l'eficàcia de les mesures de seguretat implantades per mitjà d'avaluacions i auditories.

e. Establir una estructura organitzativa adequada per gestionar la seguretat de la informació i definir els rols i els comitès necessaris, a més de les funcions i les responsabilitats respectives.

f. Garantir l'operació continuada i adequada dels serveis i dels sistemes, i actuar per prevenir, detectar, reaccionar i operar de manera oportuna davant els incidents de seguretat que es produeixin, a més de vetlar perquè s'implantin els mecanismes necessaris per assegurar la continuïtat de les activitats crítiques i permetre que es recuperin en un període de temps acceptable.

g. Impulsar i fomentar la formació, la conscienciació i el compliment de les obligacions en matèria de seguretat de la informació del personal al servei de l'organització, a fi de garantir el coneixement de les polítiques i de les normatives aprovades, i de les pràctiques recomanades, amb l'objectiu últim d'aconseguir que la seguretat de la informació es converteixi en un factor inherent al desenvolupament de les funcions i de les operatives quotidianes.

h. Promoure que les activitats destinades a aconseguir els nivells de seguretat requerits s'estructurin i es concebin com un procés de millora contínua, i no com a accions o esforços puntuals, i sustentar-ho en l'anàlisi i la gestió sistematitzades dels riscos.

i. Protegir els actius d'informació de l'administració del Consell i la tecnologia que els gestionen davant qualsevol amenaça, intencionada o accidental, interna o externa, per assegurar-ne la confidencialitat, la integritat, la disponibilitat, l'autenticitat i la traçabilitat.

Aquesta política de seguretat assegura un compromís continu i manifest del Consell per difondre i consolidar la cultura de la seguretat.

5. Marc normatiu

El disseny, l'operació, l'ús i l'administració de la informació, dels sistemes d'informació i dels serveis del Consell han de complir les normes següents, les quals s'esmenten amb caràcter enunciatiu i no limitador:

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

b. Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques

c. Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic

d. Llei 59/2003, de 19 de desembre, de signatura electrònica

e. Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica

f. Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica

g. Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999

h. Reglament 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)

i. Ordenança per la qual es regula l'Administració electrònica del Consell Insular de Mallorca i els organismes que en depenen (BOIB núm. 69, de 16 de maig de 2013)

6. Organització de la seguretat

L'estructura organitzativa per gestionar la seguretat de la informació en l'àmbit descrit per aquesta política de seguretat de la informació està formada pels agents següents:

a. Comitè de Seguretat de la Informació

b. Responsables de la informació

c. Responsables del servei

d. Responsable de la seguretat

e. Responsables del sistema

f. Delegat o delegada de la protecció de dades de caràcter personal

L'estructura organitzativa és competent per mantenir, actualitzar i fer complir, dins l'àmbit definit, la política de seguretat de la informació.

6.1 Comitè de Seguretat de la Informació

Composició i funcionament

Integren el Comitè de Seguretat de la Informació:

a) Presidència: el conseller executiu o la consellera executiva competent en matèria de tecnologies i sistemes d'informació

b) Vocalies:

- Les persones titulars de les secretaries tècniques de tots els departaments del Consell de Mallorca
- La persona titular de la Secretaria General
- La persona responsable de la seguretat
- El delegat o la delegada de la protecció de dades de caràcter personal

Així mateix formen part del Comitè com a vocals amb veu, però sense vot:

- Les persones responsables del sistema.

- Les persones que, en cada cas, proposi la Presidència, en qualitat d'assessors.

El Comitè de Seguretat de la Informació pot consultar al personal tècnic, propi o extern, la informació pertinent per prendre decisions.

El Comitè s'ha de reunir amb caràcter ordinari almanco una vegada a l'any i, amb caràcter extraordinari, en els supòsits següents:

a. A instància de la Presidència.

b. Quan hi hagi incidències de seguretat greus o sorgeixin necessitats de seguretat noves que requereixin la participació dels components del Comitè.

Perquè el Ple del Comitè es pugui constituir de manera vàlida i fer sessions, deliberar i prendre acords es requerirà, en primera convocatòria, la presència del president o presidenta, del secretari o secretària i de la meitat més un dels membres.

El Ple ha d'adoptar els acords per majoria dels membres presents amb dret a vot.

El funcionament del Comitè s'ha d'ajustar al que preveu la Llei 40/2015.

Funcions

Al Comitè de Seguretat de la Informació li corresponen funcions d'assessorament, de consultoria i de proposta en matèria de seguretat de la informació.

En particular, li correspon:

a. Informar regularment de l'estat de la seguretat de la informació als òrgans superiors corresponents.

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

c. Elaborar i revisar la política de seguretat de la informació perquè els òrgans superiors corresponents l'aprovin.

d. Impulsar el compliment de la política de seguretat de la informació i el seu desplegament normatiu.

e. Aprovar la normativa de seguretat de la informació a proposta de la persona responsable de la seguretat.

f. Aprovar els procediments d'actuació en relació amb la seguretat dels serveis de les TIC.

g. Aprovar el pla d'auditoria i el pla de formació proposats per la persona responsable de la seguretat.

h. Proposar plans de millora de la seguretat de la informació de l'organització.

i. Vetlar perquè la seguretat de la informació es tengui en compte en tots els projectes de tecnologies de la informació en totes les fases: a l'hora de redactar l'especificació inicial, en el moment de la posada en marxa i en el manteniment posterior, així com a l'hora de preservar la informació que sigui requerida una vegada que s'ha deixat d'utilitzar. En particular, ha de vetlar per crear i utilitzar serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes de les TIC.

j. Divulgar la política de seguretat de la informació i les normatives i instruccions de seguretat de la informació aprovades, amb la promoció d'activitats de conscienciació i formació en matèria de seguretat per al personal.

k. Monitorar els principals riscos residuals assumits per l'organització i recomanar possibles actuacions sobre aquests riscos.

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

6.2 Responsables de la informació

La persona responsable de la informació és la que té la competència suficient per decidir sobre la finalitat, el contingut i l'ús d'aquesta informació, i de determinar dins el marc establert en l'Annex I 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, els requisits de seguretat de la informació tractada.

La persona designada ha de figurar en la documentació de seguretat del sistema d'informació.

Funcions

a. Establir els requisits, en matèria de seguretat, de la informació que manegen. Si aquesta informació inclou dades de caràcter personal, a més s'han de tenir en compte les mesures de seguretat que correspongui implantar, atesos els riscos generats pel tractament d'acord al que exigeix el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016.

b. Fer, juntament amb les persones responsables del servei i de la responsable de la seguretat, les anàlisis de riscos preceptives i seleccionar les salvaguardes que s'han d'implantar.

c. Acceptar els riscos residuals respecte de la informació calculats en l'anàlisi de riscos.

d. Fer el seguiment i control dels riscos, amb la participació de la persona responsable de la seguretat.

e. Suspendre, d'acord amb la persona responsable del servei i amb la responsable de seguretat, la prestació d'un servei electrònic o el maneig d'una determinada informació, si és informat de deficiències greus de seguretat.

6.3 Responsables del servei

La persona responsable del servei és la persona amb competència suficient per decidir sobre la finalitat i prestació d'aquest servei i ha de determinar dins el marc establert en l'Annex I 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, els requisits de seguretat dels serveis prestats.

La persona designada ha de figurar en la documentació de seguretat del sistema d'informació.

Funcions

a. Establir els requisits, en matèria de seguretat, dels serveis. Si aquests serveis inclouen dades de caràcter personal, a més, s'han de tenir en compte les mesures de seguretat que correspongui implantar, atesos els riscos generats pel tractament d'acord al que exigeix el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016.

b. Fer, juntament amb els responsables de la informació i de la seguretat, les anàlisis de riscos preceptives.

c. Acceptar els riscos residuals respecte de la informació calculats en l'anàlisi de riscos.

d. Fer el seguiment i control dels riscos, amb la participació de la persona responsable de la seguretat.

e. Suspendre, d'acord amb la persona responsable de la informació i amb la de la seguretat, la prestació d'un servei electrònic o el maneig d'una determinada informació, si és informat de deficiències greus de seguretat.

6.4 Responsable de la seguretat

La persona responsable de la seguretat l'ha de designar la persona titular del departament amb competències en matèria de seguretat de les tecnologies de la informació i la comunicació entre el personal adscrit a aquest departament.

La persona designada ha de figurar en la documentació de seguretat del sistema d'informació.

Funcions

Són funcions de la persona responsable de la seguretat:

a. Actuar com a secretari o secretària del Comitè de Seguretat de la Informació.

b. Estar al corrent dels canvis de la tecnologia i de l'entorn en què viu l'organització, informar-se de les conseqüències per a les activitats de seguretat de la informació, alertar el Comitè de Seguretat de la Informació i proposar les mesures oportunes d'adequació.

c. Presentar regularment informes sobre l'estat de seguretat dels serveis de les TIC al Comitè de Seguretat de la Informació.

d. Elaborar l'anàlisi de riscos dels sistemes de les TIC i presentar-la al Comitè de Seguretat de la Informació perquè l'aprovi. Aquesta anàlisi s'ha d'actualitzar regularment.

e. Executar regularment verificacions de seguretat segons un pla que el Comitè de Seguretat de la Informació ha predeterminat i aprovat. Els resultats d'aquestes inspeccions s'han de presentar al Comitè de Seguretat de la Informació perquè els conegui i els aprovi. Si, com a resultat de la inspecció, apareixen incompliments, la persona responsable de la seguretat ha de proposar mesures correctores que ha de presentar al Comitè de Seguretat de la Informació perquè les aprovi.

f. Elaborar el pla de seguretat i fer-ne el seguiment. Aquest pla s'ha de presentar al Comitè de Seguretat de la Informació perquè l'aprovi.

g. Promoure el desplegament del marc normatiu en matèria de seguretat.

h. Elaborar perquè el Comitè de Seguretat de la Informació els aprovi els requisits de formació i qualificació de persones administradores, operadores i usuàries des del punt de vista de seguretat de les TIC.

i. Preparar els informes pertinents en cas d'incidents excepcionalment greus i en cas de desastres. Se n'ha de presentar un informe detallat al Comitè de Seguretat de la Informació.

j. Coordinar la resposta en cas d'incidents que desbordin els casos previstos i procedimentats. És la persona responsable de coordinar la investigació forense relacionada amb incidents que es considerin rellevants.

k. Proposar a les persones responsables de la informació la determinació dels nivells de seguretat en cada dimensió de seguretat sempre que se li sol·liciti.

l. Proposar a les persones responsables del servei la determinació dels nivells de seguretat en cada dimensió de seguretat sempre que se li sol·liciti.

m. Mantenir la documentació de seguretat organitzada i actualitzada i gestionar els mecanismes per accedir-hi.

n. Promoure la millora contínua en la gestió de la seguretat de la informació.

o. Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de la seguretat i pels mecanismes d'auditoria implementats en el sistema.

p. Proposar la categoria del sistema segons el procediment descrit en l'annex I del Reial decret 3/2010, de 8 de gener, i les mesures de seguretat que s'han d'aplicar d'acord amb el que preveu l'annex II del mateix Reial decret.

q. Assumir les funcions explícitament atribuïdes a la figura de responsable de seguretat en el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat.

6.5 Responsables del sistema

Les persones responsables del sistema les ha de designar la persona titular del departament amb competències en matèria de les tecnologies de la informació i la comunicació entre el personal adscrit a aquest departament.

Les persones designades han de figurar en la documentació de seguretat del sistema d'informació.

Funcions

a. Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, així com encarregar-se de les especificacions, de la instal·lació i de la verificació que funciona correctament.

b. Definir la topologia i el sistema de gestió del sistema d'informació, i establir-ne els criteris d'ús i els serveis disponibles.

c. Assegurar que les mesures específiques de seguretat s'integrin adequadament dins el marc general de seguretat.

d. Acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei, si la persona responsable del sistema és informada de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió s'ha d'acordar amb les persones responsables de la informació afectada, del servei afectat i amb la persona responsable de la seguretat, abans d'executar-la.

e. Elaborar els plans de millora de la seguretat juntament amb la persona responsable de la informació.

f. Planificar la implantació de salvaguardes en els sistemes.

g. Executar els plans de seguretat aprovats.

6.6 Delegat o delegada de protecció de dades

El delegat o la delegada de protecció de dades és únic per a tots els òrgans i organismes del Consell Insular de Mallorca i se n'ha d'informar del nomenament i cessament a l'Agència Espanyola de Protecció de Dades.

Les funcions del delegat o de la delegada de protecció de dades són les que s'indiquen en el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, i en altres disposicions reguladores de la matèria.

La persona designada ha de figurar en la documentació de seguretat del sistema d'informació.

6.7 Resolució de conflictes

En cas de conflicte entre les diferents persones responsables que componen l'estructura organitzativa de la política de seguretat de la informació, la Presidència del Comitè és l'encarregada de resoldre'l i han de prevaldre les exigències més altes derivades de la protecció de dades de caràcter personal. Els casos en què no tengui prou autoritat per decidir, els ha d'elevar.

7. Dades de caràcter personal

Pel que fa a les dades de caràcter personal que tracta el Consell, s'han d'adoptar les mesures tècniques i organitzatives que correspongui implantar, atesos els riscos generats pel tractament un cop feta l'avaluació exigida per l'article 24.1 del Reglament (UE) 2016/679.

En cas de conflicte entre les diferents persones responsables han de prevaldre les exigències més altes derivades de la protecció de dades de caràcter personal.

8. Gestió de riscos

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 i en l'avaluació periòdica. La persona responsable del servei s'ha d'encarregar que es faci l'anàlisi preceptiva de riscos i que es proposi el tractament adequat, calculant els riscos residuals.

La persona responsable de la seguretat, dins el seu àmbit d'actuació, és l'encarregada de recomanar un marc de directrius bàsiques per harmonitzar els criteris a seguir per valorar els riscos.

Les persones responsables de la informació i del servei són les propietàries dels riscos sobre la informació i sobre els serveis, respectivament, i en són responsables del 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, anàlisi de riscos i selecció de mesures de seguretat a aplicar, que han de ser proporcionals als riscos i han d'estar justificades; s'ha de revisar i s'ha d'aprovar cada any per la persona titular de l'òrgan o de la unitat administrativa o, si escau, de l'organisme autònom, a través d'un pla d'adequació a l'Esquema Nacional de Seguretat.

Les fases indicades del procés de gestió de riscos s'han de fer segons el que disposen els annexos I i II del Reial decret 3/2010, de 8 de gener, i seguint les normes, instruccions, guies CCN-STIC i recomanacions per a l'aplicació elaborades pel Centre Criptològic Nacional, així com tota la informació referent a l'anàlisi de risc i d'impacte en la protecció de dades especificada en l'esmentat Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril del 2016.

Encara que es necessita un control continu dels canvis fets en els sistemes, aquesta anàlisi s'ha de repetir:

a. Almanco una vegada a l'any (mitjançant una revisió i una aprovació formal).

b. Quan canviï la informació manejada.

c. Quan canviïn els serveis prestats.

d. Quan hi hagi un incident greu de seguretat.

e. Quan es reportin vulnerabilitats greus.

9. Desplegament de la política de seguretat de la informació

El marc normatiu de la política de seguretat de la informació s'ha d'estructurar en els nivells següents:

a. Aquesta política de seguretat de la informació ha d'establir els requisits i criteris de protecció de caràcter global.

b. Les normes de seguretat han de definir què cal protegir i els requisits de seguretat desitjats.

El conjunt de totes les normes de seguretat ha d'abastar la protecció de tots els entorns dels sistemes d'informació de l'organització.

Aquestes normes han d'establir un conjunt d'expectatives i de requisits que s'han d'assolir per poder satisfer i complir cadascun dels objectius de seguretat establerts en la política.

Les ha de proposar la persona responsable de la seguretat i les ha d'aprovar el Comitè de Seguretat de la Informació.

c.Els procediments de seguretat han de descriure, de forma concreta, com protegir tot el que s'estableix en les normes, i també les persones o els grups que han de ser responsables d'implantar-los, mantenir-los i fer-ne el seguiment del nivell de compliment.

- Són documents que han d'especificar com dur a terme les tasques habituals, qui ha de fer cada tasca i com identificar i reportar comportaments anòmals.
- L'aprovació depèn de l'àmbit d'aplicació, que pot ser en un àmbit específic o en un sistema d'informació determinat.

A més, es poden establir guies amb recomanacions i bones pràctiques.

10. Revisió de la política

El Comitè de Seguretat de la Informació ha de revisar i proposar les actualitzacions necessàries de la política de seguretat de la informació quan:

a. Es facin canvis en el marc legal que puguin qüestionar la validesa d'aquesta política.

b. Es detectin incidències de seguretat que suposin un increment significatiu del nivell de risc actual o que hagin causat un impacte en els sistemes d'informació del Consell.

c. Ho consideri oportú per millorar la seguretat de la informació del Consell.

La revisió de la política de seguretat de la informació ha de garantir l'alineació amb l'estratègia, la missió i la visió del Consell en matèria de seguretat de la informació i ha d'assegurar que es compleixen els objectius de control establerts.

Per complir aquest objectiu, el Comitè de Seguretat de la Informació pot proposar qualsevol modificació que consideri necessària.

11. Obligacions del personal

Tot el personal amb responsabilitat en l'ús, operació o administració de sistemes de tecnologies de la informació i les comunicacions té l'obligació de conèixer i complir aquesta política de seguretat de la informació i la normativa de seguretat derivada, independentment del tipus de relació jurídica que el vinculi amb el Consell.

Totes les persones rebran formació per al maneig segur dels sistemes en la mesura que la necessitin per dur a terme el seu treball.

La política de seguretat ha de ser accessible per a tot el personal que presti els serveis en el Consell Insular de Mallorca.

Amb l'objectiu de fomentar la cultura de la seguretat, el Comitè de Seguretat de la Informació promourà un programa de conscienciació continua per formar tot el personal.

Si s'incompleix la política de seguretat i la normativa de desplegament, s'establiran mesures preventives i correctives encaminades a salvaguardar i protegir les xarxes i els sistemes d'informació, sense perjudici d'exigir la responsabilitat disciplinària corresponent.

12. Relacions amb tercers

Quan l'Administració del Consell presti serveis o cedeixi informació a altres administracions públiques o organismes, se'ls ha de fer partícips d'aquesta política de seguretat de la informació i de les normes i instruccions derivades.

Així mateix, quan l'Administració utilitzi serveis de tercers o cedeixi informació a tercers, se'ls ha de fer igualment partícips d'aquesta política de seguretat de la informació, de la normativa i de les instruccions de seguretat que pertoqui a aquests serveis o informació. Els tercers queden subjectes a les obligacions i mesures de seguretat que estableix la normativa i les instruccions, i poden desenvolupar els seus procediments operatius propis per satisfer-la. S'han d'establir procediments específics de detecció i resolució d'incidències. S'ha de garantir

que el personal de tercers està conscienciat adequadament en matèria de seguretat de la informació, almanco al mateix nivell que el que s'estableix en aquesta política de seguretat de la informació.

En concret, els tercers han de garantir que es compleix la política de seguretat de la informació basant-se en estàndards auditables que permetin verificar que aquestes polítiques es compleixen. Així mateix, s'ha de garantir, mitjançant una auditoria o un certificat de destrucció o d'esborrament, que el tercer cancel·la i elimina les dades pertanyents a l'Administració del Consell en acabar el contracte.

Quan algun aspecte de la política de seguretat de la informació no pugui ser satisfet per una tercera part, es requerirà un informe de la persona responsable de seguretat de la informació que precisi els riscos en què s'incorren i la forma de tractar-los. Es requerirà que la persona responsable de la informació i dels serveis afectats aprovi aquest informe abans de seguir endavant.»

Palma, 11 d'octubre de 2018

El secretari general per delegació del president
(Decret de dia 20 de juliol de 2015, BOIB núm. 114, de 28 de juliol)
Jeroni M. Mas Rigo