Ajuntament de Simat de la Valldigna

Anunci de l'Ajuntament de Simat de la Valldigna sobre aprovació definitiva de la Política de Seguretat de la Informació.

ANUNCI

El Ple de la Corporació de Simat de la Valldigna, en sessió ordinària de data 28 de març de 2022, acordà l'aprovació inicial de la Política de Seguretat de la Informació de l'Ajuntament de Simat de la Valldigna.

L´anunci publicat al BOPV núm. 70, de data 11 de maig de 2022, ha estat exposat al públic durant un termini de trenta dies, a efectes de reclamacions de conformitat amb el que disposa l'article 49 de la Llei Reguladora de les bases del Règim Local, 7/1985 de 2 d'abril, entenent-se definitivament aprovat per no haver-se produït reclamacions durant l´esmentat termini, en els següents termes:

Política de seguretat de la informació

Adequació dels Serveis Informàtics de l'Ajuntament de Simat de la Valldigna a l'Esquema Nacional de Seguretat

Índex

Introducció
1.1. Justificació de la política de seguretat de la informació
1.2 Missió i serveis prestats
Marc normatiu
Organització de la seguretat
1.3 definició de Rols
A Responsable de la Informació
B Responsable del Servei
C Delegat en protecció de dades
D Responsable de Seguretat de la Informació
1.4 comitè de seguretat de la informació
1.5 jerarquia en el procés de decisions i mecanismes de coordinació
1.6 procediments de designació de persones
dades de caràcter personal
gestió de riscos
1.7 justificació
1.8 criteris d'avaluació de riscos
1.9 directrius de tractament
1.10 procés d'acceptació del risc residual
1.11 necessitat de realitzar o actualitzar les avaluacions de riscos
Gestió d'incidents de seguretat
1.12 Prevenció d'incidents
1.13 monitorització i detecció d'incidents
1.14 resposta davant d'incidents
1.15 recuperació davant d'incidents i plans de continuïtat
Obligacions del personal
Terceres parts
Revisió i aprovació de la política de seguretat
Documentació complementària
Annex i. Glossari de termes

Introducció

1.1 Justificació de la política de seguretat de la informació

L'Ajuntament de Simat de la Valldigna 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 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 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. Per defensar-se d'aquestes amenaces, cal una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació continuada dels serveis. És per això que l'Esquema Nacional de Seguretat (Reial Decret 3/2010 de 8 de Gener, ENS en endavant), a l'article 11 estableix que "Tots els òrgans superiors de les Administracions Públiques hauran de disposar formalment de la seua política de seguretat, que serà aprovada pel titular de l'òrgan superior corresponent".

Això implica que les diferents àrees de l'Ajuntament de Simat de la Valldigna 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.

Totes les àrees s'han de assegurar 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. 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. Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, segons l'article 7 de l'ENS.

1.2 Missió i serveis prestats

L'Ajuntament de Simat de la Valldigna com a Òrgan de Govern Municipal, per a la gestió dels seus interessos, i en l'àmbit de les seves competències i com a Administració pública, serveix amb objectivitat els interessos generals i actua d'acord amb els principis d'eficàcia, jerarquia, descentralització i coordinació, promou tota classe activitats i presta els serveis públics que contribueixen a satisfer les necessitats i aspiracions dels habitants del municipi.

Esta Política de Seguretat aplica a les diferents activitats en què participa l'Ajuntament de Simat de la Valldigna a través de mitjans electrònics, en concret:

a. Les relacions de caràcter juridicoeconòmic entre els ciutadans i l'Ajuntament de Simat de la Valldigna

b. La consulta per part dels ciutadans de la informació pública administrativa i de les dades administratives que estiguin en poder de l'Ajuntament de Simat de la Valldigna.

c. La realització dels tràmits i procediments administratius incorporats per a la seua tramitació a la Seu Electrònica de l'Ajuntament de Simat de la Valldigna, de conformitat amb allò previst a l'Ordenança Municipal Reguladora de l'Ús de l'Administració Electrònica.

d. El tractament de la informació obtinguda per l'Ajuntament de Simat de la Valldigna l'exercici de les potestats.

Marc normatiu

Com a base normativa per realitzar aquesta guia de seguretat, s'ha analitzat la legislació vigent, que afecta el desenvolupament de les activitats de l'Administració, pel que fa a administració electrònica, i que implica la implantació de manera explícita de mesures de seguretat sistemes d'informació. El marc legal en matèria de seguretat de la informació ve establert per la següent legislació:

• Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, que assenyala a l'art. 17.3 que els mitjans o suports en què s'emmagatzemin documents hauran de comptar amb les mesures de seguretat que estableix l'Esquema Nacional de Seguretat, que garanteixin una sèrie de principis (com integritat, autenticitat, confidencialitat, qualitat, protecció i conservació dels documents emmagatzemats);i, estableix també, al seu art. 27.3 que les administracions públiques hauran de complir amb l'Esquema Nacional de Seguretat per garantir la identitat i el contingut de les còpies electròniques o en paper, és a dir, el caràcter de còpies autèntiques. Finalment, disposa a la seua Disposició Addicional segona que, tant les Comunitats Autònomes, com les Entitats Locals, hauran de garantir la seua compatibilitat informàtica i interconexió, així com la transmissió telemàtica de les sol·licituds, escrits i comunicacions que es realitzin en els seus registres i plataformes corresponents. mitjançant el compliment, igualment, de l'Esquema Nacional de Seguretat. I que, a més, deroga la Llei 11/2007, del 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

• 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, fixa els principis bàsics i els requisits mínims, així com les mesures de protecció a implantar en els sistemes de Administració.

• 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.

• Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica, la finalitat de la qual és la creació de les condicions necessàries per garantir el nivell d'interoperabilitat tècnica, semàntica i organitzativa adequat. dels sistemes i les aplicacions emprats per les administracions públiques, que permeti l'exercici de drets i el compliment de deures a través de l'accés electrònic als serveis públics, alhora que redunda en benefici de l'eficàcia i l'eficiència.

• 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 (d'ara endavant RGPD) .

Organització de la seguretat

1.3 Definició de rols

Tal com indica l'article 12 de l'ENS, la seguretat ha de comprometre tots els membres de l'organització. S'estableixen els rols següents a l'organització relacionats amb la Seguretat de la Informació:

A Responsable de la informació

S'ha designat responsable de la informació a l'Alcaldia, a qui corresponen les funcions següents:

• Adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat dels tractaments de dades de caràcter personal i evitin la seua 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 què estan exposats, ja provinguin de l'acció humana o del medi físic o natural.

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

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

• 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.

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

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

B Responsable del servei

S'ha designat ala Secretaria/Intervenció com a Responsable del Servei, a qui correspon les funcions següents:

• Quant al RGPD, per delegació del Responsable del tractament s'encomana al Responsable del Servei el desenvolupament de les tasques relacionades amb la gestió dels fitxers i tractaments de dades personals que es realitzen a la seua àrea en concret. Aquesta figura en terminologia de protecció de dades de caràcter personal s'anomena Gestor de Fitxers Concrets.

• 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.

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

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

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

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

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

C Delegat en protecció de dades

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

1 Informar i assessorar el responsable, l'encarregat i els empleats.

1. Supervisar el compliment incloent-hi assignació de responsabilitats, conscienciació i formació personal.

2. Assessorar sobre l'avaluació d'impacte i supervisar-ne l'aplicació.

3. Cooperar amb l'autoritat de control.

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

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

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

• Identificació de les bases jurídiques dels tractaments.

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

• Existència de normativa sectorial que pugui determinar condicions de tractament específiques, diferents de les establertes per la normativa general de protecció de dades.

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

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

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

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

• 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.

• Disseny i implantació de polítiques de protecció de dades.

• Auditoria de protecció de dades.

• Establiment i gestió dels registres d'activitats de tractament.

• Anàlisi de risc dels tractaments realitzats.

• Implantació de les mesures de protecció de dades des del disseny i protecció de dades per defecte, adequades als riscos i naturalesa dels tractaments

• Implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments

• 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

• Determinació de la necessitat de fer avaluacions d'impacte sobre la protecció de dades

• Realització d'avaluacions d'impacte sobre la protecció de dades

• Relacions amb les autoritats de supervisió.

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

Este rol ha estat assignat a Govertis Advisory Services SL.

D Responsable de seguretat de la informació

S'ha designat com a responsable de Seguretat de la Informació a la persona Responsable d'Informàtica, a qui correspondran les següents funcions:

• Coordinarà i controlarà les mesures definides al Registre d'activitats del tractament i en general s'encarregarà del compliment de les mesures de seguretat que detalla l'informe d'avaluació d'impacte a la protecció de dades.

• Reportarà directament al Comitè de Seguretat de la Informació.

• Actuarà com a secretari del Comitè de Seguretat de la Informació.

• Convocarà el Comitè de Seguretat de la Informació, recopilant la informació pertinent.

• Mantindrà la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb allò establert a la Política de Seguretat de l'Organització.

• Promourà la formació i la conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.

• Recopilarà els requisits de seguretat dels Responsables d'Informació i Servei i determinarà la categoria del Sistema.

• Realitzarà l'Anàlisi de Riscos.

• Elaborarà una Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides d'acord amb l'Annex II de l'ENS i el resultat de l'Anàlisi de Riscos.

• Facilitarà 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 a l'anàlisi de riscos i les mesures de seguretat requerides per l'ENS.

• Coordinarà l'elaboració de la documentació de seguretat del sistema.

• Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per aprovar-la per Direcció.

• Participarà en l'elaboració i aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de seguretat de la informació.

• Elaborarà i aprovarà els procediments operatius de seguretat de la informació.

• Facilitarà 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).

• Elaborarà, juntament amb els Responsables de Sistemes, Plans de Millora de la Seguretat, per a la seua aprovació pel Comitè de Seguretat de la Informació.

• Elaborarà 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.

• Validarà 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.

• Aprovarà les directrius proposades pels Responsables 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.

1.4 Comitè de seguretat de la informació

S'ha creat el Comitè de Seguretat de la Informació que estarà compost pels membres següents:

Presidència: l'alcaldia

Secretaria: administrativa d'administració general.

Vocals: la Secretaria de l'Ajuntament, la Prefectura de Policia Local i la Prefectura d'Administració

Poden acudir a requeriment del Comitè qualssevol altres caps de servei o àrea i responsables la intervenció dels quals sigui necessària per ser afectats per l'Esquema Nacional de Seguretat i pel RGPD.

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

• Atendre les inquietuds de l'Alta Direcció i dels diferents departaments.

• Informar regularment de l'estat de seguretat de la informació a l'Alta Direcció.

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

• Elaborar l'estratègia devolució de l'Ajuntament pel que fa a la seguretat de la informació.

• 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.

• Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè sigui aprovada per la Direcció.

• Aprovar la normativa de seguretat de la informació.

• Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.

• Monitoritzar els principals riscos residuals assumits per l'Ajuntament i recomanar possibles actuacions respecte d'aquests.

• Monitoritzar l'exercici dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'aquests. En particular, vetllar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.

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

• Aprovar plans de millora de la seguretat de la informació de l'Ajuntament. En particular, vetllarà per la coordinació de diferents plans que es puguin fer en diferents àrees.

• Vetllar perquè la seguretat de la informació es tingui en compte en tots els projectes TIC des de la seua 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.

• Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents àrees de l'Organització, elevant aquells casos en què no tingui prou autoritat per decidir.

• Demanarà regularment del personal tècnic propi o extern, la informació pertinent per prendre decisions.

• S'assessorarà sobre els temes que hagi 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 mixtos.

- Assessoria interna i/o externa.

- Assistència a cursos o altres tipus d'entorns formatius o d'intercanvi d'experiències.

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

• Aprovarà el Pla de Millora de la Seguretat, amb la dotació pressupostària corresponent.

1.5 Jerarquia en el procés de decisions i mecanismes de coordinació

Els diferents rols de seguretat de la informació (autoritat principal i possibles delegades) es limiten a una jerarquia simple: el Comitè de Seguretat de la Informació dóna instruccions al Responsable de la Seguretat de la Informació que s'encarrega d'emplenar, supervisant que administradors i operadors implementen les mesures de seguretat segons el que estableix la política de seguretat aprovada per a l'Organització.

El Responsable de la Seguretat informa el Responsable de la Informació de les decisions i incidents en matèria de seguretat que afectin la informació que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

El Responsable de la Seguretat informa al Responsable del Servei de les decisions i incidents en matèria de seguretat que afectin el servei que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

Quan hi hagi un Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta a aquest comitè com a secretari:

• Resum consolidat d'actuacions en matèria de seguretat.

• Resum consolidat d'incidents relatius a la seguretat de la informació.

• Estat de la seguretat del sistema, en particular del risc residual a què el sistema està exposat.

El Responsable de la Seguretat informa a la Direcció de l'Organització, segons allò acordat al Comitè de Seguretat de la Informació.

Quan no hi hagi un Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta directament a la Direcció de l'Organització:

• Resum consolidat d'actuacions en matèria de seguretat.

• Resum consolidat d'incidents relatius a la seguretat de la informació.

• Estat de la seguretat del sistema, en particular del risc residual a què el sistema està exposat.

1.6 Procediments de designació de persones

La Direcció de l'Organització nomenarà formalment:

• Al Responsable de la Informació; pot ser un càrrec unipersonal o un òrgan col·legiat (típicament, el Comitè de Seguretat de la Informació).

• Als Responsables del Servei; pot ser un càrrec unipersonal o un òrgan col·legiat (típicament, el Comitè de Seguretat de la Informació).

• Al Responsable de la Seguretat, que ha de reportar directament a la Direcció o, quan n'hi hagi, al Comitè de Seguretat de la Informació.

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 a la naturalesa i finalitat de les dades de caràcter personal recollides a l'esmentat Registre d'Activitats del Tractament.

Gestió de riscos

1.7 Justificació

Tots els sistemes subjectes a aquesta Política hauran de fer una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats.

L'anàlisi de riscos serà la base per determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establerts per l'Esquema Nacional de Seguretat, segons el que preveu l'article 6 de l'ENS.

1.8 Criteris d'avaluació de riscos

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

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

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

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

1.9 Directrius de tractament

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

1.10 Procés d'acceptació del risc residual

Els riscos residuals seran determinats pel Responsable de Seguretat de la Informació.

Els nivells de risc residuals esperats sobre cada informació després de la implementació de les opcions de tractament previstes (incloent-hi la implantació de les mesures de seguretat previstes a l'annex II de l'ENS) hauran de ser acceptats prèviament pel seu responsable d'aquesta informació.

Els nivells de Risc residuals esperats sobre cada Servei després de la implementació de les opcions de tractament previstes (incloent-hi la implantació de les mesures de seguretat previstes a l'Annex II de l'ENS) hauran de ser acceptats prèviament pel seu Responsable d'aquest Servei.

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

1.11 Necessitat de realitzar o actualitzar les avaluacions de riscos

L'anàlisi dels riscos i el seu tractament han de ser una activitat repetida regularment, segons el que estableix l'article 9 de l'ENS. Aquesta anàlisi es repetirà:

- Regularment, si més no una vegada a l'any.

- Quan es produeixin canvis significatius a la informació manejada.

- Quan es produeixin canvis significatius als serveis prestats.

- Quan es produeixin canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.

- Quan es produeixi un incident greu de seguretat.

- Quan es reportin vulnerabilitats greus.

Gestió d'incidents de seguretat

1.12 Prevenció d'incidents

Els departaments han d'evitar, o almenys prevenir en la mesura que sigui possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. L'ENS a través del seu article 19 estableix que els sistemes s'han de dissenyar i configurar de manera que garanteixin la seguretat per defecte. De la mateixa manera, l'article 17 de l'ENS esmentat defineix que els sistemes s'instal·laran en àrees separades, dotades d'un procediment de control d'accés.

Per això, els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat mitjançant una avaluació d'amenaces i riscos. Aquests controls, i els rols i les responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per garantir el compliment de la política, els departaments han de:

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

• Autoritzar els sistemes abans d'entrar a operació.

• Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de forma rutinària.

• Sol·licitar la revisió periòdica per part de tercers per obtenir una avaluació independent.

1.13 Monitorització i detecció d'incidents

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seua detenció, els serveis han de monitoritzar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons allò establert a l'article 9 de l'ENS.

La monitorització és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i reporti que arribin als responsables regularment i quan es produeixi una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

Els sistemes de detecció d'intrusos compleixen fonamentalment una tasca de supervisió i auditoria sobre els recursos de l'Organització, verificant que la política de seguretat no és violada i intenta identificar qualsevol tipus d'activitat maliciosa d'una manera primerenca i eficaç.

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

• Sistemes de detecció d'intrusos a nivell de xarxa.

• Sistemes de detecció d'intrusos a nivell sistema.

1.14 Resposta davant d'incidents

Els departaments han de:

• Establir mecanismes per respondre eficaçment als incidents de seguretat.

• Designar punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o altres organismes.

• Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).

1.15 Recuperació davant d'incidents i plans de continuïtat

Per garantir la disponibilitat dels serveis crítics, els departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del pla general de continuïtat de negoci i activitats de recuperació.

Obligacions del personal

Tots els membres de l'organització 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 lorganització atendran a una sessió de conscienciació en matèria de seguretat TIC almenys una vegada cada dos anys. S'establirà un programa de conscienciació continuada per atendre tots els membres de l'organització, 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 seua primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats.

El compliment de la present Política de Seguretat és obligatori per part de tot el personal intern o extern que intervingui en els processos

l'organització, constituint el seu incompliment infracció greu a efectes laborals.

Terceres parts

Quan es prestin serveis o es gestioni informació d'altres organitzacions, se'ls farà partícip d'aquesta Política de Seguretat de la Informació, s'establiran canals per reportar i coordinar els Comitès de Seguretat de la Informació respectius i s'establiran procediments d'actuació per a la reacció. davant d'incidents de seguretat.

Quan s'utilitzin serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que afecta aquests serveis o informació. Aquesta tercera part queda subjecta a les obligacions establertes en aquesta normativa, i poden desenvolupar els seus propis procediments operatius per satisfer-la.

S'establiran procediments específics de reporti i resolució d'incidències.

Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que el que estableix aquesta Política.

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

Revisió i aprovació de la política de seguretat

La Política de Seguretat de la Informació serà revisada pel Comitè de Seguretat de la Informació a intervals planificats, que no podran excedir l'any de durada, o sempre que es produeixin canvis significatius, per assegurar que se'n mantingui la idoneïtat, l'adequació i eficàcia.

Els canvis sobre la política de seguretat de la informació han de ser aprovats per l'òrgan superior competent que correspongui, d'acord amb l'article 11 de l'ENS.

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

Documentació complementària

La Política de Seguretat de la Informació s'emplenarà amb documents més precisos que ajuden a dur a terme allò proposat. Per això s'utilitzaran:

- Normes de seguretat (security standards).
- Guies de seguretat (security guides).
- procediments de seguretat (security procedures).

Les normes uniformitzen l'ús d'spectes concrets del sistema. Indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori.

Les guies tenen un caràcter formatiu i busquen ajudar els usuaris a aplicar correctament les mesures de seguretat proporcionant raonaments on no hi ha procediments precisos. Per exemple, hi sol haver una guia sobre com escriure procediments de seguretat. Les guies ajuden a prevenir que es passin per alt aspectes importants de seguretat que es poden materialitzar de diverses maneres.

Els procediments [operatius] de seguretat afronten tasques concretes, indicant què cal fer, pas a pas. Són útils en tasques repetitives.

ANNEX I. GLOSSARI DE TERMES

Anàlisi de riscos

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

Dades de caràcter personal

Qualsevol informació concernent persones físiques identificades o identificables.

Gestió d'incidents

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

Gestió de riscos

Activitats coordinades per dirigir i controlar una organització pel que fa als riscos.

Incident de seguretat

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

Informació

Cas concret d´un cert tipus d´informació.

Política de seguretat

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

Principis bàsics de seguretat

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

Responsable de la informació

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

Responsable de la seguretat

El responsable de seguretat determinarà les decisions per satisfer els requisits de seguretat de la informació i dels serveis.

Responsable del servei

Persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.

Responsable del sistema

Persona que sencarrega de l'explotació del sistema d'informació.

Servei

Funció o prestació exercida per alguna entitat oficial destinada a cuidar interessos o satisfer necessitats dels ciutadans.

Sistema d'informació

Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, fer servir, compartir, distribuir, posar a disposició, presentar o transmetre.

Simat de la Valldigna, a 30 de maig de 2022.—L'alcalde, Víctor Mansanet Boïgues.

2022/6277