Número de Referència: DX762HKBV7EC

Podeu validar i obtenir la versió electrònica d'aquest document a http://www.ajmanresa.cat/validar

SERVEI DE COOPERACIÓ EN L'ADMINISTRACIÓ ELECTRÒNICA, TRANSPARÈNCIA I PROTECCIÓ DE DADES
SGR.PDP2023000003

RESOLUCIÓ

Montserrat Clotet Masana, quarta tinent d'alcalde, regidora delegada de Recursos Humans i Govern Obert de l'Ajuntament de Manresa, dicto la resolució següent per aprovar la Política de Seguretat de la Informació i nomenar el Responsable del Sistema i el Responsable de Seguretat.

ANTECEDENTS DE FET

La informació constitueix un element essencial per a la prestació dels serveis municipals per part de l'Ajuntament de Manresa. Aquesta informació és processada mitjançant les tecnologies de la informació i les comunicacions que han esdevingut un element indispensable per a les administracions públiques en suportar el tractament d'aquesta informació, especialment en els serveis de l'administració electrònica adreçats a la ciutadania.

Tot i les millores que suposa el tractament de la informació i els serveis per mitjans electrònics quant a operativitat i eficiència, aquestes impliquen l'assumpció de nous riscos que requereixen implantar un conjunt de mesures específiques per protegir la informació i els serveis prestats per l'Ajuntament. En aquest sentit, la seguretat de la informació té com a objectiu protegir la informació i els serveis, analitzant els riscos als quals estan sotmesos i proposar les mesures necessàries que permetin reduir-los fins a un nivell que resulti acceptable per a l'organització. Aquest nivell de risc acceptable ha de ser determinat per la direcció de l'entitat, així com ordenar les actuacions necessàries i habilitar els mitjans que siguin necessaris per dur-les a terme.

La finalitat de l'Esquema Nacional de Seguretat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, que permeti als ciutadans i a les administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans.
Amb aquest objectiu, l'Ajuntament ha elaborat la Política de Seguretat de la Informació i donant compliment de l'exigència del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració Electrònica, que en l'article 12 estableix l'obligació per a les administracions públiques de disposar d'una política de seguretat i els requisits mínims que ha de complir.

L'establiment d'una **política de seguretat de la informació**, amb la subsegüent **distribució de funcions i responsabilitats** en l'àmbit de la seguretat de la informació resulta una actuació prioritària, ja que són els dos instruments principals per al govern de la seguretat de la informació i constitueixen el marc de referència per a totes les actuacions posteriors.

La Política de Seguretat segueix les indicacions de la guia CCN-STIC-805 del Centre Criptològic Nacional (CCN), centre adscrit al Centre Nacional d'Intel·ligència (CNI). L'adaptació a l'Esquema Nacional de Seguretat (ENS) implica que l'Ajuntament de Manresa, mitjançant el seu personal i els tercers que facilitin serveis relacionats amb l'Administració Electrònica, han d'aplicar les mesures mínimes de seguretat exigides pel mateix ENS, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

L'Ajuntament de Manresa té el deure d'assegurar que la seguretat de la informació és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la retirada del servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i els costos associats han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes relacionats amb els sistemes d'informació.

L'Ajuntament de Manresa ha contractat el servei de suport en matèria de seguretat dels sistemes d'informació, així com la implementació, revisió i manteniment continuat de l'Esquema Nacional de Seguretat a l'empresa Objectivo Tarsys S.L., la qual ja ha presentat una proposta d'adequació.

FONAMENTS DE DRET

- Llei 39/2015, de l'1 d'octubre, de Procediment Administratiu Comú de les administracions públiques.
- Llei 40/2015, de l'1 d'octubre, del Règim Jurídic del Sector Públic.
- Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'Actuació i Funcionament del sector públic per mitjans electrònics.
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat
- Llei 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia de drets digitals

L'adopció d'aquesta resolució és competència de la quarta tinent d'alcalde, regidora delegada de Recursos Humans i Govern Obert, en exercici de les competències que li han estat conferides per la delegació efectuada per Resolució de l'alcalde núm. 11378 de data 23 de juny de 2023, i publicada al BOPB del dia 27 de juny de 2023.

En virtut de tot el que s'ha exposat,

RESOLC:

PRIMER.- Aprovar la Política de Seguretat de la Informació de l'Ajuntament de Manresa, en els termes de l'annex que s'incorpora a la present resolució.

SEGON.- Els criteris i instruccions contingudes en el document que s'aprova mitjançant la present resolució constitueixen directrius vinculants per a totes les unitats organitzatives de l'Ajuntament de Manresa. L'Ajuntament mantindrà a la seu electrònica la versió actualitzada del document de Política de Seguretat de la Informació.

TERCER.- Nomenar al Responsable del Sistema, responsabilitat que recaurà en el Cap Servei de Tecnologies i Sistemes d'Informació.

QUART.- Nomenar al Responsable de Seguretat, responsabilitat que recaurà en el Grup de treball de seguretat de la informació, integrat per personal dels següents serveis:

- Servei de Cooperació en l'Administració electrònica, Transparència i Bon Govern.
- Servei d'Organització i Recursos Humans
- Servei de Tecnologies i Sistemes de la Informació.

Número de Referència: DX762HKBV7EC

Podeu validar i obtenir la versió electrònica d'aquest document a http://www.ajmanresa.cat/validar

ANNEX

ESQUEMA NACIONAL DE SEGURETAT
POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE L'AJUNTAMENT DE MANRESA

1. INTRODUCCIÓ

L'Ajuntament de Manresa, d'ara endavant l'Ajuntament, en tant que Administració Pública al servei de la ciutadania disposa d'una infraestructura de Tecnologies d'Informació i Comunicacions (TIC) per a desenvolupar les seves competències i assolir els seus objectius.

La gestió de les TIC ha de ser portada a terme aplicant les mesures necessàries que li permetin garantir la protecció davant de les possibles incidències (accidentals o deliberades) que es puguin produir, de forma que es puguin minimitzar les afectacions sobre la disponibilitat, integritat o confidencialitat de la informació relacionada amb els serveis prestats.

La qualitat de la informació i la prestació continuada de serveis hauran de ser garantits actuant de forma preventiva, mitjançant una adequada supervisió periòdica i constant, tenint com a objectiu final la seguretat de la informació com a cultura general a l'entitat.

D'acord amb allò que s'estableix a l'article 12.6 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), la política de seguretat s'ha d'establir sobre la base dels principis bàsics en l'àmbit de l'Administració electrònica i estableix que tots els òrgans superiors de les administracions públiques han de disposar formalment de la seva política de seguretat, que ha de ser aprovada pel titular de l'òrgan superior corresponent i s'ha de desenvolupar aplicant els requisits mínims següents en proporció als riscos identificats en cada sistema:

a) Organització i implantació del procés de seguretat.
b) Anàlisi i gestió dels riscos.
c) Gestió de personal.
d) Professionalitat.
e) Autorització i control dels accessos.
f) Protecció de les instal·lacions.
g) Adquisició de productes de seguretat i contractació de serveis de seguretat.
h) Mínim privilegi.
i) Integritat i actualització del sistema.
j) Protecció de la informació emmagatzemada i en trànsit.
k) Prevenció davant d'altres sistemes d'informació interconnectats.
l) Registre de l'activitat i detecció de codi nociu.
m) Incidents de seguretat.
n) Continuïtat de l'activitat.
o) Millora contínua del procés de seguretat.

Així mateix, l'article 12.2 de l'ENS indica que la política de seguretat ha de ser formalment aprovada per l'òrgan competent.

Per tot el que s'exposa anteriorment, en aquest document es defineix la política de seguretat de la informació de l'Ajuntament.

1.1 Abast

Aquesta política s'aplica a tots els sistemes TIC (infraestructures, programari, comunicacions,...) de l'Ajuntament i a tots els seus membres, sense excepcions.

Els serveis contemplats a l'àmbit d'aplicació, així com el Servei o Secció Responsable i el sistema informàtic associat, es troben identificats a l'Anàlisi de Riscos de l'Ajuntament.

1.2 Missió

Mitjançant la present Política de Seguretat l'Ajuntament de Manresa expressa el seu compromís amb l'administració de la seguretat de la seva informació, d'acord amb els requeriments propis, així com amb les lleis i normatives vigents.

1.3 Aprovació i entrada en vigor

Aquesta política de seguretat de la Informació és efectiva des de la data d'aprovació mitjançant resolució de l'alcaldia (o de la regidoria delegada) i fins que sigui reemplaçada per una nova política.

2. MARC LEGISLATIU

L'ús de les TIC per part de l'Ajuntament de Manresa es troba regulat per les següents normes jurídiques:

ESTATAL
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques
- Reial decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat.
- Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.
- Reglament (UE) 2016/679 del Parlament 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 (RGPD).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD)
- Reial decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics
- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.
- Instruccions del Centre Criptogràfic Nacional, CCN-STIC.

AUTONÒMICA
- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, d'ús dels mitjans electrònics al sector públic de Catalunya.

LOCAL
- Reglament Orgànic Municipal (ROM).
- Ordenança d'Administració Electrònica i Transparència de l'Ajuntament de Manresa.
- Reglament d'ús de les dades personals i els sistemes d'informació de l'Ajuntament de Manresa.

Número de Referència: DX762HKBV7EC
Podeu validar i obtenir la versió electrònica d'aquest document a http://www.ajmanresa.cat/validar

3. PRINCIPIS DE COMPLIMENT DE LA POLÍTICA DE SEGURETAT

Les TIC utilitzades per l'Ajuntament han de disposar d'elements que en garanteixin una protecció adient contra amenaces que, a causa de la seva constant evolució, tenen un gran potencial per a produir afectacions en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis.

Amb l'objectiu de disposar d'elements per a la defensa d'aquestes amenaces, l'Ajuntament necessita disposar d'una estratègia que s'adapti als canvis constants que es produeixen a l'entorn per garantir la prestació contínua dels serveis. Això implica que l'Ajuntament ha d'aplicar les mesures mínimes de seguretat exigides pel Reial decret 311/2022, de 3 de maig, que regula l'ENS, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

L'Ajuntament ha de garantir que la seguretat TIC esdevingui un element integral del sistema, des del seu disseny inicial fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició de programari i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació de l'àrea, en la sol·licitud de propostes de serveis, i en l'elaboració dels plecs per a la licitació de projectes relacionats amb les TIC.

Els procediments i normatives aplicables als sistemes informàtics i organització informàtica es recullen als Procediments tècnics TIC.

3.1 Dades de caràcter personal

L'Ajuntament, en el desenvolupament de les seves competències, tracta dades personals de la ciutadania, el seu personal i tercers.

Els sistemes d'informació que tractin dades personals hauran d'aplicar el que disposa la normativa vigent en matèria de protecció de dades personals. Per a això, l'Ajuntament, amb l'assessorament i participació del Delegat de Protecció de Dades, durà a terme una anàlisi de riscos d'acord el definit als articles 24 i 32 de l'RGPD i, si s'escau, una avaluació d'impacte en la protecció de dades dels tractaments de l'Ajuntament.

Els sistemes d'informació de l'Ajuntament han d'aplicar les mesures de seguretat resultants d'aquesta anàlisi, que prevaldran si són més exigents a les definides per l'Esquema Nacional de Seguretat.

3.2 Gestió de riscos

Tots els sistemes subjectes a aquesta política hauran de ser objecte d'una anàlisi de riscos, on s'avaluïn les amenaces i els riscos a què estan exposats.

Aquesta anàlisi es portarà quan es produeixin les següents circumstàncies:

- Regularment, almenys un cop l'any.
- Quan es produeixin canvis en la informació tractada.
- Quan es produeixin canvis en els serveis prestats.
- Quan es detecti una incidència de seguretat greu.
- Quan es detectin vulnerabilitats greus.

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

L'Ajuntament garantirà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

3.3 Prevenció i reacció davant incidències

El personal de l'Ajuntament ha de disposar dels mecanismes per a la prevenció, detecció, resposta i conservació per a minimitzar les vulnerabilitats, evitar que les amenaces es materialitzin i – en cas contrari - reaccionar davant de possibles incidents, d'acord amb l'article 8 i 25 de l'ENS, i l'article 33 de l'RGPD si afecta dades personals.

La seguretat del sistema ha de contemplar les accions relatives als aspectes de prevenció, detecció i resposta, a fi de minimitzar les seves vulnerabilitats i aconseguir que les amenaces sobre aquest no es materialitzin o que, en el cas de fer-ho, no afectin greument la informació que maneja o als serveis que presta.

Les mesures de prevenció, que poden incorporar components orientats a la dissuasió o a la reducció de la superfície d'exposició, han d'eliminar o reduir la possibilitat que les amenaces arribin a materialitzar-se.

Les mesures de detecció aniran dirigides a descobrir la presència d'un incident de seguretat.

Les mesures de resposta, que es gestionaran en temps oportú, estaran orientades a la restauració de la informació i els serveis que es puguin haver estat afectats per un incident de seguretat.

El sistema d'informació garantirà la conservació de les dades i la informació en suport electrònic, garantint que la seva aplicació no suposi una reducció en l'aplicació principis bàsics i requisits mínims establerts.

De la mateixa manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital, mitjançant una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

4. ORGANITZACIÓ DE LA SEGURETAT

4.1 Funcions i responsabilitats

Els rols i les funcions de l'organització de la seguretat establerts a l'Esquema Nacional de Seguretat seran assumits pel Grup de treball de seguretat de la informació i el rol de Responsable del Sistema que serà assumit per la Cap del Servei de Tecnologies i Sistemes d'Informació.

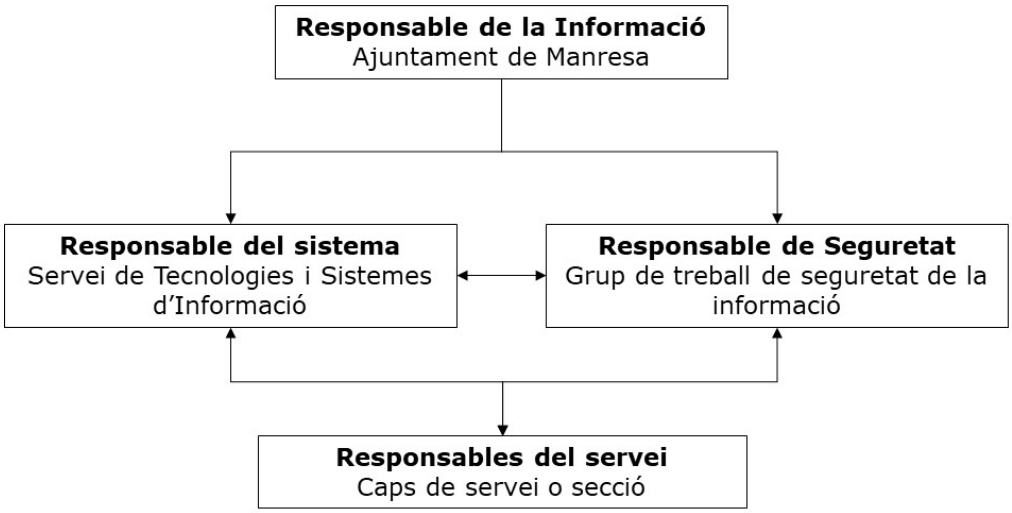
Les Responsabilitats dels Òrgans de Direcció de l'Ajuntament de Manresa respecte al compliment de la legislació són:

- Assignar al Grup de treball de seguretat de la informació a càrrec de coordinar i controlar les mesures definides en la present Política de Seguretat.
- Nomenar el Responsable de Seguretat, tasca assumida pel Grup de treball de seguretat de la informació.
- Donar el suport i dotar dels recursos necessaris al Grup de treball de seguretat de la informació i al Cap del Servei de Tecnologies i Sistemes d'Informació per a poder portar a terme les seves funcions.

Número de Referència: DX762HKBV7EC

Podeu validar i obtenir la versió electrònica d'aquest document a http://www.ajmanresa.cat/validar

L'organització per a la gestió de la protecció de dades de l'Ajuntament de Manresa és:



4.1.1 Responsable de la Informació

Responsable de la Informació	Alcaldia
Funcions	- Nomenar el Responsable de Seguretat ENS, tasca assumida pel Grup de treball de seguretat de la informació. - Nomenar el Responsable del Sistema, tasca assumida pel Cap del Servei de Tecnologies i Sistemes de la Informació. - Donar el suport i dotar dels recursos necessaris al Responsable de Seguretat i al Responsable del Sistema per a poder portar a terme les seves funcions.

4.1.2 Responsable de Seguretat

Responsable de Seguretat	Grup de treball de seguretat de la informació
Composició	- Servei de Cooperació en l'Administració electrònica, Transparència i Bon Govern - Servei d'Organització i Recursos Humans - Servei de Tecnologies i Sistemes de la Informació.
Funcionament	- 1 reunió trimestral, amb caràcter ordinari - Extraordinàriament, aquesta Comissió es reuniria per tractar temes urgents o de necessitat.

Actua com a secretari/ària	Servei de Cooperació en l'Administració electrònica, Transparència i Bon Govern, o qui delegui, amb la col·laboració de personal administratiu en qui es delegui, que exercirà les següents funcions: - Coordinar i preparar l'agenda de les reunions i enviar comunicacions de convocatòries. - Elaborar actes de les reunions ordinàries i extraordinàries - Gestió administrativa de la documentació emesa per la Comissió. - Comunicació al personal i responsables de les decisions preses pel Grup de treball de seguretat de la informació.
Relació amb les dades personals	El Grup de treball de seguretat de la informació implanta les mesures per a la protecció de les dades i dona suport al DPD
Funcions	- Establir, impulsar i garantir l'aplicació i el compliment de les polítiques i procediments de Seguretat aprovats per l'Ajuntament. - Validar i tramitar l'aprovació de la documentació relacionada amb la seguretat de la informació (Política de Seguretat, Reglaments Interns...). - Garantir la correcta implantació de les polítiques i procediments de Seguretat. - Promoure les auditories i controls regulars que permetin verificar el compliment de les obligacions de l'Ajuntament en seguretat de la informació. - Promoure la formació i conscienciació de la seguretat de la informació al personal de l'Ajuntament. - Garantir, amb el suport del Responsable del Sistema, la implantació i control de les mesures de seguretat de manera que aquestes s'integrin adequadament a l'operativa d'Administració Electrònica. - Garantir la correcta regulació legal dels proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS. - Vetllar per tal que es dugui a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema. - Fer el seguiment dels incidents de seguretat que hagin ocorregut relatius a la seguretat de la informació, amb el suport del Responsable del Sistema.

4.1.3 Responsable del Sistema

Responsable del Sistema	Servei de Tecnologies i Sistemes d'Informació
Funcions delegades	- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar el seu correcte funcionament i operativitat. - Gestió, configuració i actualització, del maquinari i programari sota el seu àmbit de gestió en què es basen els mecanismes i serveis de seguretat del sistema. - Implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema que es trobi sota el seu àmbit de gestió. - Interlocució amb dels proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS. - Assegurar que la traçabilitat, auditoria i altres registres de seguretat es duen a terme sovint, d'acord amb la política de seguretat establerta. - Establir procediments de seguiment i reacció davant incidències. - Donar d'alta nous rols d'accés als programes i aplicacions corporatives que es trobin sota el seu àmbit de gestió.

Número de Referència: DX762HKBV7EC

Podeu validar i obtenir la versió electrònica d'aquest document a http://www.ajmanresa.cat/validar

4.1.4 Responsables de Serveis

Responsables de Serveis	Caps de secció o servei
Funcions delegades	- Definir els serveis necessaris per portar a terme les competències de l'Ajuntament de Manresa. - Vetllar pel compliment de les polítiques i normes de seguretat determinades per l'Ajuntament de Manresa en la gestió dels serveis i en el tractament de la informació de l'àmbit de responsabilitat. - Implementar totes les mesures de seguretat definides a la documentació de seguretat per a sistemes d'informació no automatitzats (arxiu i emmagatzematge de documentació). - Definir els perfils i criteris d'accés a la documentació i aplicacions informàtiques sota l'àmbit de responsabilitat. - Concedir o denegar l'autorització d'accés als usuaris a la informació sota el seu àmbit de responsabilitat.

4.2 Procediments de designació

El responsable de Seguretat i el Responsable de Sistema serà nomenat per resolució d'alcaldia (o de la regidoria en què hagi delegat la competència). El nomenament s'ha de revisar quan el lloc quedi vacant.

En el cas que un Servei o Secció presti electrònicament un servei sense la gestió ni coordinació o, com a mínim, la comunicació prèvia al Grup de treball de seguretat de la informació, haurà de designar el Responsable del Sistema i el Responsable de Seguretat que hauran de ser aprovats per Alcaldia, precisant les seves funcions i responsabilitats dins el marc establert per aquesta Política.

5. OBLIGACIONS DEL PERSONAL

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

Tots els membres de l'Ajuntament realitzaran una sessió de conscienciació en matèria de seguretat TIC quan el Responsable de Seguretat ho estimi necessari. Igualment, s'establirà un programa de conscienciació contínua per atendre tots els membres de l'Ajuntament, en particular als 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. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats.
Les obligacions del personal es troben recollides al Reglament d'ús de les dades personals i els sistemes d'informació.

6. TERCERES PARTS

Quan l'Ajuntament presti serveis a altres organismes o gestioni informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals per informe i coordinació dels respectius Responsables de Seguretat i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'Ajuntament utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que pertoqui a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, i poden desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta política.

Quan algun aspecte de la política no pugui ser satisfet per una tercera part, tal com s'exigeix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Serà necessària l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de continuar endavant.

Aquestes obligacions seran regulades mitjançant acord, conveni o contracte que defineixi la relació amb els tercers, així com els criteris de nivell de servei i els sistemes de control i monitoratge del compliment.

7. GESTIÓ I DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

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

La normativa de seguretat estarà disponible a la unitat de servidor definida per als documents a compartir entre el personal de l'Ajuntament.
La política serà aprovada per resolució d'alcaldia (o la regidoria en qui s'hagi delegat la competència), i difosa perquè la coneguin totes les parts afectades.

7.1 Revisió de la política de seguretat de la informació

Per verificar que s'acompleix amb tot allò que queda establert en aquesta Política de Seguretat, es realitzaran els controls interns que determini el Responsable de Seguretat (el Grup de treball de seguretat de la informació), en el referent als sistemes d'informació.

La periodicitat d'aquests controls serà definida pel Grup de treball de seguretat de la informació, existint també la possibilitat de portar a terme altres controls que pugui determinar en funció del desenvolupament de les operacions.

L'objectiu de les auditories serà verificar la possibilitat que els controls establerts a través de les mesures de seguretat siguin efectius, i que sigui possible garantir la integritat, la confidencialitat i la disponibilitat de la informació, les dades personals i els serveis TIC.

Serà missió del Responsable de Seguretat la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment d'aquesta. La política serà aprovada per resolució d'alcaldia (o de la regidoria en què s'hagi delegat la competència) i difosa perquè la coneguin totes les parts afectades.

Número de Referència: **DX762HKBV7EC**

Podeu validar i obtenir la versió electrònica d'aquest document a http://www.ajmanresa.cat/validar

Signat electrònicament per: MONTSERRAT CLOTET MASANA
Data: 25/10/2023 15:03:49
Raó: Ho resolc
Lloc: Manresa

Signat electrònicament per: JOSE LUIS GONZALEZ LEAL
Data: 26/10/2023 17:29:00
Raó: En dono fe
Lloc: Manresa