Ajuntament de Terrassa

EDICTE

Aprovació d'instruccions "Política de Seguretat de la Informació de l'Ajuntament de Terrassa"
Expedient ICOS/2024/6

En data 2 de juliol de 2024 l'Alcalde-President d'aquest Ajuntament, ha dictat el Decret núm. 21043/2024 que es transcriu literalment a continuació:

"L'Ajuntament de Terrassa és conscient de que la informació és un actiu important per qualsevol entitat, pública i privada, tota vegada que permet portar a terme les funcions, activitats i potestats encomanades, garantint unes condicions de validesa, veracitat, neutralitat i justícia.

La informació es tracta i es transmet, entre d'altres, per una sèrie de mitjans en constant evolució i que formen part de les tecnologies de la informació i la comunicació (TIC), sector que ha propiciat un nou entorn de prestació de serveis públics de qualitat a la ciutadania, i que s'ha tornat imprescindible per a les administracions públiques, ja que permet fer un tractament eficaç d'aquesta informació.

Cal considerar que si bé l'entorn de les comunicacions facilita l'accés a la informació per part de tot els que tenen un interès legítim, també comporta nous riscos per a la integritat, disponibilitat, confidencialitat i seguretat d'aquesta, els quals evolucionen i apareixen amb una freqüència cada vegada major.

El Reial Decret 311/2022, de 3 de maig que regula l'Esquema Nacional de Seguretat, amb la finalitat de crear les condicions necessàries per a la 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 permetin als ciutadans i a les administracions públiques, garantir l'exercici de drets i el compliment de deures a través d'aquests mitjans, planteja de manera crucial la protecció de la informació establint una sèrie de principis bàsics i requisits mínims amb l'objectiu de generar seguretat i confiança en la utilització dels mitjans electrònics en les relacions amb l'Administració.

En la mateixa línia de l'Esquema Nacional de Seguretat, l'Ajuntament de Terrassa planteja com a ordre prioritari la implantació i execució de mesures organitzatives i tècniques per protegir la informació i serveis prestats amb el suport de mitjans electrònics, amb una visió integral i amb vocació de permanència, és a dir, no es tracta de fixar actuacions concretes i puntuals, o de elaborar documents tècnics i polítiques que no s'apliquen en la pràctica, sinó de mantenir unes directrius i una consciència general en la gestió de la informació i el desenvolupament dels serveis electrònics a la nostra Corporació.

Amb aquest objectiu, l'Ajuntament de Terrassa va aprovar la seva "Política de Seguretat de la Informació" al març de 2018, actualment vigent i aplicable, que estableix les bases de protecció de la informació i serveis de l'Ajuntament de Terrassa prestats als ciutadans amb mitjans electrònics, amb l'objectiu de preservar la integritat dels drets i llibertats de les persones, entre els quals destaca la intimitat i la protecció de les dades personals.

L'aprovació al maig de 2022 del RD 311/2022, que modifica el RD 951/2015, que regula l'Esquema Nacional de Seguretat, incorpora novetats respecte al contingut que ha de incloure la Política de Seguretat de la Informació de les administracions públiques.

Amb l'objectiu d'adequar la Política de Seguretat de la Informació de l'Ajuntament de Terrassa als requeriments del nou reial decret de l'Esquema Nacional de Seguretat, el Responsable de la Seguretat de la Informació va elaborar una nova proposta de "Política de Seguretat de la Informació".

En aquesta proposta, addicionalment a complir amb els requisits del nou Esquema Nacional de Seguretat, s'han incorporat altres canvis com una modificació de la composició del Comitè de Seguretat de la Informació per a dotar a aquest òrgan de major efectivitat, la inclusió de noves figures en l'organització de la seguretat de la informació corporativa, com el Comitè de Crisi de la Seguretat de la Informació i el Grup de treball tècnic, i l'actualització del marc normatiu de la política per adequar-la a la legislació vigent.

La proposta de "Política de Seguretat de la Informació" que ha estat elaborada, alinea la implantació de les mesures de seguretat previstes a l'Esquema Nacional de Seguretat amb l'estratègia de desplegament de l'administració electrònica municipal, tot definint i regulant les aplicacions, serveis o sistemes propis dels Sistemes d'Informació emprats per l'Ajuntament de Terrassa i les seves entitats vinculades, per oferir els seus serveis a la ciutadania. Així mateix aplica i és d'obligat compliment per tots el membres de la organització en general, els òrgans superiors i directius de l'Ajuntament de Terrassa, entitats vinculades, així com per tercers als quals l'Ajuntament i entitats vinculades prestin o els hi prestin serveis i/o informació.

El Responsable de Seguretat de la informació va presentar al Comitè de Seguretat de l'Ajuntament de Terrassa aquesta nova versió de la Política de Seguretat, que ha estat revisada, incorporant alguns canvis, derivant el text definitiu que s'acompanya al present, als efectes de que per part de la seva Presidenta, es proposi la seva aprovació a l'òrgan de govern competent.

Consta a l'expedient la Providència de la Regidora instant la tramitació administrativa per a l'aprovació formal de la Política de seguretat de la Informació de l'Ajuntament de Terrassa i l'informe tècnic del Cap del Servei de Seguretat TIC que motiven la seva aprovació.

Vistes les atribucions de l'Alcaldia-Presidència, establertes a l'article 53 del Text refós de la Llei municipal i de règim local de Catalunya, aprovat pel Decret Legislatiu 2/2003, de 28 d'abril i les concordants de l'article 21 de la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local.

En l'ús de les competències que tinc assignades, RESOLC:

Primer.- Aprovar la "Política de Seguretat de la Informació de l'Ajuntament de Terrassa i les seves Societats Municipals", que consta en document annex, i que fixa les directrius en la gestió de la informació i desenvolupament dels serveis electrònics a la Corporació i que serà d'obligat compliment per a tots els membres de la organització en general, els Òrgans superiors i directius de l'Ajuntament de Terrassa, les Societats Municipals i els tercers als quals l'Ajuntament i Societats Municipals prestin o els hi prestin serveis i/o informació.

Segon.- Aprovar la designació dels òrgans previstos en la política de seguretat i la seva composició, essent:

1. COMITÈ DE SEGURETAT DE LA INFORMACIÓ
El Comitè de Seguretat de la Informació, al que correspondrà les funcions i responsabilitats previstes a l'apartat 6.1 de la Política de Seguretat de la Informació aprovada, estarà integrat per:
o Regidor/a o tinent d'alcalde que tingui atribuïdes les competències municipals en matèria de Tecnologia i Sistemes d'Informació (President/a del Comitè)
o Secretari/a General o Interventor/a
o Tresorer/a o Coordinador/a general
o Director/a d'Àrea en que es trobi circumscrit el servei de Tecnologia i Sistemes d'Informació
o Director/a dels Serveis de Secretaria d'Empreses i Grans Contractes
o Delegat/da de Protecció de Dades o Director/a serveis de Tecnologia i Sistemes d'Informació
o Responsable de Seguretat de la Informació, que actuarà com a secretari o secretària
o Responsable de Sistemes

Ajuntament de Terrassa

2. COMITÈ DE CRISI DE LA SEGURETAT DE LA INFORMACIÓ
El Comitè de Crisi de la Seguretat de la Informació, al que correspondrà les funcions i responsabilitats previstes a l'apartat 6.3 de la Política de Seguretat de la Informació aprovada, estarà integrat per:
- Alcalde/ssa o bé Regidor/a de Tecnologia i Sistemes d'Informació (President/a)
- Secretari/a General - Interventor/a - Tresorer/a - Coordinador/a general
- Director/a d'Àrea en que es trobi circumscrit el servei de Tecnologia i Sistemes d'Informació
- Delegat/da de Protecció de Dades - Responsable de Serveis Jurídics
- Director/a dels Serveis de Secretaria d'Empreses i Grans Contractes
- Director/a de Tecnologia i Sistemes d'Informació
- Responsable de Seguretat, que actuarà com a secretari o secretària.
- Responsable de Sistemes.
- Responsables de Comunicació: Comunicació externa, Comunicació Interna, Premsa i Xarxes Socials.
- Responsables dels serveis afectats
- En cas d'incidents molt greus, s'afegiran al comitè de crisi responsables de l'Agència de Ciberseguretat de Catalunya

3. GRUP DE TREBALL TÈCNIC
El grup de treball tècnic, al que correspondrà les funcions i responsabilitats previstes a l'apartat 6.2 de la Política de Seguretat de la Informació aprovada, estarà integrat per:

- Director/a de Tecnologia i Sistemes d'Informació
- Responsable de Seguretat, que actuarà com a secretari o secretària
- Responsable de Sistemes
- Tècnics de seguretat
- El cap de Processos en totes les reunions on es tractin temes de la seva competència o afectació

Tercer.- Facultar a la Regidora Sra. Laura Rivas Moreno, o persona que la substitueixi amb les competències en matèria de tecnologia i sistemes de la informació, per tal que dicti i signi quantes disposicions siguin necessàries per al desplegament i efectivitat de la política de seguretat de la informació que ha estat aprovada, així com per a l'adequació i/o renovació dels nomenaments efectuats a l'apartat anterior, d'acord amb les persones que ocupin aquestes llocs de treball.

Quart.- Comunicar el contingut del present Decret als interessats i que es publiqui el contingut íntegre de la "Política de Seguretat de la Informació de l'Ajuntament de Terrassa" que ha estat aprovada al Butlletí oficial de la Província de Barcelona i a la seu electrònica corporativa. "

ANNEX I - Política de Seguretat de la Informació de l'Ajuntament de Terrassa i les seves Societats Municipals

Anna Cardellach Giménez - DNI 39170934W

Signat digitalment per Anna Cardellach Giménez - DNI 39170934W
Data: 2024.07.11 11:54:08 +02'00'

Anna Cardellach Giménez
Subdirectora de l'Àrea de Serveis Generals i Govern Obert

Per delegació de signatura del Secretari General
de data 4 de març de 2024

Terrassa, 11 de juliol de 2024

Diputació Barcelona
https://bop.diba.cat
Pàg. 3-22
CVE 20241012740 3
Data 18-7-2024
BOPB Butlletí Oficial de la Província de Barcelona

Ajuntament de Terrassa

Annex 1

Política de Seguretat de la Informació de l'Ajuntament de Terrassa i les seves Societats Municipals

ÍNDEX

1. Introducció

L'Ajuntament de Terrassa és conscient de que la informació és un actiu important per qualsevol entitat, pública i privada, tota vegada que permet portar a terme les funcions, activitats i potestats encomanades, garantint unes condicions de validesa, veracitat, neutralitat i justícia.

La informació es tracta i es transmet, entre d'altres, per una sèrie de mitjans en constant

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 202410127403 | Pàg. 4-22 | https://bop.diba.cat | Diputació Barcelona

evolució i que formen part de les tecnologies de la informació i la comunicació (TIC), sector que ha propiciat un nou entorn de prestació de serveis públics de qualitat a la ciutadania, i que s'ha tornat imprescindible per a les administracions públiques, ja que permet fer un tractament eficaç d'aquesta informació.

Cal considerar que si bé l'entorn de les comunicacions facilita l'accés a la informació per part de tot els que tenen un interès legítim, també comporta nous riscos per a la integritat, disponibilitat, confidencialitat i seguretat d'aquesta, els quals evolucionen i apareixen amb una freqüència cada vegada major.

D'acord amb el Reial Decret 311/2022, de 3 de maig , pel qual es regula l'Esquema Nacional de Seguretat (en endavant ENS) en l'àmbit de l'Administració Electrónica, l'Ajuntament de Terrassa planteja com a ordre prioritari la implantació i execució de mesures organitzatives i tècniques per protegir la informació i serveis prestats amb el suport de mitjans electrònics.

L'ENS planteja de manera crucial la protecció de la informació establint una sèrie de principis bàsics i requisits mínims amb l'objectiu, igual que l'Ajuntament, de generar seguretat i confiança en la utilització dels mitjans electrònics en les relacions amb l'Administració. Aquesta seguretat representa per l'Ajuntament **una activitat de caràcter integral i amb vocació de permanència**, és a dir, no es tracta de fixar actuacions concretes i puntuals, o de elaborar documents tècnics i polítiques que no s'apliquen en la pràctica, sinó de mantenir unes directrius i una consciència general en la gestió de la informació i el desenvolupament dels serveis electrònics a la nostra corporació.

L'ENS estableix el marc regulador de la present Política de Seguretat de la Informació, la qual estableix les bases de protecció de la informació i serveis de l'Ajuntament de Terrassa prestats als ciutadans amb mitjans electrònics, amb l'objectiu de preservar la integritat dels drets i llibertats de les persones, entre els quals destaca la intimitat i la protecció de les dades personals.

La present Política de Seguretat de la Informació romandrà accessible i comprensible per tot el personal que directa o indirectament estigui al servei de l'Ajuntament de Terrassa, i definirà com es gestiona i protegeix la informació i els sistemes en funció del nivell de seguretat requerit.

2. Missió de l'Ajuntament de Terrassa

La missió de l'Ajuntament és millorar la qualitat de vida dels ciutadans i ciutadanes de Terrassa i respondre a les necessitats i expectatives de les persones usuàries dels serveis

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 202410127403 | Pàg. 5-22 | https://bop.diba.cat | Diputació Barcelona

municipals, contribuint a consolidar una ciutat més solidària, sostenible i activa, que generi oportunitats de desenvolupament industrial i de dinamisme comercial, d'innovació, de projecció exterior, ocupació, educació i formació, equilibri, igualtat i justícia social i millora de la qualitat de vida, el benestar i progrés de la ciutadania, incorporant la voluntat permanent de diàleg, respecte i consens polític i social, transparència, l'honestedat, la proximitat a la ciutadania, la qualitat democràtica, les llibertats, la igualtat, la convivència, el respecte i el progrés social, l'aposta per la cooperació públic-privada, la cooperació institucional, i l'ús eficient dels recursos com a valors fonamentals que defineixen l'acció municipal.

3. Objecte i Abast

Les disposicions d'aquesta Política afecten a l'Ajuntament de Terrassa així com a les societats municipals que estan integrades amb l'Ajuntament a nivell tecnològic, i a la resta de societats municipals que s'hi vulguin adscriure. Aquesta política s'aplicarà als sistemes d'informació d'aquests organismes que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu dels ciutadans i ciutadanes, i que es troben dins de l'àmbit d'aplicació del l'Esquema Nacional de Seguretat (ENS).

4. Marc Normatiu

El marc normatiu de les activitats de l'Ajuntament de Terrassa en l'àmbit d'aquesta Política de Seguretat de la Informació està integrat per les següents normes:

a) Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament General de Protecció de Dades).
b) Llei orgànica 3/2018 de 5 de desembre de protecció de dades personals i garantia dels drets digitals.
c) Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre de protecció de Dades de caràcter personal, aplicable en allò que no s'oposi al Reglament (UE) 2016/679 ni a la llei orgànica 3/2018 de 5 de desembre de protecció de dades personals i garantia dels drets digitals.
d) Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local.
e) Decret Legislatiu 2/2002, de 28 d'abril, pel qual s'aprova el Text refós de la Llei municipal i de règim local de Catalunya.

Diputació Barcelona | https://bop.diba.cat | Pàg. 6-22 | CVE 202410127403 | Data 18-7-2024 | BOPB Butlletí Oficial de la Província de Barcelona

f) Llei 39/2015, de 1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.
g) Llei 34/2002, d'11 de juliol, de Serveis de la Societat de la Informació i de Comerç Electrònic.
h) Llei 59/2003, de 19 de desembre, de Signatura Electrònica.
i) Llei 25/2007, de 18 d'octubre, de Conservació de Dades Relatives a les Comunicacions Electròniques i a les Xarxes Públiques de Comunicacions.
j) Llei 37/2007, de 16 de novembre, sobre Reutilització de la Informació del Sector Públic.
k) Llei 56/2007, de 28 de desembre, de Mesures d'Impuls de la Societat de la Informació.
l) Llei 11/2022, de 28 de juny, General de Telecomunicacions.
m) Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
n) Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'administració electrònica.

Diputació Barcelona | https://bop.diba.cat | Pàg. 7-22 | CVE 202410127403 | Data 18-7-2024 | BOPB Butlletí Oficial de la Província de Barcelona

o) Ordenança Municipal per al govern i l'administració electrònica, en vigor des del 15 de març de 2019 (BOP de 20 de febrer de 2019).

p) Decret d'Alcaldia nun 1957 de 9 de març de 2018, d'aprovació de la Política de Seguretat de la Informació, designació dels membres del Comitè de Seguretat de la Informació, Responsable de Seguretat de la Informació i Responsable de Sistemes.

q) Decret 2158/2020,de 25 de febrer, pel qual es designa la Delegada de Protecció de Dades de l'Ajuntament de Terrassa i ens depenents.

5. Principis bàsics i requisits mínims

L'ENS determina una sèrie de principis bàsics i requisits mínims de seguretat que cal respectar i desenvolupar de forma proporcional a les característiques de la informació i dels serveis a protegir i tenint en compte la categoria dels sistemes afectats.

Seguretat com un procés integral (article 6) i Millora contínua del procés de seguretat (article 27)

La seguretat constitueix un procés integrat per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes. L'aplicació del ENS a l'Ajuntament de Terrassa estarà presidida per aquest principi, que exclou qualsevol actuació puntual o tractament circumstancial.

El procés integral de seguretat implantat haurà de ser actualitzat i millorat de manera contínua. Per a això, s'aplicaran els criteris i mètodes reconeguts en la pràctica nacional i internacional relatius a la gestió de la seguretat de les tecnologies de la informació.

Es prestarà la màxima atenció a la conscienciació de les persones que intervenen en el procés i als seus responsables jeràrquics, perquè, ni la ignorància, ni la falta d'organització i coordinació, ni instruccions inadequades, siguin font de risc per a la seguretat.

Mínim privilegi (article 20)

Els sistemes es dissenyaran i configuraran atorgant els mínims privilegis necessaris per al correcte exercici de les seves funcions, el que implica incorporar els següents aspectes:

- Els sistemes d'informació proporcionaran la funcionalitat mínima imprescindible perquè l'organització aconsegueixi els seus objectius competencials o contractuals.
- Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'assegurarà que només són desenvolupades per les persones autoritzades, des d'emplaçaments o equips així mateix autoritzats.
- S'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades a la finalitat que es persegueix. L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari.

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 2024101274O3 | Pàg. 8-22 | https://bop.diba.cat | Diputació Barcelona

Vigilància continua i reavaluació periòdica (article 10) i Integritat i actualització del sistema (Article 21)

La vigilància contínua permetrà la detecció d'activitats o comportaments anòmals i la seva oportuna resposta.

L'avaluació permanent de l'estat de la seguretat dels actius permetrà mesurar la seva evolució, detectant vulnerabilitats i identificant deficiències de configuració, i corregint-les aplicant les actualitzacions i modificacions necessàries.

Les mesures de seguretat es reavaluaran i actualitzaran periòdicament, adequant la seva eficàcia a l'evolució dels riscos i els sistemes de protecció, podent arribar a un replantejament de la seguretat, si fos necessari.

La inclusió de qualsevol element físic o lògic en el catàleg actualitzat d'actius del sistema, o la seva modificació, requerirà autorització formal prèvia.

Gestió de personal (article 15) i Professionalitat (article 16)

El personal, propi o aliè, relacionat amb els sistemes d'informació de l'Ajuntament de Terrassa, haurà de ser format i informat dels seus deures, obligacions i responsabilitats en matèria de seguretat.

El personal, en l'acompliment de les seves funcions, aplicarà les normes i procediments operatius de seguretat aprovats, i la seva actuació haurà de ser supervisada per a verificar que així sigui.

S'establirà un programa de conscienciació contínua per a tot el personal de l'Ajuntament, en particular per als de nova incorporació, incloent formació periòdica en matèria de seguretat de la informació i en l'ús segur dels sistemes d'informació.
El significat i abast de l'ús segur dels sistemes d'informació es concretarà i plasmarà en unes normes de seguretat que seran aprovades pel Comitè de Seguretat de la Informació i que tot el personal haurà d'aplicar en l'acompliment de les seves funcions.

La seguretat dels sistemes d'informació estarà atesa i serà revisada i auditada, en totes les fases del seu cicle de vida per personal degudament qualificat, dedicat i instruït.

L'Ajuntament de Terrassa exigirà, de manera objectiva i no discriminatòria, que les organitzacions que els prestin serveis de seguretat comptin amb professionals qualificats i amb uns nivells idonis de gestió i maduresa en els serveis prestats.

L'Ajuntament de Terrassa determinarà els requisits de formació i experiència necessària del personal per al desenvolupament del seu lloc de treball.

Gestió de la seguretat basada en els riscos (article 7) i Anàlisi i gestió de riscos (article 14)

L'anàlisi i la gestió dels riscos és part essencial del procés de seguretat, havent de constituir una activitat contínua i permanentment actualitzada.

La gestió dels riscos permetrà el manteniment d'un entorn controlat, minimitzant els riscos a nivells acceptables. La reducció a aquests nivells es realitzarà mitjançant una apropiada aplicació de mesures de seguretat, de manera equilibrada i proporcionada a la naturalesa de la informació tractada, dels serveis a prestar i dels riscos als quals estiguin exposats.

L'Ajuntament de Terrassa realitzarà periòdicament l'anàlisi i tractament dels riscos de tots els sistemes afectats per aquesta Política de seguretat, emprant metodologies reconegudes internacionalment.

Incidents de seguretat (article 25), Prevenció, detecció, resposta i conservació (article 8)

L'Ajuntament de Terrassa disposarà de procediments de gestió d'incidents de seguretat que millorin la capacitat de resposta davant d'aquestes crisis i permetin afrontar-les de forma eficaç i eficient, amb l'objectiu de poder tornar a la normalitat amb les menors conseqüències per a l'organització i la ciutadania.

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 el mateix no es materialitzin o que, en el cas de fer-lo, no afectin greument la informació que gestiona o als serveis que presta.

Les mesures de prevenció, que podran 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 ciberincident. En el moment de detectar un incident de seguretat s'aplicaran criteris de classificació per decidir si la gravetat del mateix requereix o no la convocatòria del Comitè de Crisi.

Les mesures de resposta, que es gestionaran en temps oportú, estaran orientades a la restauració de la informació i els serveis que poguessin haver-se vist afectats per un incident de seguretat, així com a la comunicació que correspongui a les parts interessades, i al registre de les actuacions. Aquest registre s'emprarà per a la millora contínua de la seguretat del sistema.

Sense detriment dels restants principis bàsics i requisits mínims establerts, el sistema d'informació garantirà la conservació de les dades i informació en suport electrònic.

D'igual manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital, a través d'una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 20241012740 3 | Pàg. 10-22 | https://bop.diba.cat | Diputació Barcelona

Línies de defensa (article 9)

L'Ajuntament de Terrassa implementarà una estratègia de protecció constituïda per múltiples capes de seguretat, constituïdes per mesures organitzatives, físiques i lògiques, de manera que, quan una de les capes sigui compromesa, permeti:

a) Desenvolupar una reacció adequada enfront dels incidents que no han pogut evitar-se, reduint la probabilitat que el sistema sigui compromès en el seu conjunt.

b) Minimitzar l'impacte final sobre aquest.

Prevenció davant altres sistemes interconnectats (article 23)

Es protegirà el perímetre dels sistemes d'informació, especialment, si es connecten a xarxes públiques, reforçant-se les tasques de prevenció, detecció i resposta a incidents de seguretat.
En tot cas, s'analitzaran els riscos derivats de la interconnexió del sistema amb altres sistemes i es controlarà el seu punt d'unió.

Autorització i control dels accessos (article 17) i Registres d'activitat i detecció de codi maliciós (article 24)

L'accés controlat als sistemes d'informació estarà limitat als usuaris, processos, dispositius o altres sistemes d'informació, degudament autoritzats, i exclusivament a les funcions permeses.

A fi de preservar la seguretat dels sistemes d'informació i de conformitat amb la normativa sobre protecció de dades personals i el respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació allà enunciats, es registraran les activitats dels usuaris, retenint la informació estrictament necessària per a monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar a cada moment a la persona que actua. Així mateix es podran, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, de manera que sigui possible impedir accessos no autoritzats, atacs i danys a les xarxes i sistemes d'informació.

Per a corregir o, en el seu cas, exigir responsabilitats, cada usuari que accedeixi al sistema d'informació haurà d'estar identificat de manera única, de manera que se sàpiga, en tot moment, qui rep drets d'accés, de quin tipus són aquests, i qui ha realitzat una determinada activitat.

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 202410127403 | Pàg. 11-22 | https://bop.diba.cat | Diputació Barcelona

Protecció de les instal·lacions (article 18)

Els sistemes d'informació i la seva infraestructura de comunicacions associada hauran de romandre en àrees controlades i disposar dels mecanismes d'accés adequats i proporcionals en funció de l'anàlisi de riscos.

Adquisició de productes de seguretat i contractació de serveis de seguretat (article 19)

En l'adquisició de productes de seguretat o contractació de serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació s'utilitzaran, de forma proporcionada a la categoria del sistema i el nivell de seguretat determinats, aquells que tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició.

L'entitat de certificació preferent segons el ENS és l'Organisme de Certificació de l'Esquema Nacional d'Avaluació i Certificació de Seguretat de les Tecnologies de la Informació del Centre Criptològic Nacional. En cas que aquest organisme no hagi realitzat encara certificacions d'una determinada categoria de productes o serveis de seguretat, o per causa major, es podran seleccionar productes amb altres certificacions de seguretat reconegudes internacionalment, principalment la de Common Criteria.

L'ús de productes o serveis de seguretat certificats només es podrà obviar en aquells casos en què les exigències de proporcionalitat en quant als riscos assumits no ho justifiquin, segons el criteri del Comitè de Seguretat.

Protecció de la informació emmagatzemada i en trànsit (article 22) i continuïtat de l'activitat (article 26)

En l'organització i implantació de la seguretat es prestarà especial atenció a la informació emmagatzemada o en trànsit a través dels equips o dispositius portàtils o mòbils, els dispositius perifèrics, els suports d'informació i les comunicacions sobre xarxes obertes, que hauran d'analitzar-se especialment per a aconseguir una adequada protecció.

S'aplicaran procediments que garanteixin la recuperació i conservació a llarg termini dels documents electrònics produïts pels sistemes d'informació, quan això sigui exigible.

Tota informació en suport no electrònic que hagi estat causa o conseqüència directa de la informació electrònica, haurà d'estar protegida amb el mateix grau de seguretat que aquesta. Per a això, s'aplicaran les mesures que corresponguin a la naturalesa del suport, de conformitat amb les normes que resultin d'aplicació.

Els sistemes disposaran de còpies de seguretat i s'establiran els mecanismes necessaris per a garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals.

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 20241012740 3 | Pàg. 12-22 | https://bop.diba.cat | Diputació Barcelona

Compliment dels requisits mínims (article 28)

Per a donar compliment als requisits mínims establerts en el ENS, l'Ajuntament de Terrassa adoptarà les mesures i reforços de seguretat corresponents indicats en l'annex II del ENS, tenint en compte:

a) Els actius que constitueixen els sistemes d'informació implicats.

b) La categoria del sistema.

c) Les decisions que s'adoptin per a gestionar els riscos identificats.

Les mesures anteriors tindran la condició de mínims exigibles, sent ampliables a criteri del responsable de la seguretat, qui podrà incloure mesures addicionals, tenint en compte l'estat de la tecnologia, la naturalesa de la informació tractada o els serveis prestats i els riscos als que estan exposats els sistemes d'informació afectats. La relació de mesures de seguretat seleccionades es formalitzarà en un document denominat Declaració d'Aplicabilitat, signat pel responsable de la seguretat.

Les mesures de seguretat referenciades en l'annex II del ENS podran ser reemplaçades per altres compensatòries, sempre que es justifiqui documentalment que protegeixen, igual o millor, del risc sobre els actius i se satisfan els principis bàsics i els requisits mínims previstos en el ENS. Com a part integral de la Declaració d'Aplicabilitat s'indicarà, de manera detallada, la correspondència entre les mesures compensatòries implantades i les mesures de l'annex II del ENS que compensen.

6. Organització de la seguretat de la informació

6.1 Comitè de Seguretat de la Informació

El Comitè de Seguretat de la Informació és l'òrgan col·legiat que dirigeix, gestiona, coordina, estableix i aprova les actuacions en matèria de seguretat de la informació. Aquest Comitè estarà composat per les persones següents:

- Regidor/a o tinent d'alcalde que tingui atribuïdes les competències municipals en matèria de Tecnologia i Sistemes d'Informació (President/a del Comitè)
- Secretari/a General
- Interventor/a
- Tresorer/a
- Coordinador/a general
- Director/a d'Àrea en que es trobi circumscrit el servei de Tecnologia i Sistemes d'Informació

- Director/a dels Serveis de Secretaria d'Empreses i Grans Contractes
- Delegat/da de Protecció de Dades
- Director/a serveis de Tecnologia i Sistemes d'Informació
- Responsable de Seguretat de la Informació, que actuarà com a secretari o secretària.
- Responsable de Sistemes.

Les decisions del Comitè de Seguretat es prendran per majoria. En cas d'empat el vot de la presidència serà de qualitat.

El Comitè es reunirà periòdicament, com a mínim semestralment.

Amb caràcter opcional, altres membres de l'organització, podran incorporar-se a petició del Comitè a les reunions i/o tasques del Comitè, inclosos grups de treball especialitzats, ja siguin de caràcter intern, extern o mixt.

Tots els serveis i unitats de l'Ajuntament de Terrassa estaran obligats a informar i donar suport al Comitè de Seguretat de la Informació quan aquest així ho requereixi.

El Comitè de Seguretat de la Informació tindrà informats als Òrgans de Govern.

El Comitè té les següents funcions i responsabilitats concretes:

- Elaborar i impulsar l'estratègia i noves línies de treball pel que fa a la Seguretat de la Informació.
- Atendre les sol·licituds de l'organització i assessorar-la en matèria de Seguretat de la Informació.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents rols implicats en la Seguretat de la Informació o en l'aplicació de les diferents normatives de Seguretat de la Informació aprovades a l'Ajuntament de Terrassa, incloent aquesta Política.
- Promoure la millora contínua del sistema de gestió de la seguretat de la informació. Amb aquesta finalitat s'encarregarà de:
    - Coordinar els esforços de les diferents àrees en matèria de Seguretat de la Informació, per assegurar que aquests siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
    - Proposar plans de millora de la Seguretat de la Informació i procurar que se'ls hi assigni una dotació pressupostària adequada, prioritzant les actuacions en matèria de seguretat quan els recursos siguin limitats.
    - Supervisar i aprovar les tasques d'implantació del ENS per avançar en el seu compliment.
    - Vetllar per a què la Seguretat de la Informació sigui un eix fonamental de tots els projectes des de la seva especificació inicial fins a la posada en operació. En particular haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i suportin un funcionament homogeni de tots els

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 2024101274O3 | Pàg. 14-22 | https://bop.diba.cat | Diputació Barcelona

sistemes TIC.

- Realitzar un seguiment dels principals riscos residuals assumits per l'Ajuntament de Terrassa i recomanar possibles actuacions respecte a ells.
- Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte a ells.
- Elaborar i revisar regularment la Política de Seguretat de la Informació per a la seva aprovació per l'òrgan competent.
- Revisar i aprovar les normatives i procediments de Seguretat presentats pel Responsable de Seguretat que dicti la Norma per a la Gestió de la Documentació.
- Elaborar programes de formació destinats a formar i sensibilitzar al personal en matèria de Seguretat de la Informació i en particular en matèria de protecció de dades de caràcter personal.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de la Seguretat de la Informació.
- Promoure la realització de les auditories periòdiques del ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l'Ajuntament de Terrassa en matèria de Seguretat de la Informació.

Addicionalment, el Comitè de Seguretat de la Informació assumeix els rols de Responsable de la Informació i Responsable dels Serveis que estableix el ENS, i per tant les seves funcions associades, entre les quals:

a) Determinar i aprovar els requisits de seguretat aplicables a la informació tractada i als serveis prestats, segons els paràmetres de l'annex I del ENS.

b) Acceptar els nivells de risc residual que afectin als serveis i a la informació.

6.2 Grup de treball tècnic

Donat que el Comitè de Seguretat no es podrà reunir amb la freqüència desitjable per a la gestió contínua de la Seguretat de la Informació, es crearà un grup de treball tècnic.

El grup de treball tècnic realitzarà una gestió més freqüent i a nivell més operatiu de la Seguretat de la Informació que el que efectua el Comitè de Seguretat.

Aquest grup es reunirà mensualment per revisar els temes que requereixin atenció en matèria de Seguretat de la Informació, prendre les decisions adients, i impulsar l'execució de les resolucions del Comitè de Seguretat.

El grup de treball dependrà del Comitè de Seguretat, que supervisarà les seves decisions.

Aquest grup de treball estarà composat per les persones següents:

- Director/a de Tecnologia i Sistemes d'Informació

- Responsable de Seguretat, que actuarà com a secretari o secretària
- Responsable de Sistemes
- Tècnics de seguretat
- El cap de Processos en totes les reunions on es tractin temes de la seva competència o afectació

En aquestes reunions es podran afegir altres persones, d'acord amb els assumptes a tractar i a petició dels membres del grup de treball.

6.3 Comitè de crisi de la Seguretat de la Informació

El Comitè de Crisi de la Seguretat de la Informació és l'òrgan que s'activarà davant incidents de seguretat d'especial gravetat i impacte que siguin qualificats com a crisi. El pla de gestió de ciberincidents corporatiu determinarà exactament quins incidents de seguretat requereixen de l'activació d'aquest Comitè, com es realitzarà aquesta activació i altres detalls sobre el seu funcionament.

El Comitè de crisi és l'òrgan encarregat de prendre les decisions i coordinar les accions necessàries per a la resolució de la crisi en tots els seus aspectes. Les seves funcions són:

- Avaluar la informació rebuda sobre l'incident i fer una valoració inicial del seu impacte.
- Realitzar previsions dels escenaris als que pot evolucionar l'incident per prendre mesures preventives.
- Determinar, validar i supervisar les estratègies i mesures implementades i/o proposades per l'equip de resposta a incidents.
- Determinar les prioritats per recuperar les activitats i serveis en el menor temps possible.
- Activar la mobilització de recursos extraordinaris quan sigui necessari.
- Assumir la responsabilitat de la comunicació i assegurar la interlocució amb totes les parts interessades i afectades internes o externes a l'organització.
- Definir l'estratègia de comunicació.
- Un cop finalitzada la crisi, extraure lliçons apresses i punts de millora i reportar-los al Comitè de Seguretat per a que s'executi el pla d'acció resultant.

La composició d'aquest Comitè pot variar depenent de les característiques de cada crisi, però, en general, estarà composat per següents figures:

- Alcalde/ssa o bé Regidor/a de Tecnologia i Sistemes d'Informació (President/a)
- Secretari/a General
- Interventor/a

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 2024101274O3 | Pàg. 16-22 | https://bop.diba.cat | Diputació Barcelona

- Tresorer/a
- Coordinador/a general
- Director/a d'Àrea en que es trobi circumscrit el servei de Tecnologia i Sistemes d'Informació
- Delegat/da de Protecció de Dades
- Responsable de Serveis Jurídics
- Director/a dels Serveis de Secretaria d'Empreses i Grans Contractes
- Director/a de Tecnologia i Sistemes d'Informació
- Responsable de Seguretat, que actuarà com a secretari o secretària.
- Responsable de Sistemes.
- Responsables de Comunicació: Comunicació externa, Comunicació Interna, Premsa i Xarxes Socials.
- Responsables dels serveis afectats
- En cas d'incidents molt greus, s'afegiran al comitè de crisi responsables de l'Agència de Ciberseguretat de Catalunya

6.4 Rols de seguretat de la informació

6.4.1 Responsables d'informació i/o serveis

Les figures del Responsable de la informació i el Responsable dels serveis són assumides pel Comitè de Seguretat de la Informació, de forma que el Comitè s'atribueix les funcions associades a aquestes figures, com es detalla a l'apartat 6.1.

6.4.2 Responsable de seguretat de la Informació

La figura del Responsable de Seguretat de la Informació té les següents funcions i responsabilitats:

- Mantenir i verificar el nivell adequat de seguretat de la informació gestionada i dels serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la declaració d'aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries, elaborar documentació del sistema.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el Responsable del Sistema i/o Comitè de Seguretat de la Informació.

Diputació Barcelona
https://bop.diba.cat
Pàg. 17-22
CVE 2024101274O3
Data 18-7-2024
BOPB Butlletí Oficial de la Província de Barcelona

- Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comitè de Seguretat l'aprovació de normatives, instruccions tècniques, canvis i altres requisits del sistema que consideri necessaris.
- Acordar, juntament amb el Responsable del Sistema, la suspensió de l'accés a determinada informació o la prestació de determinat servei si es té coneixement de que presenten deficiències greus de seguretat.
- Realitzar informes sobre les incidències greus produïdes per a la seva posterior presentació al Comitè de Seguretat de la Informació.

6.4.3 Responsable de Sistemes

La figura del o la Responsable dels Sistemes tindrà definides les següents funcions i responsabilitats:

- Paralitzar o donar suspensió a l'accés a determinada informació o la prestació de determinat servei si té el coneixement que aquests presenten deficiències greus de seguretat.
- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida.
- Elaborar els procediments operatius necessaris.
- Definir la topologia i la gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en aquest.
- Satisfer els requisits de seguretat del Sistema d'Informació implementant les mesures de seguretat estipulades pel Responsable de Seguretat i/o el Comitè de Seguretat.
- Comprovar que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Donar assessorament al Responsable de Seguretat de la Informació per a la determinació de la Categoria del Sistema.
- Col·laborar, si així se li requereix, en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat.
- Dur a terme les funcions de l'administrador de la seguretat del sistema:
    - La gestió, configuració i actualització, si és el cas, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
    - La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la seva correspondència amb l'autoritzat.
    - Aprovar els canvis en la configuració vigent del Sistema d'Informació.

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 2024101274O3 | Pàg. 18-22 | https://bop.diba.cat | Diputació Barcelona

- Assegurar que els controls de seguretat establerts són complerts estrictament.
- Assegurar que són aplicats els procediments aprovats per a gestionar el Sistema d'Informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

Quan la complexitat del sistema ho justifiqui, el Responsable de Sistema podrà designar els responsables de sistema delegats que consideri necessaris, que tindran dependència funcional directa d'ell i seran responsables en el seu àmbit de totes aquelles accions que els delegui. D'igual mode, també podrà delegar en un altre/s funcions concretes de les responsabilitats que se li atribueixen.

6.5 Procediments de designació

La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants i la designació dels Responsables identificats en aquesta Política ha estat realitzada per Alcaldia de l'Ajuntament de Terrassa i comunicada degudament a les parts afectades.

Els membres del Comitè, així com els rols de seguretat podran seran revisats a cada inici de mandat o en ocasió de vacant, o en cas de qualsevol circumstància que impedeixi que els membres del Comitè puguin continuar desenvolupant el seu càrrec.

6.6 Resolució de conflictes

El Comitè de Seguretat de la Informació s'encarregarà de la resolució dels conflictes i/o diferencies d'opinions que puguin sorgir entre els diferents rols de seguretat.

7. Dades de caràcter personal

L'Ajuntament de Terrassa, en el tractament de les dades personals, compleix amb els principis i obligacions de la normativa vigent, entre una altra el Reglament 679/2016, 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-RGPD-) i la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia de drets digitals, respectant, en tot cas, el dret fonamental a la protecció de dades personals, la intimitat i la resta dels drets fonamentals reconeguts tant en la legislació i tractats internacionals com en la Constitució vigent.

En desenvolupament dels principis de la vigent normativa de protecció de dades, entre altres, els de minimització, confidencialitat o proactivitat, l'Ajuntament ha definit una Política de Protecció de Dades i condicions generals de l'ús de terrassa.cat publicades a la seu electrònica municipal amb accés públic a l'adreça https://www.terrassa.cat/es/protecciodades.

8. Desenvolupament de la política de seguretat de la informació

El compliment dels objectius marcats en aquesta Política de Seguretat es duu a terme mitjançant el desenvolupament de documentació que constitueixen les normes i procediments de seguretat associats al compliment de l'Esquema Nacional de Seguretat. Per a la seva organització s'ha definit una Norma per a la Gestió de la Documentació, que estableix les directrius per a l'organització, gestió i accés.

La revisió anual de la present Política correspon al Comitè de Seguretat de la Informació proposant en cas que sigui necessari millores d'aquesta, per a la seva aprovació per part del mateix òrgan que la va aprovar inicialment.

9. Obligacions del personal

Tots els membres de l'Ajuntament de Terrassa i de les societats municipals adscrites a aquesta Política tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi als interessats.

10. Terceres parts

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

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 20241012740 3 | Pàg. 20-22 | https://bop.diba.cat | Diputació Barcelona

Quan l'Ajuntament de Terrassa utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat en els punts que concerneixi a aquests serveis o informació, i hauran de complir les instruccions de l'encàrrec de tractament de dades que específicament estableixi l'Ajuntament quan hi hagi cessió de dades o informació a tercers per l'encàrrec de serveis externs. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la. Així mateix s'establiran procediments específics de comunicació 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.

Segons el que es disposa a la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat, els operadors del sector privat que prestin serveis o proveeixin solucions a les entitats públiques, a les quals resulti exigible el compliment de l'Esquema Nacional de Seguretat, hauran d'estar en condicions d'exhibir la corresponent Declaració de Conformitat amb l'Esquema Nacional de Seguretat quan es tracti de sistemes de categoria BÀSICA, o la Certificació de Conformitat amb l'Esquema Nacional de Seguretat, quan es tracti de sistemes de categories MITJANA o ALTA.

Els contractes o convenis que es subscriguin a partir de l'entrada en vigor d'aquesta Política hauran de contenir una clàusula que estableixi l'obligació de complir aquesta Política segons s'especifica en els paràgrafs anteriors, el sistema de verificació del seu compliment i incloure un acord de confidencialitat.

Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es sol·licitarà un informe al Responsable de Seguretat de la Informació on es detallin els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats, o pel Comitè de Seguretat quan aquest actuï com a responsable, abans de seguir endavant.

11. Aprovació i entrada en vigor

L'article 2.3 en relació amb l'article 12 del Real Decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de seguretat, determina que la política de seguretat serà aprovada per l'òrgan competent que ostenti les màximes competències executives. Conseqüentment, i d'acord amb el que preveu l'article 21.1.4) de la Llei Reguladora de les Bases de Règim Local, que assigna a l'Alcalde les atribucions per ordenar l'execució i fer complir els acords de l'ajuntament, serà aquest l'òrgan competent de forma originària. Atenent aquesta previsió legal, el present document ha estat aprovat per l'Alcalde -

President de l'Ajuntament de Terrassa, derogant la Política de Seguretat de la informació aprovada per Decret d'Alcaldia núm. 1957, de 9 de març de 2018, i mantindrà la seva vigència mentre no es produeixi la seva modificació i/o derogació.

S'autoritza a l'òrgan amb competències en matèria de tecnologies de la informació i d'acord amb les previsions de la present política per dictar quantes disposicions siguin necessàries per l'aplicació i execució d'aquesta Política de Seguretat de la Informació.

BOPB Butlletí Oficial de la Província de Barcelona | Data 18-7-2024 | CVE 20241012740 3 | Pàg. 22-22 | https://bop.diba.cat | Diputació Barcelona