Política de seguretat de la informació

• *1. APROVACIÓ I ENTRADA EN VIGOR*

Text aprovat el dia 20 de gener de 2022 per decret d'Alcaldia de l'Ajuntament de Granollers .

Aquesta "Política de Seguretat de la Informació", en endavant Política, serà efectiva des de la data esmentada i fins que sigui reemplaçada per una nova Política.

• *2. INTRODUCCIÓ*

L'Ajuntament de Granollers 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 la activitat diària i reaccionant amb prestesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i 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. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els diferents departaments han de assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva 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, d'acord amb l'article 7 de l'ENS (Esquema Nacional de Seguretat).

• *3. MISSIÓ DE L'AJUNTAMENT DE GRANOLLERS*

El 2019 l'Ajuntament de Granollers va alinear tot el seu pla de mandat amb els Objectius de Desenvolupament Sostenible (ODS). La voluntat és avançar en un model de ciutat inclusiva, transformadora, compromesa i sostenible. En aquesta línia, un dels eixos

principals és el de definir un model d'administració oberta i participativa, que doni accés a la ciutadania a la informació i als serveis.

• *4. ABAST*

Aquesta Política s'aplicarà als sistemes d'informació de l'Ajuntament de Granollers i Organismes Autònoms (Patronat Museu de Granollers, Granollers Escena SL, Granollers Promocions SA, Consorci Montserrat Montero, Consorci Teledigital de la demarcació de Granollers, Granollers Mercat EPE i Roca Umbert Fàbrica de les Arts SL), que estiguin 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 i que es troben dintre de l'abast de l'Esquema Nacional de Seguretat (ENS).

• *5. MARC NORMATIU*

La base normativa que afecta el desenvolupament de les activitats i competències del Ajuntament de Granollers, pel que fa a administració electrònica es refereix, i que implica la implantació de forma explícita de mesures de seguretat en els sistemes d'informació, està constituïda per la legislació següent:

- *Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les administracions públiques.*
- *Llei 40/2015, de l'1 d'octubre, de Règim Jurídic del Sector Públic.*
- *Reial Decret 3/2010, del 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat a l'àmbit de l'administració electrònica, modificat per Reial Decret 951/2015, del 23 d'octubre.*
- *Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat de Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de conformitat amb l´Esquema Nacional de Seguretat.*
- *Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat de Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Informe de l'Estat de la seguretat.*
- *Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, pel qual aprova la Instrucció Tècnica de Seguretat d'Auditoria de la seguretat dels sistemes d'informació.*
- *Resolució de 13 d'abril del 2018, de la Secretaria d'Estat de Funció Públic, pel qual aprova la Instrucció Tècnica de Seguretat Notificació d'incidents de seguretat.*
- *Reial Decret 4/2010 de 8 de gener, que regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.*
- *Reial Decret 1671/2009, de 6 de novembre, pel que es desenvolupa parcialment la Llei 11/2007, de 22 de juny d'accés electrònic dels ciutadans als serveis públics.*
- *Els articles 23 i 24 de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.*

» *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 que es deroga la Directiva 95/46/CE (Reglament general de protecció de dades, RGPD).*

» *Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.*

» *Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.*

» *Llei 19/2013, del 9 de desembre, de transparència, accés a la informació pública i bon govern.*

» *Llei 25/2007, de 18 d'octubre, relativa a la conservació de dades relatives a comunicacions electròniques i a les xarxes públiques de comunicacions.*

» *Llei 56/2007, de 28 de desembre, de Mesures de Foment de la Societat de la Informació.*

» *Llei 9/2014, del 9 de maig, General de Telecomunicacions.*

» *Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local, modificada per la llei 11/1999, de 21 d'abril.*

» *Reial Decret Legislatiu 1/1996, de 12 d'abril, que aprova el Text Refós de la Llei de propietat intel·lectual.*

» *Reial Decret Legislatiu 5/2015 de 30 d'octubre, que aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic.*

» *Llei 59/2003, del 19 de desembre, de signatura electrònica.*

» *Reial Decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.*

» *Text refós de la Llei de Contractes de Sector Públic, aprovat pel Reial Decret legislatiu 3/2011, de 14 de novembre, i la normativa de desenvolupament.*

» *Reial decret llei 14/2019, de 31 d'octubre, mitjançant l'adopció de mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions.*

» *Política de signatura electrònica de l'Ajuntament de Granollers*

» *Reglament pel qual s'estableix la Seu Electrònica de l'Ajuntament de Granollers*

També formen part del marc normatiu les restants normes aplicables a l'Administració Electrònica de l'Ajuntament de Granollers, derivat de l'anterior i publicat en les seus electròniques incloses dins de l'àmbit d'aplicació de la present Política.

El manteniment del marc normatiu serà responsabilitat de l'Ajuntament de Granollers, i es mantindrà en un Annex a aquest document. Incloses les instruccions tècniques de seguretat de compliment obligat, publicades per resolució de la Secretaria d'Estat d'Administracions Públiques i aprovat pel Ministeri d'Hisenda i Administracions Públiques, a proposta del Comitè Sectorial d'Administració Electrònica i la iniciativa del Centre Criptològic Nacional (CCN) tal com s'estableix al "Article 29. Instruccions tècniques de seguretat i guies de seguretat".

Així mateix, l'Ajuntament de Granollers, també serà responsable d'identificar les guies de seguretat del CCN, referenciades a l'article mencionat, que s'aplicarà a millorar el compliment del que està establert en l'Esquema Nacional de Seguretat.

• 6. COMPLIMENT

L'Ajuntament de Granollers, per assolir el compliment dels articles 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, que recullen els principis bàsics i els requisits mínims, implementarà diverses mesures de seguretat proporcionals a la naturalesa de la informació i els serveis a protegir i tenint en compte la categoria dels sistemes afectats, mesures que seguidament es descriuen.

• 6.1 Seguretat com un procés integral i seguretat per defecte

La seguretat constitueix un procés integrat per tots els elements tècnics, humans, materials i organitzatius, relacionats amb el sistema. L'aplicació de l'Esquema Nacional de Seguretat a l'Ajuntament de Granollers, estarà presidida per aquest principi, que exclou qualsevol actuació puntual o tractament conjuntural.

Es prestarà la màxima atenció a donar a conèixer als implicats en el procés i als seus responsables jeràrquics, perquè, ni la ignorància, ni la manca d'organització o coordinació, ni instruccions inadequades, siguin una font de risc per la seguretat.

Els sistemes seran dissenyats de tal manera que es garanteixi la seguretat per defecte, de la següent manera:

- *a El sistema proporcionarà la mínima funcionalitat requerida perquè l'organització assoleixi els seus objectius.*
- *b Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'assegurarà que només són accessibles per les persones, o des d'emplaçaments o equips, autoritzats, podent exigir-se si és el cas restriccions de temps i punts d'accés facultats.*
- *c En un sistema d'explotació s'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que no siguin d'interès, siguin innecessàries i, fins i tot, aquelles que siguin inadequades pel fi que persegueix.*
- *d 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.*

• 6.2 Reavaluació periòdica i integritat i actualització del sistema

L'Ajuntament de Granollers implementarà controls i avaluacions regulars de la seguretat, (incloent avaluacions dels canvis de configuració de forma rutinària), per conèixer en tot moment l'estat de la seguretat dels sistemes en relació a les especificacions dels fabricants, a

les vulnerabilitats i a les actualitzacions que els afectin, reaccionant amb diligència per gestionar el risc a la vista de l'estat de seguretat dels mateixos. Abans de l'entrada de nous elements, ja siguin físics o lògics, aquests requeriran d'una autorització formal.

Així mateix, es sol·licitarà la revisió periòdica per part de tercers per tal d'obtenir una avaluació independent.

- ***6.3 Gestió de personal i professionalitat***

Tots els membres de l'Ajuntament de Granollers, dins de l'àmbit de l'ENS, assistiran a una sessió de conscienciació en matèria de seguretat com a mínim un cop l'any. S'establirà un programa de sensibilització contínua per atendre a tots els membres, en particular els de nova incorporació.

Les persones amb responsabilitat per 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 seva feina. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

- ***6.4 Gestió de la seguretat basada en els riscos i anàlisi i gestió de riscos***

Tots els sistemes afectats per aquesta Política de Seguretat, així com tots els tractaments de dades personals, hauran de ser objecte d'una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats. Aquesta anàlisi es repetirà:

» *Regularment, almenys un cop a l'any.*

» *Quan canviïn la informació manejada i/o els serveis prestats de manera significativa.*

» *Quan es produeixi un incident greu de seguretat o es detectin vulnerabilitats greus.*

El Responsable de Seguretat de l'ENS serà l'encarregat de fer l'anàlisi de riscos, així com d'identificar mancances i debilitats i posar-les en coneixement del Comitè de Seguretat de la Informació.

- ***6.5 Incidents de seguretat, prevenció, reacció i recuperació***

L'Ajuntament de Granollers, implementarà un procés integral de detecció, reacció i recuperació davant de codi nociu mitjançant el desenvolupament de procediments que cobreixen els mecanismes de detecció, els criteris de classificació, els procediments d'anàlisi i resolució, així com les vies de comunicació a les parts interessades i el registre de les actuacions. Aquest registre s'emprarà per a la millora contínua de la seguretat del sistema.

Perquè la informació i/o els serveis no es vegin perjudicats per incidents de seguretat, l'Ajuntament de Granollers implementarà les mesures de seguretat establertes per l'ENS, així com qualsevol altre control addicional, que hagi identificat com a necessari, mitjançant

una avaluació d'amenaces i riscos. Aquests controls, així com els rols i responsabilitats de seguretat de tot el personal, estaran clarament definits i documentats.

Quan es produeixi una desviació significativa dels paràmetres que hi hagi preestablerts com a normals, s'establiran els mecanismes de detecció, anàlisi i comunicació necessaris perquè arribin als responsables regularment.

L'Ajuntament de Granollers establirà les següents mesures de reacció davant d'incidents de seguretat:

- *Mecanismes per respondre eficaçment als incidents de seguretat.*
- *Designar un 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).*
- *Per garantir la disponibilitat dels serveis, l'Ajuntament de Granollers disposarà dels mitjans i tècniques necessàries que permeten garantir la recuperació dels serveis més crítics.*

- ***6.6 Línies de defensa i prevenció davant d'altres sistemes interconnectats***

L'Ajuntament de Granollers implementarà una estratègia de protecció basada en múltiples capes, constituïdes per mesures organitzatives, físiques i lògiques, de manera que quan una de les capes falli, el sistema implementat permeti:

- *Guanyar temps per a una reacció adequada davant dels incidents que no han pogut evitar-se.*
- *Reduir la probabilitat que el sistema sigui compromès en conjunt.*
- *Minimitzar-ne l'impacte final.*

Aquesta estratègia de protecció ha de protegir el perímetre, en particular, si es connecta a xarxes públiques. En tot cas s'analitzaran els riscos derivats de la interconnexió del sistema, a través de xarxes, amb altres sistemes, i se'n controlarà el punt d'unió.

- ***6.7 Funció diferenciada i organització i implantació del procés de seguretat***

L'Ajuntament de Granollers organitzarà la seguretat comprometent a tots els membres de la corporació mitjançant la designació de diferents rols de seguretat amb responsabilitats clarament diferenciades, tal i com es recull a l'apartat "ORGANITZACIÓ DE LA SEGURETAT" del present document.

- ***6.8 Autorització i control dels accessos***

L'Ajuntament de Granollers implementarà mecanismes de control d'accés al sistema d'informació, limitant-los als estrictament necessaris i degudament autoritzats.

- ***6.9 Protecció de les instal·lacions***

L'Ajuntament de Granollers implementarà mecanismes de control d'accés físic, prevenint els accessos físics no autoritzats, així com els danys a la informació i als recursos, mitjançant perímetres de seguretat, controls físics i proteccions generals en àrees.

- ***6.10 Adquisició de productes de seguretat i contractació de serveis de seguretat***

Per la adquisició de productes, l'Ajuntament de Granollers tindrà en compte que aquests productes tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició, excepte en aquells casos en què les exigències de proporcionalitat quant als riscos assumits no ho justifiquin, segons el parer del Responsable de Seguretat.

- ***6.11 Protecció de la informació emmagatzemada i en trànsit i continuïtat de l'activitat***

L'Ajuntament de Granollers implementarà mecanismes per protegir la informació emmagatzemada o en trànsit, especialment quan aquesta es troba en entorns insegurs (portàtils, tauletes, suports d'informació, xarxes obertes, etc.).

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

Es desenvoluparan procediments que assegurin la recuperació i conservació a llarg termini dels documents electrònics produïts en l'àmbit de les competències de l'Ajuntament de Granollers. De la mateixa manera, s'implementaran mecanismes de seguretat en la base a la naturalesa del suport en què es trobin els documents, per garantir que tota informació relacionada en suport no electrònic estigui protegida amb el mateix grau de seguretat que la electrònica.

- ***6.12 Registres d'activitat***

L'Ajuntament de Granollers habilitarà registres de l'activitat dels usuaris retenint la informació necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar a cada moment a la persona que actua. Tot això amb la finalitat exclusiva d'aconseguir el compliment de l'objecte del Reial decret que regula l'ENS, amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge dels afectats, i d'acord amb la normativa sobre protecció de dades personals, de funció pública o laboral, i altres disposicions que siguin aplicables.

• *7. ORGANITZACIÓ DE LA SEGURETAT*

L'organització de la seguretat de la informació a l'Ajuntament de Granollers s'estableix en la forma que s'indica a continuació.

• *7.1. Rols o perfils de seguretat*

Per garantir el compliment i l'adaptació de les mesures exigides reglamentàriament, es crearan els rols o perfils de seguretat següents i es designaran els càrrecs o òrgans que els ocuparan:

» *Delegat de Protecció de Dades (DPD)*

» *Responsable de Seguretat*

» *Responsable del Sistema*

» *Responsable/s de la Informació*

» *Responsable/s dels Serveis*

• *7.2. Comitè de Seguretat de la Informació*

L'Ajuntament de Granollers constituirà un Comitè de Seguretat de la Informació, com a òrgan col·legiat, format pels següents membres:

Composició

» *President: el regidor de Sistemes Tecnològics i Societat del Coneixement*

» *Secretari: el Responsable de Seguretat*

» *Vocals:*

- *Delegat de Protecció de Dades*
- *Responsable de Seguretat*
- *Responsable del Sistema*
- *Gerent*
- *Director de Serveis Tecnològics i Societat del Coneixement*
- *Director de RRHH i Organització*
- *Responsable tècnic de Protecció de Dades*
- *La persona responsable de transparència*

Els Responsables de la Informació i dels Serveis seran convocats en funció dels assumptes a tractar.

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

El Comitè de Seguretat de la Informació celebrarà les seves sessions a les dependències de l'Ajuntament de Granollers amb periodicitat semestral prèvia convocatòria a aquest efecte realitzada pel President del Comitè esmentat, o de forma excepcional per produir-se un incident de seguretat o alteració important que pugui afectar a la mateixa

7.3. Responsabilitats associades al Marc de Seguretat

A continuació, es detallen i s'estableixen les funcions i les responsabilitats de cada una de les funcions de seguretat de l'ENS:

7.3.1 Funcions del Responsable de la Informació i dels Serveis

- *Establir i aprovar els requisits de seguretat aplicables al servei i la informació dins del marc establert a l'annex I del Reial decret 3/2010, de 8 de gener, prèvia proposta al Responsable de Seguretat ENS i/o Comitè de Seguretat de la Informació*
- *Acceptar els nivells de risc residual que afectin el Servei i la Informació.*

7.3.2 Funcions del Responsable de Seguretat

- *Mantenir i verificar el nivell adequat de seguretat de la informació manejada 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.*
- *Participar en l'elaboració i la 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 d'auditoria i certificació.*
- *Elevar al Comitè de Seguretat l'aprovació de canvis i altres requisits del sistema.*

El Responsable de Seguretat, en funció de la complexitat de l'organització, podrà proposar delegats de les seves funcions per àrees diferenciades que seran designats per l'Alcaldia o Regidoria delegada. Aquests delegats tindran dependència funcional directa i seran responsables en l'àmbit assignat.

7.3.3 Funcions del Responsable del Sistema

- *Paralitzar o donar suspensió a l'accés a informació o prestació de servei si en té coneixement que aquests presenten deficiències greus de seguretat.*

» *Desenvolupar, operar i mantenir el sistema d'informació durant tot el 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.*

» *Assegurar que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.*

» *Prestar el Responsable de Seguretat de la Informació i/o el Comitè de Seguretat assessorament per a la determinació de la categoria del sistema.*

» *Col·laborar, si així se'l requereix, en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, als plans de continuïtat.*

» *Dur a terme les funcions de l'administrador de la seguretat del sistema:*

- *La gestió, configuració i actualització, si escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat.*
- *La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent el monitoratge de l'activitat desenvolupada en el sistema i la seva correspondència amb allò autoritzat.*
- *Aprovar els canvis a la configuració vigent del Sistema d'Informació.*
- *Assegurar que els controls de seguretat establerts són complerts estrictament.*
- *Assegurar que són aplicats els procediments aprovats per manejar el Sistema d'Informació.*
- *Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.*
- *Monitoritzar 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 del Sistema podrà proposar els responsables de sistema delegats que consideri necessaris, designats per l'Alcaldia o Regidoria delegada, que tindran dependència funcional directa d'aquell i seran responsables en el seu àmbit de totes aquelles accions que els delegui el mateix. De la mateixa manera, també podrà delegar a altres funcions concretes de les responsabilitats que se li atribueixen.

7.4 Funcions del Comitè de Seguretat de la Informació

El Comitè de Seguretat tindrà les funcions següents:

» *Atendre les sol·licituds, en matèria de Seguretat de la Informació, de la Administració i dels diferents rols de seguretat i/o àrees informant regularment de l'estat de la seguretat de la informació.*

» *Assessorar en matèria de seguretat de la informació.*

» *Resoldre els conflictes de responsabilitat que puguin aparèixer entre les diferents unitats administratives.*

» *Promoure la millora contínua del sistema de gestió de la seguretat de la informació. Per això 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, amb la seva dotació pressupostària corresponent, prioritzant les actuacions en matèria de seguretat quan els recursos siguin limitats.*
- *Vetllar perquè la seguretat de la informació es tingui en compte a 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 donin suport a un funcionament homogeni de tots els sistemes TIC.*
- *Realitzar un seguiment dels principals riscos residuals assumits per l'Administració i recomanar possibles actuacions respecte d'ells.*
- *Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'ells.*
- *Elaborar i revisar regularment la Política de Seguretat de la Informació per aprovar-la l'òrgan competent.*
- *Elaborar i revisar regularment la Normativa de Seguretat de la Informació per a la seva aprovació.*
- *Elaborar i revisar regularment els Procediments de Seguretat de la informació i altre documentació per a la seva aprovació.*
- *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 de l'ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l'Administració en matèria de seguretat de la informació.*

7.5. 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 es realitzarà per decret o resolució de l'òrgan competent.

Els membres del Comitè, així com els rols de seguretat seran revisats cada 4 anys o amb ocasió de vacant.

7.6. Resolució de conflictes

El President del Comitè de Seguretat s'encarregarà de la resolució dels conflictes i/o diferències d'opinions que poguessin sorgir entre els rols de seguretat.

8. DADES DE CARÀCTER PERSONAL

Les mesures de seguretat a implantar només recolliran dades de caràcter personal quan siguin adequades, pertinents i no excessives i aquestes es trobin en relació amb l'àmbit i les finalitats per les que s'hagin obtingut. De la mateixa manera, s'adoptaran les mesures de caire tècnic i organitzatives necessàries per al compliment de la normativa de protecció de dades vigent en cada cas.

En vista de l'entrada en aplicació, el 25 de maig de 2018, del 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 que es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) i la seva translació a la legislació espanyola amb la Llei Orgànica 3/2018, del 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, s'aniran adaptant les mesures oportunes tals com l'anàlisi de legitimitat jurídica de cadascun dels tractaments de dades que es duguin a terme, l'anàlisi de riscos, l'avaluació d'impacte si el risc és alt, el registre d'activitats i el nomenament de qui exerceixi les funcions de Delegat de Protecció de Dades, d'acord amb la Política de Protecció de Dades Personals de l'Ajuntament de Granollers.

9. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El Comitè de Seguretat de la Informació aprovarà el desenvolupament d'un sistema de gestió, que serà establert, implementat, mantingut i millorat, conforme als estàndards de seguretat. Aquest sistema s'adequarà i servirà de gestió dels controls de l'Esquema Nacional de Seguretat. El sistema serà documentat i permetrà generar evidències dels controls i del compliment dels objectius marcats pel Comitè.

Hi haurà un procediment de gestió documental que establirà les directrius per a l'estructuració de la documentació de seguretat del sistema, la gestió i l'accés.

Correspon al Comitè de Seguretat de la Informació la revisió anual de la present Política, proposant, en cas que sigui necessari, millores de la mateixa, per a la seva aprovació per part de l'òrgan competent.

10. TERCERS

Quan l'Ajuntament de Granollers presti serveis a altres organismes, o manegi informació d'altres organismes, se'ls farà partícip d'aquesta Política de Seguretat de la Informació. L'Ajuntament de Granollers definirà i aprovarà els canals per a la coordinació de la informació i els procediments d'actuació i reacció davant d'incidents de seguretat, així com

per la resta d'actuacions que l'Ajuntament de Granollers dugui a terme en matèria de seguretat en relació amb altres organismes.

Quan l'Ajuntament de Granollers utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícip d'aquesta Política de Seguretat i de la Normativa de Seguretat existent que afecta aquests serveis o informació.

Aquests tercers queden subjectes a les obligacions establertes a l'esmentada normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics de comunicació i resolució d'incidents. Es garantirà que el personal de tercers estigui degudament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert a aquesta Política de Seguretat. De la mateixa manera, tenint en compte l'obligació de complir amb el que disposen les Instruccions Tècniques de Seguretat recollides a l'article 29 "Instruccions tècniques de seguretat i guies de seguretat" del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat a l'àmbit de l'Administració Electrònica, modificat pel Reial Decret 951/2015 de 23 d'octubre, i en consideració a la Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat, on s'estableix que 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, en el cas de sistemes de categoria MITJANA o ALTA.

Quan algun aspecte d'aquesta Política de Seguretat no pugui ser satisfet per un tercer segons es requereix 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. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant."