REGLAMENT PEL QUAL ES REGULA LA POLÍTICA DE SEGURETAT I DE LA PROTECCIÓ DE DADES DE CARÀCTER PERSONAL EN LA DIPUTACIÓ PROVINCIAL DE VALÈNCIA I ES DEROGA EL REGLAMENT ANTERIOR

Per al compliment de la seua missió, la prestació dels serveis identificats i el compliment dels seus objectius, la Diputació de València depén dels sistemes TIC (Tecnologies de la Informació i Comunicacions). Aquests sistemes han de ser administrats amb diligència, i s'han adoptar les mesures adequades per a protegir-los contra danys accidentals o deliberats que puguen afectar la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de la informació tractada o dels serveis prestats.

L'objectiu de la seguretat de la informació és garantir la qualitat d'aquesta i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces d'evolució ràpida amb potencial per a incidir en la confidencialitat, integritat, disponibilitat, autenticitat, traçabilitat, ús previst i valor de la informació i els serveis. Per a defensar-se d'aquestes amenaces es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn, per a garantir la prestació contínua dels serveis.

Més encara, en el marc específic de l'administració electrònica, l'antiga Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics, proclamava com un dels seus fins crear les condicions de confiança en l'ús dels mitjans electrònics, establint les mesures necessàries per a la preservació de la integritat dels drets fonamentals, i especialment els relacionats amb la intimitat i la protecció de dades de caràcter personal, per mitjà de la garantia de la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics. L'actual norma d'aplicació en la matèria, la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, recorda a més que el desenvolupament de les TIC també ha vingut afectant profundament la forma i el contingut de les relacions de l'Administració amb els ciutadans i les empreses.

És per això que el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració Electrònica, estableix que «tots els òrgans superiors de les Administracions Públiques hauran de disposar formalment de la seua Política de seguretat, que serà aprovada pel titular de l'òrgan superior corresponent».

D'altra banda, l'aplicació de la normativa sobre protecció de dades de caràcter personal comporta per a aquesta Corporació, com a responsable i encarregada de tractaments d'aquesta naturalesa, la necessària adopció d'una sèrie de mesures de caràcter tècnic i organitzatiu tendents a garantir els drets dels titulars d'aquestes dades personals. En aquest sentit, la disposició addicional primera de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, determina que els responsables enumerats en l'article 77.1 d'aquesta llei orgànica —sector públic— hauran d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguen de les previstes en l'Esquema Nacional de Seguretat. En conseqüència, la convergència dels requisits de seguretat sobre els sistemes d'informació TIC i dels reclamats per la protecció de dades de caràcter personal en una mateixa norma (ENS) fa aconsellable no emprendre accions desagregades, que atenguen cada dimensió per separat, perquè això podria provocar duplicitats, antinòmies, confusió i descoordinació internes, a més de resultar més onerós des del punt de vista de la inversió de recursos humans, econòmics, tècnics i organitzatius.

En virtut d'això, i per a donar resposta a les necessitats exposades anteriorment, el Ple de la Diputació de València va aprovar el Reglament de Política de Seguretat i de la Protecció de Dades de Caràcter Personal de la

Diputació de València —BOP núm. 159, de 6-VII-2013—, el qual va ser desenvolupat mitjançant el Decret núm. 6353, de 3 de juliol de 2015, del diputat de Modernització, pel qual s'aproven les Normes de Seguretat per al Personal Tècnic dels Sistemes d'Informació TIC; el Decret núm. 6111, de 26 de juny de 2015, del diputat de Modernització, pel qual s'aproven les Normes de Seguretat per als Usuaris dels Sistemes d'Informació; el Decret núm. 5448, de 12 de juny de 2015, del diputat de Modernització, pel qual s'aprova la Normativa de Protecció de Dades de Caràcter Personal; i el Decret núm. 6110, de 26 de juny de 2015, del diputat de Modernització, pel qual s'aproven els Procediments de Protecció de Dades de Caràcter Personal. Després de l'aprovació de les normes citades anteriorment s'han produït canvis importants. Aquests canvis són de diferent naturalesa: Avanços tecnològics, noves amenaces cibernètiques, canvis geopolítics, modificació d'hàbits socials, alteració de l'organització administrativa de la Corporació, incidència de pandèmies i nova producció legislativa tant de l'entorn europeu com nacional. La suma d'aquests canvis ens situa en un escenari diferent a l'existent en el moment en què es van elaborar les normatives internes exposades.

Precisament la nova producció legislativa ha tingut una incidència notable en els dos àmbits de referència, la protecció de dades personals i la seguretat de la informació. El règim normatiu en matèria de protecció de dades personals vigent durant els quasi vint últims anys ha sigut desplaçat per sengles normes, el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades —d'ara en avant RGPD— i la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD). Pel que fa a l'ENS, en el moment actual s'ha elaborat un projecte legislatiu que haurà de substituir el text del RD 3/2010, el qual obeeix a la directriu continguda en el Pla de Digitalització de les Administracions Públiques, un dels instruments principals per a l'execució dels fons del Component 11 «Modernització de les Administracions Públiques» del Pla de Recuperació, Transformació i Resiliència, com també per al desenvolupament de les inversions i reformes previstes en l'agenda Espanya Digital 2025, la qual contempla l'actualització de l'ENS entre les reformes normatives a abordar amb la finalitat d'evolucionar la Política de seguretat de les Administracions Públiques espanyoles, tenint en compte les regulacions de la Unió Europea dirigides a incrementar el nivell de ciberseguretat dels sistemes d'informació.

En conclusió, resulta necessari aprovar una nova normativa que, en l'àmbit intern de la Diputació de València, substituïsca l'anterior i hi incorpore aquesta nova realitat tecnològica, social, organitzativa interna i legislativa, i proporcione la deguda actualitat a la regulació de l'activitat pròpia de la Corporació.

Per a l'elaboració de la present disposició s'han tingut en consideració la legislació següent: la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les Administracions Públiques; la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic; el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica (amb la seua modificació per Reial decret 951/2015, de 23

d'octubre); el Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica; el 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; la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, com també les denominades instruccions tècniques de seguretat i les guies de seguretat de les tecnologies de la informació i les comunicacions (sèrie CCN-STIC) elaborades pel Centre Criptològic Nacional per al millor compliment del que s'estableix en l'ENS —article 29 ENS—, a més de les resolucions, informes i guies de l'Agència Espanyola de Protecció de Dades, adequant tot això a la realitat orgànica i funcional de la Diputació de València.

TÍTOL PRELIMINAR

Àmbit d'aplicació i disposicions generals

Capítol primer

Disposicions comunes

Article 1. OBJECTE

El present reglament té per objecte definir i regular, en l'àmbit de la Diputació de València, la Política de seguretat i de protecció de dades de caràcter personal aplicable als sistemes d'informació que intervinguen en el tractament de la informació que resulte necessària per a l'exercici de les seues competències.

Article 2. DEFINICIONS

A l'efecte de la present disposició s'entendrà per:

• Actiu. Component o funcionalitat d'un sistema d'informació susceptible de ser atacat deliberadament o accidentalment amb conseqüències per a l'organització. Inclou: informació, dades, serveis, aplicacions (programari), equips (maquinari), comunicacions, recursos administratius, recursos físics i recursos humans.

• Anàlisi de riscos. Estudi de les conseqüències previsibles d'un possible incident de seguretat, considerant el seu impacte en l'organisme (en la seua missió, en la seua imatge o reputació, o en les seues funcions) i la probabilitat que ocórrega.

• Auditoria de la seguretat. Revisió i examen independents dels registres i les activitats del sistema per a verificar la idoneïtat d'aquests controls, assegurar que es compleixen la Política de seguretat i els procediments operatius

establits, detectar les infraccions de la seguretat i recomanar modificacions apropiades dels controls, de la Política i dels procediments.

• Autenticitat. Propietat o característica consistent en el fet que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.

• Ciberincident. Incident de seguretat l'àmbit dels Sistemes d'Informació i les Comunicacions.

• Ciberseguretat. La protecció de les xarxes i sistemes d'informació, els seus usuaris i altres persones contra les ciberamenaces.

• Confidencialitat. Propietat o característica consistent en el fet que la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.

• Dades personals. Qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus concernent a persones físiques identificades o identificables.

• Disponibilitat. Propietat o característica dels actius consistent en el fet que les entitats o processos autoritzats tenen accés a aquests quan ho requereixen.

• Encarregat del tractament o encarregat. La persona física o jurídica, autoritat pública, servei o un altre organisme que tracte dades personals per compte del responsable del tractament.

• Incident de seguretat. Un esdeveniment o una sèrie d'esdeveniments de seguretat de la informació no desitjats o inesperats que tenen una probabilitat significativa de comprometre les operacions i amenaçar la seguretat de la informació.

• Integritat. Propietat o característica consistent en el fet que l'actiu d'informació no ha sigut alterat de manera no autoritzada.

• Mesures de seguretat. Conjunt de disposicions encaminades a protegir-se dels riscos possibles sobre el sistema d'informació, amb la finalitat d'assegurar els seus objectius de seguretat. Pot tractar-se de mesures de prevenció, de dissuasió, de protecció, de detecció i reacció, o de recuperació.

• Responsable del tractament o responsable: La persona física o jurídica, autoritat pública, servei o un altre organisme que, només o juntament amb uns altres, determine els fins i mitjans del tractament.

• Risc. Estimació del grau d'exposició al fet que una amenaça es materialitze sobre un o més actius i cause danys o perjudicis a l'organització.

• Risc residual. És el risc resultant de l'aplicació de contramesures i, per tant, constitueix el risc a assumir.

• Sistema d'informació. Conjunt organitzat de recursos perquè la informació es puga recollir, emmagatzemar, processar o tractar, mantindre, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

• Sistema d'informació TIC. Sistema d'informació que empra tecnologies de la informació i de les comunicacions.

• Traçabilitat. Propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

Article 3. ABAST

Aquesta Política s'aplica a tots els sistemes d'informació TIC, com també a aquells sistemes d'informació de qualsevol naturalesa que tracten dades de caràcter personal, que siguen de la titularitat de la Diputació de València o la gestió o la responsabilitat de la qual tinga encomanada.

Quan la informació la titularitat la gestió o responsabilitat de la qual corresponga a la Diputació de València es trobe o es tracte en entorns aliens, la Diputació exigirà les mateixes garanties i requisits que les determinades en la present Política.

Sense perjudici d'això anterior, la Diputació aplicarà la present Política en el marc de les seues relacions amb les entitats locals del seu territori, i respectarà en qualsevol cas l'autonomia d'aquelles i les seues facultats de gestió i control sobre la informació i els serveis que els són propis. La Diputació promourà acords amb aquestes entitats locals per a l'intercanvi de la informació necessària que facilite les garanties i el compliment legal en matèria de seguretat i de protecció de dades personals en els sistemes d'informació afectats.

Queda exclosa de manera específica de l'aplicació de la present Política la informació tractada pels grups polítics i/o els seus membres, les centrals sindicals i/o membres representants dels treballadors, sempre que aquesta informació no forme part dels actius d'informació de titularitat de la Corporació.

La normativa que desenvolupe el present Reglament establirà les condicions d'ús dels actius dels sistemes d'informació corporatius i dels dispositius posats a la disposició d'aquests col·lectius.

Article 4. ÀMBIT SUBJECTIU D'APLICACIÓ

Les presents disposicions són aplicables a tots els departaments i unitats de la Diputació de València. Els ens o organismes públics vinculats o dependents de la Diputació de València adoptaran la seua pròpia Política de seguretat i de protecció de dades de caràcter personal, que haurà d'adequar-se en la mesura que siga possible a les presents prescripcions.

Capítol segon

Missió i marc legal

Article 5. MISSIÓ

La Diputació de València és una entitat local d'àmbit provincial que té les competències següents:

a) La coordinació dels serveis municipals entre si per a la garantia de la prestació integral i adequada en la totalitat del territori provincial dels serveis mínims de competència municipal.
b) L'assistència i la cooperació jurídica, econòmica i tècnica als municipis, especialment els de menor capacitat econòmica i de gestió.
c) La prestació de serveis públics de caràcter supramunicipal i, si escau, supracomarcal.
d) La cooperació en el foment del desenvolupament econòmic i social i en la planificació en el territori provincial, d'acord amb les competències de les altres Administracions Públiques en aquest àmbit.
e) En general, el foment i l'administració dels interessos peculiars de la província.
f) Qualssevol altres que els siguen atribuïdes per les lleis de l'Estat i de la Comunitat Autònoma en els diferents sectors d'acció pública.

Article 6. MARC LEGAL

En la seua qualitat d'administració pública, la Diputació de València duu a terme les competències que li són pròpies amb ple sotmetiment a l'ordenament jurídic, en general, i especialment:

a. A la normativa sobre règim jurídic local: Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local; Reial decret legislatiu 781/1986, de 18 d'abril, pel qual s'aprova el text refós de les disposicions legals vigents en matèria de règim local; Reial decret legislatiu 2/2004, de 5 de març, pel qual s'aprova el text refós de la Llei reguladora de les hisendes locals; Reial decret 2568/1986, de 28 de novembre, pel qual s'aprova el Reglament d'organització, funcionament i règim jurídic de les entitats locals; i Llei 8/2010, de 23 de juny, de la Generalitat, de règim local de la Comunitat Valenciana.

b. A la normativa sobre procediment administratiu i contractació: Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques; Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic; i Llei 9/2017, de 8 de novembre, de contractes del sector públic.

D'igual manera, en la utilització de mitjans tecnològics per al desenvolupament de les seues activitats, hi són d'especial aplicació:

a. La normativa sobre administració electrònica: Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques; Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic; Decret 220/2014, del Consell, pel qual s'aprova el Reglament d'administració electrònica de la Comunitat Valenciana; Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica; Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica; Reial decret 203/2021, de 30 de març (BOE 31/03/2021), pel qual s'aprova el Reglament d'actuació i funcionament

del sector públic per mitjans electrònics; Reglament de desenvolupament de l'Administració Electrònica de la Diputació de València (BOP 30/09/2013).

b. La normativa sobre signatura electrònica: Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

c. La normativa sobre protecció de dades de caràcter personal: el 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), i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

TÍTOL PRIMER

Principis de seguretat TIC i de la protecció de dades de caràcter personal

Capítol primer

Principis comuns

Article 7. SEGURETAT COORDINADA I ESTRUCTURADA

La seguretat dels sistemes d'informació s'abordarà aplicant de manera coherent i coordinada aquesta política, les normes que la desenvolupen i el referent legislatiu de l'ENS a qualsevol classe d'informació tractada en aquests sistemes, atesa la previsió que en matèria de seguretat de les dades personals conté la disposició addicional primera de la Llei 3/2018 LOPD-GDD.

D'igual forma, a l'hora d'executar les activitats de la seguretat de la informació es respectaran els principis de competència i separació de funcions establits en el present Reglament, conforme a les atribucions conferides a cada component de l'estructura d'organització de la seguretat i de la protecció de dades personals.

Article 8. ACCÉS A LA INFORMACIÓ

Els drets d'accés dels usuaris a la informació es regiran pels següents principis:

a) Mínim privilegi. Els privilegis de cada usuari es reduiran al mínim estrictament necessari per a complir les seues obligacions.
b) Necessitat de conéixer. Els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per a complir les seues obligacions.

c) Capacitat d'autoritzar. Només i exclusivament el personal amb competència per a això podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establits pel seu responsable.

Article 9. CICLE VITAL DE LA INFORMACIÓ

La seguretat i la protecció de les dades de caràcter personal estaran presents durant tot el cicle de vida de la informació.

La normativa que desenvolupe la present Política haurà d'establir els criteris i requisits que haurà de complir la recollida, utilització, publicació, transferència i l'intercanvi de la informació, com també la seua destrucció o destí final després de complir el seu cicle de vida útil, amb l'objectiu de garantir els anteriors principis de seguretat i de protecció de dades de caràcter personal.

Article 10. DEURE DE SECRET

Tots els usuaris estan obligats a guardar secret professional de tota aquella informació de la qual tinguen coneixement en ocasió de l'exercici del seu càrrec o activitat professional. Aquesta obligació es mantindrà fins i tot després d'haver finalitzat la relació amb la Diputació de València.

El deure de confidencialitat i secret professional s'establirà de manera expressa en tota mena de relacions —administratives, civils o mercantils— que impliquen o suposen accés o tractament de la informació, inclosos els serveis de simple allotjament, transport o suport tècnic.

Capítol segon

Principis de seguretat TIC

Article 11. PROCÉS INTEGRAL

La seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb el sistema d'informació.

En virtut d'això, qualsevol acció dirigida a l'objectiu de la seguretat ha de considerar la interacció de tots els elements citats, la qual cosa exclou qualsevol actuació puntual o tractament conjuntural.

Per a evitar que la ignorància, la falta d'organització i coordinació, o instruccions inadequades, siguen fonts de risc per a la seguretat, s'haurà de procedir, especialment, a la conscienciació i formació adequada de les persones que intervenen en el procés i els seus responsables jeràrquics.

Article 12. GESTIÓ BASADA EN RISCOS

La gestió de la seguretat es recolzarà en un procés continu d'anàlisi i tractament de riscos. Aquest procés haurà de mantindre's actualitzat de manera permanent.

La gestió de riscos ha de permetre el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells es realitzarà mitjançant el desplegament de mesures de seguretat, que establirà un equilibri entre la naturalesa de les dades i els tractaments, els riscos als quals estiguen exposats i les mesures de seguretat.

Tots els sistemes d'informació subjectes a aquesta política de seguretat hauran de realitzar una anàlisi de riscos, tot avaluant les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà:

- regularment, almenys una vegada a l'any
- quan canvie la informació manejada
- quan canvien els serveis prestats
- quan ocórrega un incident greu de seguretat
- quan es reporten vulnerabilitats greus

L'anàlisi de riscos serà la base per a determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establits per l'ENS.

Per a l'harmonització de les anàlisis de riscos, el Comité de Seguretat TIC podrà establir una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

Article 13. PREVENCIÓ

Els departaments interns han d'evitar, o almenys previndre en la mesura que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, com també qualsevol control addicional identificat a través de l'avaluació d'amenaces i riscos. Aquests controls i els rols i responsabilitats de seguretat de tot el personal han d'estar clarament definits i documentats.

Per a garantir el compliment de la present política caldrà:

- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de manera rutinària.
- Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtindre una avaluació independent.

Article 14. DETECCIÓ

Atés que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seua detenció, els serveis han de

monitorar l'operació de manera contínua per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que s'estableix en l'article 9 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i report, que arriben als responsables regularment, i quan es produeix una desviació significativa dels paràmetres que s'hagen preestablit com a normals.

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

Article 15. RESPOSTA

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

Hauran d'establir-se mecanismes per a respondre eficaçment als incidents de seguretat, designar un punt de contacte per a les comunicacions respecte a incidents detectats en els departaments i 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).

En l'àmbit de la Diputació de València s'haurà de crear un Grup de Resposta a Incidents TIC (Grup RITIC), la funció del qual serà la presa de decisions urgent en cas de contingència greu que afecte la seguretat de sistemes d'informació crítics de la Corporació. El Grup RITIC estarà format per membres designats pel Comité de Seguretat TIC.

Article 16. CONSERVACIÓ

Els sistemes d'informació garantiran la conservació de les dades i informacions en suport electrònic. D'igual manera, els sistemes mantindran disponibles els serveis durant tot el cicle vital de la informació digital, a través d'una concepció i procediments que siguen la base per a la preservació del patrimoni digital.

Capítol tercer

Principis de la protecció de dades de caràcter personal

Article 17. LICITUD, TRANSPARÈNCIA I LLEIALTAT

Les dades han de ser tractades de manera lícita, lleial i transparent per a l'interessat.

Tots els mitjans que s'utilitzen per a recaptar dades de caràcter personal hauran de guardar la transparència i proporcionar a l'interessat la informació a què fa referència l'article 11 de la LOPDGDD, amb les excepcions legalment contemplades.

Tant la seu electrònica de la Diputació de València com qualsevol espai en Internet o tecnologies similars dels continguts de les quals siga responsable la Corporació contindran referència al Registre d'Activitats de Tractament, les polítiques i normatives internes sobre protecció de dades de caràcter personal i, en particular, dels drets que assisteixen els titulars de les dades.

Mitjançant procediments interns es garantirà, prèviament a la seua activació, que els mitjans i espais anteriorment citats compleixen degudament els requisits establits.

Article 18. PROTECCIÓ DE DADES DES DEL DISSENY

En desenvolupar, dissenyar, seleccionar i usar aplicacions, serveis i productes que estiguen basats en el tractament de dades personals o que tracten dades personals per a complir la seua funció, cal inclinar-se per aquells que tinguen en compte el dret a la protecció de dades quan es desenvolupen i dissenyen aquests productes, serveis i aplicacions, i que s'assegure, amb la deguda atenció a l'estat de la tècnica, que els responsables i els encarregats del tractament estan en condicions de complir les seues obligacions en matèria de protecció de dades.

Tots els departaments de la Corporació hauran de tindre en compte, a l'hora d'incorporar nous tractaments de dades personals, que, prèviament a la seua execució, es consideren en el seu disseny i desenvolupament les accions que garantisquen el compliment de les garanties de protecció de dades personals.

Article 19. DRETS D'ACCÉS, RECTIFICACIÓ, SUPRESSIÓ, OPOSICIÓ, LIMITACIÓ I PORTABILITAT

Haurà d'establir-se un procediment intern que assegure l'exercici dels drets d'accés, rectificació, supressió, oposició, limitació i portabilitat als titulars de les dades de caràcter personal. Aquest procediment haurà de ser comú a tots els tractaments dels quals siga responsable la Corporació, llevat que les lleis aplicables a determinats tractaments establisquen un procediment especial per a la rectificació o supressió de les dades tractades.

S'adoptaran les mesures oportunes per a garantir que el personal de la Corporació que té accés a dades de caràcter personal puga informar del procediment a seguir per l'afectat per a l'exercici dels seus drets.

En seu electrònica s'habilitarà un espai per a oferir informació als afectats sobre el contingut d'aquests drets i el procediment a seguir per a exercir-los, com també un canal electrònic per al seu exercici, preferentment a través de la mateixa seu electrònica de la Corporació.

Article 20. COMUNICACIÓ DE DADES

Només amb el consentiment de l'interessat, sempre que una norma no ho impedisca, o a l'empara d'algun dels supòsits recollits expressament en la normativa sobre protecció de dades personals, podrà procedir-se a la comunicació o cessió de les dades.

Quan, amb suport legal i sense ser preceptiu el consentiment de l'interessat, haja de publicar-se informació considerada com a dada de caràcter personal, el contingut d'aquesta publicació serà l'estrictament necessari per a complir l'objectiu perseguit, i es preservarà el màxim possible la intimitat de l'afectat. D'igual manera, s'optarà per aquells mitjans de publicitat que comporten menor nivell d'ingerència en el dret a la intimitat i a la protecció de dades de caràcter personal.

Sempre que siga possible es dissociaran les dades aplicant, segons siga procedent, tècniques de seudonimització o anonimització, i el xifratge de les dades.

Article 21. ACCÉS A DADES PER COMPTE DE TERCERS

Quan la Diputació haja d'encomanar a un tercer la realització d'un tractament pel seu compte, triarà únicament un encarregat que oferisca garanties suficients per a aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament siga conforme amb els requisits de la legislació de protecció de dades, del present Reglament i les seues normes de desenvolupament, i garantirà la protecció dels drets dels titulars de les dades.

Perquè la Diputació de València atorgue a tercers l'accés a dades de caràcter personal, quan el citat accés siga necessari perquè aquests tercers presten un servei a la Diputació, haurà de formalitzar-se prèviament a aquest accés a dades un contracte o un altre acte jurídic que vincule l'encarregat respecte del responsable i establisca l'objecte, la duració, la naturalesa i la finalitat del tractament, el tipus de dades personals i categories d'interessats, i les obligacions i drets del responsable, amb el contingut mínim regulat en l'article 28.3 del RGPD. Aquest contracte o acte jurídic estipularà, en particular, que l'encarregat haurà d'oferir-les garanties suficients per a aplicar les mesures tècniques i organitzatives apropiades conforme al que s'estableix en el RGPD.

D'igual manera, la Diputació de València s'abstindrà d'actuar en qualitat d'encarregat del tractament quan aquesta prestació requerisca l'accés a dades de caràcter personal si no es duen a terme les previsions anteriors, encara que el responsable del tractament no li exigisca el compliment d'aquestes.

Article 22. RESPONSABILITAT PROACTIVA

S'aplicaran les mesures tècniques i organitzatives apropiades per a garantir i estar en condicions de demostrar que el tractament de dades personals es duu a terme de conformitat amb la normativa legal i interna en la matèria.

Quan resulte preceptiu recaptar el consentiment de l'interessat per a la recollida, tractament o cessió de les seues dades, s'utilitzaran mitjans que permeten deixar-ne constància fefaent.

TÍTOL SEGON

Organització de la seguretat i de la protecció de dades personals

Capítol primer

Principis comuns

Article 23. RESPONSABILITAT GENERAL I ESPECÍFICA

Tots i cadascun dels usuaris dels sistemes d'informació de la Diputació de València són responsables de la seguretat dels actius tecnològics posats a la seua disposició mitjançant un ús correcte d'aquests, com també de la seguretat de la informació i de les dades de caràcter personal que manegen, sempre d'acord amb les seues atribucions professionals.

No obstant això, el manteniment i la gestió de la seguretat dels sistemes d'informació i de la protecció de dades personals van íntimament lligats a l'establiment d'una organització. Aquesta organització s'estableix mitjançant la identificació i definició de les diferents activitats i responsabilitats en matèria de gestió de la seguretat dels sistemes d'informació i de la protecció de dades personals, i la implantació d'una estructura que les suporte.

Article 24. ESTRUCTURA ORGANITZATIVA

En els apartats següents s'especifica l'estructura bàsica de l'organització de la seguretat i de la protecció de dades personals en els sistemes d'informació que regirà en la Diputació de València. Les figures i les responsabilitats associades a aquestes tenen caràcter de mínims i els continguts es poden desenvolupar a través de la normativa interna de seguretat i de la protecció de dades personals, que respectarà, en qualsevol cas, el que s'estableix en la present disposició.

Article 25. RESOLUCIÓ DE CONFLICTES

En cas de conflicte entre les diferents figures que componen l'estructura organitzativa, prevaldrà la decisió del Comité de Seguretat TIC sempre que el conflicte no afecte l'aplicació de la normativa legal o interna en matèria de protecció de dades personals. Per a decidir sobre el conflicte, el Comité prendrà com a referència el marc de competències i responsabilitats de les

citades figures establit per la present política i les seues normes de desenvolupament.

Quan el conflicte afecte l'aplicació de normativa legal o interna en matèria de protecció de dades personals, prevaldrà el criteri del delegat de Protecció de Dades.

Capítol segon

Figures i responsabilitats

Article 26. RESPONSABLE DEL SERVEI

El responsable del servei és qui té la potestat d'establir les característiques d'un servei, a l'efecte de determinar els requisits en matèria de seguretat i de protecció de dades personals.

Al responsable del servei li correspon:

- La valoració del servei en totes les dimensions de seguretat —disponibilitat, integritat, confidencialitat, traçabilitat i autenticitat— tenint en compte la naturalesa del servei i la normativa que poguera ser-li aplicable.
- La propietat dels riscos sobre els serveis.
- Acceptar el risc residual sobre els serveis que li competeixen.

Article 27. RESPONSABLE DE LA INFORMACIÓ

El responsable de la informació és qui té la potestat d'establir les característiques d'una informació, a l'efecte de determinar els requisits en matèria de seguretat i de protecció de dades personals.

Sense perjudici del que es dispose en procediments o disposicions en desenvolupament del present Reglament sobre cadascuna de les figures contemplades en aquest capítol, al responsable de la informació li correspon:

- La valoració de la informació en totes les dimensions de seguretat —disponibilitat, integritat, confidencialitat, traçabilitat i autenticitat— tenint en compte la naturalesa d'aquesta informació i la normativa que poguera ser-li aplicable.
- Adoptar les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat de la informació i dels tractaments de dades de caràcter personal que resulte responsable establides per la normativa interna.
- La responsabilitat última de la protecció de la informació respecte a l'ús que en facen les persones al seu càrrec, o les que depenguen de la

seua direcció, o, en general, aquelles que siguen autoritzades per ell/ella per a accedir a la informació.
- La propietat dels riscos sobre la informació.
- Acceptar el risc residual sobre la informació que li competeix.
- Autoritzar els accessos dels usuaris a la informació, tot respectant els principis de mínim privilegi i necessitat de conéixer establits en la present política.
- La responsabilitat última del compliment de totes les garanties establides per la legislació i la normativa interna de la Corporació, especialment quan la informació consistisca en dades de caràcter personal.
- La responsabilitat última de qualsevol error o negligència que porte a un incident de confidencialitat o d'integritat de la informació, quan no haja atés degudament el deure de vetlar pel compliment de les garanties al·ludides en l'apartat anterior.

Article 28. DISPOSICIONS COMUNES AL RESPONSABLE DEL SERVEI I AL RESPONSABLE DE LA INFORMACIÓ

Seran responsables del servei i de la informació el personal directiu —caps de Servei, caps d'Oficina, directors/ores, coordinadors/ores, etc.— sota la direcció tècnica del qual es trobe el servei i la informació corresponents.

En els supòsits d'informació i serveis sota la direcció exclusiva del personal eventual a què es refereix l'article 12 de l'EBEP, serà aquest personal el considerat responsable del servei i de la informació.

La responsabilitat de la valoració de la informació i dels serveis és exclusivament del responsable corresponent. La valoració podrà ser proposada pel Responsable de Seguretat dels Sistemes d'Informació, i aprovada pel responsable de la informació i del servei corresponent si aquest la considera adequada.

La normativa que desenvolupe la present Política establirà els criteris i els instruments que permeten una adequada valoració dels serveis i informacions per part dels seus corresponents responsables.

Article 29. RESPONSABLE DE SEGURETAT DELS SISTEMES D'INFORMACIÓ

El Responsable de Seguretat és qui determinarà les decisions per a satisfer els requisits de seguretat de la informació i dels serveis, supervisarà la implantació de les mesures necessàries per a garantir que se satisfan els requisits i reportarà sobre aquestes qüestions.

Per al millor compliment de les funcions relacionades amb les mesures de seguretat implantades i, especialment, per raons de complexitat o immediatesa, el Responsable de Seguretat dels Sistemes d'Informació podrà delegar determinats aspectes d'aquestes comeses en altres persones de l'organització. En aquests supòsits, els diferents responsables de seguretat delegats actuaran

ajustant-se estrictament al contingut de la delegació, la qual recollirà l'abast material i temporal, les obligacions i responsabilitats de les tasques delegades. De les possibles delegacions haurà de donar-se compte al Comité de Seguretat TIC.

Seran funcions del Responsable de Seguretat dels Sistemes d'Informació:

- Actuar com a secretari del Comité de Seguretat TIC.
- Convocar el Comité de Seguretat TIC, i recopilar la informació pertinent.
- Ser responsable, juntament amb els diferents responsables de seguretat delegats, si escau, d'estar al corrent de canvis normatius (lleis, reglaments o pràctiques sectorials) que puguen afectar directament o indirectament la seguretat dels sistemes d'informació de la Corporació, havent d'informar-se de les conseqüències per a les activitats de l'Organització, alertar el Comité de Seguretat TIC i proposar les accions oportunes d'adequació al nou marc normatiu.
- Elaborar i signar les Declaracions d'Aplicabilitat dels sistemes d'informació pertinents.
- Ser el responsable de la presa de decisions dia a dia entre les reunions del Comité de Seguretat TIC. Aquestes decisions estaran presidides pels principis d'unitat d'acció i coordinació d'actuacions en general, i, especialment, en cas d'incidències que tinguen repercussió fora de l'organització i en cas de desastres.
- En cas de desastre s'incorporarà al Grup RITIC i coordinarà totes les actuacions relacionades amb qualsevol aspecte de la seguretat dels sistemes d'informació.
- Coordinar les seues actuacions amb el Departament de Protecció de Dades i Seguretat de la Informació, i col·laborar amb aquest en tots aquells aspectes que puguen incidir en les competències atribuïdes a aquest Departament.

I qualssevol altres comeses que li siguen encomanades per la present política i per la Direcció de la Corporació.

Serà Responsable de Seguretat dels Sistemes d'Informació en l'àmbit de la Diputació de València qui designe el Comité de Seguretat TIC.

Article 30. RESPONSABLE DELS SISTEMES D'INFORMACIÓ TIC

Correspondrà al Responsable dels Sistemes d'Informació TIC:

- Desenvolupar, operar i mantindre els Sistemes d'Informació TIC durant tot el seu cicle de vida, de les seues especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i sistema de gestió dels Sistemes d'Informació TIC establint els criteris d'ús i els serveis disponibles en aquest.
- Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
- Acordar la suspensió del maneig d'una certa informació o la prestació d'un determinat servei si és informat de deficiències greus de seguretat que

pogueren afectar la satisfacció dels requisits establits. Aquesta decisió ha de ser acordada amb el responsable de la informació afectada, del servei afectat i el responsable de Seguretat dels Sistemes d'Informació abans de ser executada.

Serà Responsable dels Sistemes d'Informació TIC en l'àmbit de la Diputació de València el/la cap del Servei d'informàtica.

Atesa la complexitat, distribució, separació física dels seus elements o nombre d'usuaris que habitualment comporta la gestió dels actuals sistemes d'informació, com també la realitat funcional dels qui han de compaginar les responsabilitats derivades de la present disposició amb les seues competències habituals, el Responsable dels Sistemes d'Informació TIC podrà delegar determinats aspectes de les seues comeses en altres persones de l'organització. En aquests supòsits, els diferents responsables de sistemes d'informació delegats actuaran ajustant-se estrictament al contingut de la delegació, la qual recollirà l'abast material i temporal, les obligacions i responsabilitats de les tasques delegades. De les possibles delegacions haurà de donar-se compte al Comité de Seguretat TIC.

En cap cas no podrà ser objecte de delegació la competència per a acordar la suspensió del maneig d'una certa informació o la prestació d'un determinat servei, en els termes citats en el present article.

Article 31. ADMINISTRADOR DE SEGURETAT DELS SISTEMES D'INFORMACIÓ TIC

L'Administrador de Seguretat és el responsable de la implantació, gestió i manteniment de les mesures de seguretat aplicables als Sistemes d'Informació TIC.

Serà Administrador de Seguretat dels sistemes d'informació TIC en l'àmbit de la Diputació de València el/la cap del Servei d'informàtica.

L'Administrador de Seguretat dels Sistemes d'Informació TIC podrà delegar determinats aspectes de les seues comeses en altres persones de l'organització. En aquests supòsits, els diferents administradors de seguretat delegats actuaran ajustant-se estrictament al contingut de la delegació, la qual recollirà l'abast material i temporal, les obligacions i responsabilitats de les tasques delegades. De les possibles delegacions haurà de donar-se compte al Comité de Seguretat TIC.

Article 32. COMITÉ DE SEGURETAT TIC

És l'òrgan que gestiona i coordina la Seguretat dels Sistemes d'Informació TIC a nivell d'organització.

Es crea el Comité de Seguretat TIC de la Diputació de València, com un òrgan col·legiat de caràcter horitzontal, que es regirà en el seu funcionament per aquesta disposició, i, en allò no previst en aquesta, serà d'aplicació supletòria

la normativa reguladora dels òrgans col·legiats continguda en la subsecció 2a de la secció 3a del capítol II de la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.

El Comité de Seguretat TIC es reunirà amb caràcter ordinari, almenys, una vegada per semestre. Per raons d'urgència podrà reunir-se sempre que la Presidència del Comité ho estime convenient. Les reunions tindran lloc dins de la jornada de treball establida reglamentàriament.

El Comité podrà acordar la constitució de comissions delegades de treball, per a tractar temes, elaborar estudis o informes, o dur a terme qualsevol altra gestió que per la seua especificitat o complexitat tècnica així es considere.

El Comité podrà regular el seu propi règim de funcionament, el qual haurà de respectar, en qualsevol cas, el que es disposa en la present disposició i la normativa que resulte d'aplicació.

El Comité està compost per:

- El/La cap del Servei d'Informàtica, que assumirà la Presidència del Comité.
- El secretari/ària general de la Corporació, que exercirà la Vicepresidència del Comité.
- El/La Responsable de Seguretat dels Sistemes d'Informació, que actuarà com a Secretari del Comité.
- Els diferents Responsables de Sistemes d'Informació, Responsables de seguretat i Administradors de seguretat delegats.
- Una persona designada pel Departament de Protecció de Dades i Seguretat de la Informació, que actuarà amb veu però sense vot.
- El/La delegat/ada de protecció de dades de la Corporació, que actuarà en funcions d'informació i assessorament en matèria de protecció de dades però no participarà en la presa de decisions.

El Comité exercirà les funcions següents:

• Coordinar totes les funcions de seguretat dels sistemes d'informació TIC de la Corporació.
• Vetlar pel compliment de la legislació i normativa interna d'aplicació.
• Recaptar del Responsable de Seguretat informes regulars de l'estat de la seguretat de l'Organització i dels possibles incidents. Aquests informes es consoliden i resum per a la Direcció de la Corporació.
• Atendre les peticions d'informació que puga requerir el Departament de Protecció de Dades i Seguretat de la Informació, així com les recomanacions i propostes efectuades per aquest Departament.
• Coordinar i donar resposta a les inquietuds transmeses a través del Responsable de Seguretat.
• Dinamitzar la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes d'informació, promovent inversions de caràcter horitzontal.
• Designar als components del Grup RITIC indicat en l'article 15 de la present disposició.

I qualssevol altres comeses que els siguen encarregats per la present Política i per la Direcció de la Corporació.

El Comité podrà recaptar del personal tècnic propi o extern la informació pertinent per a la presa de les seues decisions.

Article 33. DELEGAT DE PROTECCIÓ DE DADES

El Delegat de Protecció de Dades és el garant en el si de la Corporació del compliment de la legislació europea i nacional sobre protecció de dades de caràcter personal, com també de la normativa interna en la matèria.

La regulació d'aquesta figura està recollida en els articles 36 a 38 de la present Política.

Serà Delegat de Protecció de Dades en l'àmbit de la Diputació de València el funcionari designat per el/la president/a de la Diputació.

Article 34. CENTRE GESTOR DEL TRACTAMENT

És la unitat administrativa responsable d'un tractament de dades personals, en atenció a criteris com:

a) Ser la unitat que presta el servei o té la competència per a la qual es tracten les dades personals.
b) Ser la unitat que decideix sobre la creació, finalitat i/o tipus de dades del tractament o l'ús de les dades personals.
c) Ser la principal o major usuària de les dades personals.

En qualsevol cas, seran competència del Delegat de Protecció de Dades l'estudi, la valoració i la determinació de les unitats que han de ser Centre Gestor del Tractament en cada supòsit concret.

En relació amb el tractament de dades del qual és responsable, a cada centre gestor del tractament li correspon:

- Comunicar al Delegat de Protecció de Dades la intenció de procedir a un nou tractament, prèviament a la seua iniciació, com també les variacions i cessaments en els tractaments ja iniciats.
- Mantindre actualitzada la informació en el Registre d'Activitats de Tractament de la Corporació dels tractaments dels quals siga responsable.

Article 35. DEPARTAMENT DE PROTECCIÓ DE DADES I SEGURETAT DE LA INFORMACIÓ

Al departament de Protecció de Dades i Seguretat de la Informació li correspon:

a) Proporcionar suport tècnic, humà i organitzatiu al Delegat de Protecció de Dades i assistir-lo en l'exercici de les seues competències.
b) Elaborar el Pla General Auditor de Protecció de Dades Personals i Seguretat de la Informació de la Diputació i dur a terme les actuacions auditores hi compreses que li corresponguen.
c) Executar l'auditoria de la seguretat dels sistemes d'informació a la qual es refereix l'Esquema Nacional de Seguretat.
d) Supervisar el compliment de la normativa legal i interna en matèria de seguretat de la informació.
e) Dur a terme investigacions sobre fets i incidents de seguretat de la informació.
f) Elaborar estudis, propostes de regulació, documents per a facilitar el compliment normatiu i evacuar consultes i informes en la matèria.
g) La difusió de tota mena d'informació i l'organització d'activitats que fomenten el coneixement, el compliment normatiu i les bones pràctiques en matèria de protecció de dades personals i de seguretat de la informació, tant en l'entorn corporatiu com en la societat en general.

En l'exercici de les competències recollides en els apartats *b, c, d, e*, el Departament de Protecció de Dades i Seguretat de la Informació actuarà amb la deguda independència per a assegurar l'objectivitat en les seues actuacions. Quan actue assistint al Delegat de Protecció de Dades, es garantiran les notes d'independència, no conflicte d'interessos i confidencialitat que resulten consubstancials a la figura del Delegat.

Tots els empleats i empleades de la Corporació estan obligats a facilitar tota la informació que els siga requerida pel Departament de Protecció de Dades i Seguretat de la Informació, com també l'accés a locals, instal·lacions, equips, arxius, suports d'emmagatzematge, programes, processos i procediments.

Capítol tercer

El Delegat de Protecció de Dades

Article 36. DESIGNACIÓ I REMOCIÓ

En compliment de l'article 37.5 del RGPD, el Delegat de Protecció de Dades serà designat atenent les seues qualitats professionals i, en particular, els seus coneixements especialitzats del Dret i la pràctica en matèria de protecció de dades i a la seua capacitat per a exercir les funcions indicades en l'article 39 del RGPD.

En l'àmbit de la Diputació de València, el Delegat de Protecció de Dades és designat per resolució del president o presidenta de la Corporació, i el nomenament recaurà en el/la funcionari/ària que reunisca els requisits anteriorment citats.

La designació ha de ser comunicada en el termini de deu dies a l'Agència Espanyola de Protecció de Dades.

Una vegada designat, el Delegat de Protecció de Dades no podrà ser remogut ni sancionat per exercir les seues funcions llevat que incórrega en dol o negligència greu en el seu exercici.

Article 37. FUNCIONS DEL DELEGAT

Seran funcions del Delegat de Protecció de Dades, com a mínim:

a) Informar i assessorar els serveis interns i membres de la Corporació de la normativa legal i interna sobre protecció de dades.
b) Supervisar el compliment de la normativa legal i interna sobre protecció de dades.
c) Supervisar l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
d) Oferir l'assessorament que se li sol·licite sobre l'avaluació d'impacte relativa a la protecció de dades, i supervisar la seua aplicació de conformitat amb l'article 35 del RGPD.
e) Cooperar amb l'Agència Espanyola de Protecció de Dades i, si escau, l'autoritat de control autonòmica.
f) Actuar com a punt de contacte de l'Agència Espanyola de Protecció de Dades i, si escau, l'autoritat de control autonòmica, per a qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36 del RGPD, i realitzar consultes sobre qualsevol altre assumpte.
g) Ser el contacte dels interessats per a les qüestions relatives al tractament de les seues dades personals i a l'exercici dels seues drets.
h) Intervindre en cas de reclamacions davant les autoritats de protecció de dades en els termes de l'article 37 de la LOPDGDD.

I totes aquelles que li puguen ser encomanades per les normes de desenvolupament de la present Política, tot respectant la legislació de protecció de dades i, en qualsevol cas, la normativa de funció pública. D'igual manera, les normes de desenvolupament de la present Política podran concretar i especificar amb major detall les funcions mínimes anteriors, com també els corresponents procediments de treball associats.

Article 38. ACTUACIONS I POSICIÓ DEL DELEGAT EN L'ORGANITZACIÓ

El Delegat de Protecció de Dades actuarà com a interlocutor de la Diputació davant l'Agència Espanyola de Protecció de Dades i, si escau, les autoritats autonòmiques de protecció de dades.

En l'exercici de les seues funcions el Delegat de Protecció de Dades tindrà accés a totes les dades personals i processos de tractament, i no podrà oposar a aquest accés l'existència de qualsevol deure de confidencialitat o secret.

Tots els empleats de la Corporació estan obligats a facilitar tota informació li siga requerida pel Delegat de Protecció de Dades, com també l'accés a locals, instal·lacions, equips, arxius, suports d'emmagatzematge, programes, processos i procediments.

Es considerarà una obstrucció a la labor del Delegat no atendre les obligacions exposades en els dos paràgrafs anteriors, incórrer en dilacions injustificades, establir limitacions i, en general, entorpir les actuacions del Delegat.

Quan el Delegat de Protecció de Dades aprecie l'existència d'una vulneració rellevant en matèria de protecció de dades la documentarà i la comunicarà immediatament a la Presidència de la Corporació. Procedirà d'igual forma quan en l'exercici de les seues competències el Delegat aprecie o tinga coneixement de fets que puguen ser constitutius d'una infracció penal, això sense perjudici del deure de denunciar recollit en l'article 262 de la Llei d'Enjudiciament Criminal.

El Delegat de Protecció de Dades podrà sol·licitar al Responsable dels Sistemes d'Informació TIC la suspensió temporal del tractament d'informacions, prestació de serveis o la total operació en aquells supòsits en els quals aprecie situacions que:

- puguen ser greus per a la seguretat de les dades de caràcter personal, o
- puguen causar un mal irreparable als titulars de les dades personals, o
- signifiquen una violació de la normativa de protecció de dades que siga considerada una infracció molt greu segons l'article 72 LOPDGDD.

Es garantirà la independència del Delegat de Protecció de Dades dins de l'organització:

- evitant qualsevol conflicte d'interessos,
- prohibint que se li donen instruccions pel que fa a l'acompliment de les seues funcions,
- establint les condicions necessàries perquè no s'interferisca en les seues actuacions o es menyscabe la seua competència,
- removent qualsevol actuació que puga implicar un perjudici per als drets o condicions laborals del Delegat, o que el discriminen davant la resta de funcionaris de l'organització o, en general, puga comportar una pressió o influència en la seua presa de decisions.

En compliment de l'article 38.2 del RGPD, la Presidència de la Corporació recolzarà el Delegat de Protecció de Dades en l'acompliment de les seues funcions, tot facilitant els recursos necessaris per a l'acompliment d'aquestes funcions i l'accés a les dades personals i a les operacions de tractament, com també per al manteniment dels seus coneixements especialitzats.

El Delegat de Protecció de Dades rendirà comptes directament davant la Presidència de la Corporació. En tot cas, el Delegat presentarà una memòria anual on informarà de les actuacions dutes a terme en aquest període.

Es garantirà que el Delegat de Protecció de Dades participe de manera adequada i en temps oportú en totes les qüestions relatives a la protecció de dades personals. S'establiran instruccions i procediments interns per a assegurar aquesta participació.

S'habilitaran canals, preferiblement telemàtics, perquè els titulars de les dades, els empleats públics, els encarregats de tractaments i els membres de la Corporació puguen posar-se en contacte amb el Delegat de Protecció de Dades pel que fa a totes les qüestions relatives al tractament de dades personals.

El Delegat de Protecció de Dades estarà obligat a mantindre el secret o la confidencialitat pel que fa a l'acompliment de les seues funcions.

TÍTOL TERCER

Disposicions relatives al personal

Capítol primer

Obligacions i responsabilitats

Article 39. OBLIGACIONS DEL PERSONAL

Tot el personal de la Diputació de València té l'obligació de conéixer i complir aquesta Política de seguretat i de protecció de dades de caràcter personal i la normativa que la desenvolupe, i serà responsabilitat del Comité de Seguretat TIC disposar els mitjans necessaris perquè la informació arribe als afectats.

La normativa interna que desenvolupe la present Política contindrà les especificacions necessàries perquè tot el personal conega perfectament les obligacions que, en atenció a les funcions que exerceix, li són exigibles en el marc de la present disposició.

Article 40. TERCERES PARTS

Quan la Diputació de València preste serveis a altres organismes o manege informació d'altres organismes, se'ls farà partícips d'aquesta Política, i s'establiran canals per a report i coordinació dels respectius Comités de Seguretat TIC, si escau, i procediments d'actuació per a la reacció davant incidents de seguretat.

Quan la Diputació de València utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícips d'aquesta Política i de la normativa de seguretat i de protecció de dades personals que concernisca aquests serveis o informació.

Aquests tercers quedaran subjectes a les obligacions establides en la citada normativa, i podran desenvolupar els seus propis procediments operatius per a satisfer-la.

S'establiran procediments específics de report i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat i protecció de dades personals, almenys al mateix nivell que l'establit en aquesta Política.

Quan algun aspecte de la Política no puga ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es recaptarà un informe del Responsable de Seguretat que precise els riscos en què s'incorre i la manera de tractar-los.

Tots els instruments mitjançant els quals es regulen les relacions entre la Diputació de València i tercers —convenis, contractes, plecs tècnics, etc.— contindran complida referència d'aquesta Política i de les obligacions i responsabilitats de les parts en matèria de seguretat de la informació i protecció de dades de caràcter personal.

Article 41. INCOMPLIMENTS

Als incompliments de la present Política, així com de la normativa que la desenvolupe, comesos pel personal al servei de la Diputació de València els serà aplicable el règim disciplinari legalment establit per la normativa vigent.

Si els incompliments foren comesos per tercers, sobre els quals recaiga l'obligació de compliment en virtut de contracte o qualsevol altre tipus de relació acordada, la responsabilitat els serà exigida en els termes previstos en els instruments que regulen aquestes relacions i per la normativa legal que puga resultar d'aplicació.

Capítol segon

Recursos formatius

Article 42. FORMACIÓ I CONSCIENCIACIÓ

La Diputació de València garantirà la formació i conscienciació a tots els seus empleats públics a través del Servei de Formació incloent les accions formatives necessàries en els plans de formació interna. Les persones amb responsabilitat en l'ús, operació o administració dels sistemes d'informació rebran la formació adequada per al maneig segur dels sistemes i per a un adequat tractament de les dades de caràcter personal, en la mesura en què la necessite per a fer el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seua primera assignació com si es tracta d'un canvi de lloc o de responsabilitat d'aquest.

L'assistència i la realització d'aquestes accions formatives té caràcter obligatori, excepte circumstàncies excepcionals degudament acreditades. El personal que no puga concórrer-hi per aquests supòsits serà inclòs amb caràcter preferent en convocatòries següents.

Al personal amb responsabilitats molt específiques en matèria de seguretat o de protecció de dades de caràcter personal se li facilitarà, de manera preferent, l'assistència a activitats formatives que tinguen relació directa amb aquestes responsabilitats.

El Departament de Protecció de Dades i Seguretat de la Informació dissenyarà i posarà en pràctica activitats dirigides a la conscienciació en ciberseguretat i protecció de dades, i també al foment del compliment de la normativa legal, interna i de bones pràctiques en totes dues matèries.

El Delegat de Protecció de Dades, en l'exercici de la seua competència de supervisar la conscienciació i formació del personal que participa en les operacions de tractament, participarà en la planificació dels programes formatius interns en la matèria i proposarà les accions formatives que considere necessàries en atenció a la situació que a cada moment present l'organització.

El Servei d'Informàtica i el Servei de Formació col·laboraran estretament amb el Delegat i el Departament de Protecció de Dades i Seguretat de la Informació per al compliment efectiu del que es disposa en el present article.

TÍTOL QUART

Desenvolupament i modificació de la Política de Seguretat i de Protecció de Dades de Caràcter Personal

Capítol primer

Instruments de desenvolupament

Article 43. DESENVOLUPAMENT NORMATIU

El desenvolupament de la present Política es durà a terme mitjançant instruments pertanyents a tres nivells, denominats A, B i C. Quan s'aprove un instrument de desenvolupament haurà d'especificar-se el nivell al qual pertany.

Article 43.1. NIVELL A

Pertanyen al nivell A les denominades Normes de Seguretat i de Protecció de Dades de Caràcter Personal.

Estan conformades pel conjunt de regles i directrius de caràcter obligatori que desenvolupen directament el contingut de la present Política o traslladen a l'ordre intern, mitjançant les normes corresponents, el compliment de la normativa legal aplicable en la matèria.

S'integren en aquest nivell:

- Les Normatives de Seguretat (apartat 3.2 org.2 de l'ENS).
- Les Polítiques de Protecció de Dades (article 24.2 del RGPD).

D'igual manera, s'integrarà en aquest nivell qualsevol altra normativa interna que l'òrgan o autoritat competent, segons el que s'estableix en l'article 44.1 de la present disposició, considere necessària per a complir els objectius exposats en el present article.

Article 43.2. NIVELL B

Pertanyen al nivell B els denominats Procediments de Seguretat i de Protecció de Dades de Caràcter Personal.

Estan constituïts pel conjunt de procediments tècnics de caràcter obligatori orientats a resoldre les tasques, processos de treball o maneres d'actuació considerats més rellevants atés el perjudici que causaria una actuació inadequada de seguretat, desenvolupament, manteniment i explotació dels sistemes d'informació, o de protecció de dades de caràcter personal, o per vindre imposats per la legislació aplicable.

S'integren en aquest nivell:

- Els procediments de seguretat (apartat 3.3 org.3 de l'ENS)
- El procediment per al control de l'accés físic a instal·lacions (article 17 de l'ENS).
- El procediment per a assegurar la recuperació i conservació a llarg termini dels documents electrònics (article 21.2 de l'ENS).
- El procediment del Registre d'Activitats de Tractament.
- El procediment de realització de còpies de seguretat i de recuperació de les dades (ex article 32 del RGPD).
- Els procediments per a l'arxiu de suports i documents.
- El procediment per a atendre l'exercici dels drets d'accés, rectificació, supressió, oposició, limitació i portabilitat (articles 15 a 22 del RGPD).
- El procediment de notificació, gestió i resposta davant les incidències i, si escau, bretxes o violacions de seguretat (articles 33-34 del RGPD i 4.3.7 op.exp.7 de l'ENS).
- El procediment d'assignació, distribució i emmagatzematge de contrasenyes (ex article 32 del RGPD).
- Els procediments per al control de les mesures de seguretat i d'auditoria (ex article 32 del RGPD i annex III de l'ENS).

D'igual manera, s'integrarà en aquest nivell qualsevol altre procediment que l'òrgan o autoritat competent, segons el que s'estableix en l'article 44.1 de la

present disposició, considere necessari per a complir els objectius exposats en el present article.

Article 43.3. NIVELL C

Pertanyen al nivell C les denominades Guies de Seguretat i de Protecció de Dades de Caràcter Personal.

Estan conformades pel conjunt de recomanacions i especificacions tècniques i jurídiques, de caràcter esclaridor o orientatiu, tendents a il·lustrar amb major detall aspectes concrets de la seguretat i la protecció de dades personals. El seu objectiu últim és ajudar a la correcta aplicació de les normes i procediments recollits en els nivells A i B, o complementar el seu contingut, com també contribuir a una millor informació i difusió d'aquestes.

S'integren en aquest nivell:

- Les guies tècniques de seguretat.
- Els manuals, informes, monografies, quaderns, estudis tècnics i recomanacions i qualssevol tipus de publicacions.

Capítol segon

Competències de desenvolupament

Article 44. ASSIGNACIÓ DE COMPETÈNCIES DE DESENVOLUPAMENT

Les competències per a l'elaboració i l'aprovació dels instruments de desenvolupament de la present Política s'assignen en funció dels diferents nivells en què s'enquadren, de conformitat amb l'article 43 de la present disposició.

Article 44.1. INSTRUMENTS DE NIVELL A i B

La competència per a l'aprovació de les Normes de Seguretat i de Protecció de Dades de Caràcter Personal, com també dels Procediments de Seguretat i de Protecció de Dades de Caràcter Personal, correspon al president o presidenta de la Diputació de València o al diputat o diputada en qui delegue.

El Comité de Seguretat TIC, el Departament de protecció de Dades i Seguretat de la Informació i el Delegat de Protecció de Dades, cadascun en el marc de les seues competències, formularan les propostes que consideren adequades.

Article 44.2. INSTRUMENTS DE NIVELL C

Correspon al Comité de Seguretat TIC, al Departament de protecció de Dades i Seguretat de la Informació i al Delegat de Protecció de Dades, cadascun en el

marc de les seues competències, l'elaboració de les Guies de Seguretat i de Protecció de Dades de Caràcter Personal.

Capítol Tercer

Modificació de la Política

Article 45. ACTUALITZACIÓ PERMANENT

La present Política haurà de mantindre's actualitzada permanentment per a adequar-la al progrés dels serveis d'Administració Electrònica, a l'evolució tecnològica i al desenvolupament de la societat de la informació, com també a les previsions legals que pogueren afectar-lo.

Article 46. PROCEDIMENT PER A LA MODIFICACIÓ

Les propostes de les successives revisions de la present Política s'elaboraran pel Comité de Seguretat TIC i pel Departament de Protecció de Dades i Seguretat de la Informació, i es traslladaran, a través del president/a al Ple de la Corporació, únic òrgan competent per a acordar qualsevol modificació d'aquesta Política.

DISPOSICIÓ DEROGATÒRIA

Única. DEROGACIÓ NORMATIVA

1. Queda derogat el Reglament de Política de Seguretat i de la Protecció de Dades de Caràcter Personal de la Diputació de València, aprovat pel Ple de la Corporació en sessió de 18 de juny de 2013, BOP núm. 159, de 6 de juliol.

2. Així mateix, queden derogades totes les disposicions d'igual o inferior rang que contradiguen, s'oposen, o resulten incompatibles amb el que es disposa en la present disposició.

DISPOSICIÓ TRANSITÒRIA

Única. NORMATIVA INTERNA VIGENT

La normativa interna aprovada en desenvolupament del Reglament que se cita en la disposició derogatòria continuarà sent aplicable mentre s'aproven les normatives de desenvolupament de la present disposició que les substituïsquen, en la mesura en què no incórreguen en els supòsits als quals es refereix l'apartat 2 de la disposició derogatòria.

DISPOSICIONS FINALS

Primera. CONSTITUCIÓ DEL COMITÉ DE SEGURETAT TIC

El nou Comité de Seguretat TIC haurà de quedar constituït en un termini no superior a tres mesos des de l'entrada en vigor de la present disposició.

Les actes, acords i qualsevol altra documentació referida al període d'actuació del Comité de Seguretat TIC constituït a l'empara del Reglament anterior, hauran de ser transferits al nou Comité en el moment que es constituïsca.

Segona. DESENVOLUPAMENT NORMATIU

El desenvolupament de la present Política, a través dels instruments establits en l'article 43.1, haurà de dur-se a terme en un termini màxim de sis mesos des de l'entrada en vigor d'aquesta.

Quan es tracte dels instruments contemplats en l'article 43.2, caldrà tindre aprovats dins del termini citat anteriorment aquells procediments considerats com a crítics per a la seguretat dels sistemes d'informació afectats.

Tercera. POLÍTIQUES D'ÀMBIT MUNICIPAL

La Diputació de València podrà elaborar, a l'empara del paràgraf segon de l'article 11.2 ENS, polítiques de seguretat i de protecció de dades personals comunes per als municipis de la província que desitgen adherir-se a elles.

En la configuració d'aquestes Polítiques es tindran en consideració aquells elements que resulten homogenis a l'hora de determinar el conjunt dels seus destinataris, com ara la població, el nivell d'infraestructures i serveis TIC, els recursos organitzatius, el grau de dependència de l'assistència de la Diputació o la possible transferència de competències de l'àmbit municipal al provincial.

Quarta. ENTRADA EN VIGOR

La present disposició entrarà en vigor als 15 dies hàbils des de la data de la seua publicació en el BOP.