Excel·lentíssima Diputació Provincial de València
Departament de Protecció de Dades i Seguretat de la Informació

Anunci de l'Excel·lentíssima Diputació Provincial de València sobre aprovació definitiva del reglament pel qual es regula la política de seguretat i de la protección de dades de caràcter personal en esta corporació.

Anuncio de la Excelentísima Diputación Provincial de València sobre aprobación definitiva del reglamento por el cual se regula la política de seguridad y de la protección de datos de carácter personal en esta corporación.

ANUNCI

En el BOP núm. 89, d'11 de maig de 2022, es va publicar l'anunci de l'aprovació inicial i exposició pública del Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació de València, segons acord adoptat en sessió ordinària del Ple de 26 d'abril de 2022.

Transcorregut el termini d'exposició pública de 30 dies sense que s'haja presentat reclamació o suggeriment, segons informe del Registre General de la Secretaria General de 27 de juny de 2022, el Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació de València s'entén definitivament aprovat, procedint-se a la publicació en el Butlletí Oficial de la Província de València del text íntegre d'aquest Reglament, en compliment del que es disposa en l'article 70.2 de la Llei 7/1985, de 2 d'abril, Reguladora de les Bases de Règim Local. El Reglament entrarà en vigor als quinze dies hàbils a partir del de la seua publicació.

Contra el present acord, es podrà interposar recurs contenciós administratiu, davant la Sala Contenciosa Administrativa del Tribunal Superior de Justícia de la Comunitat Valenciana, en el termini de dos mesos a comptar des de l'endemà a la publicació del present anunci, de conformitat amb l'article 46 de la Llei 29/1998, de 13 de juliol, reguladora de la Jurisdicció contenciosa administrativa.

València, a 27 de juny de 2022.—El secretari general, Vicente Rafael Boquera Matarredona.

Reglament pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València

Índex

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 esta entitat.

Article 3. ABAST

Esta 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 esta 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 estes 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. Esta 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'art. 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'estes.

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'estes 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.

ANUNCIO

En el BOP n.º 89, de 11 de mayo de 2022, se publicó el anuncio de la aprobación inicial y exposición pública del Reglamento por el cual se regula la política de seguridad y de la protección de datos de carácter personal en la Diputación de València, según acuerdo adoptado en sesión ordinaria del Pleno de 26 de abril de 2022.

Transcurrido el plazo de exposición pública de 30 días sin que se haya presentado reclamación o sugerencia, según informe del Registro General de la Secretaría General de 27 de junio de 2022, el Reglamento por el cual se regula la política de seguridad y de la protección de datos de carácter personal en la Diputación de València se entiende definitivamente aprobado, procediéndose a la publicación en el Boletín Oficial de la Provincia de València del texto íntegro de este Reglamento, en cumplimiento de lo dispuesto en el artículo 70.2 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local. El Reglamento entrará en vigor a los quince días hábiles a partir del de su publicación.

Contra el presente acuerdo, se podrá interponer recurso contencioso-administrativo, ante la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de la Comunidad Valenciana, en el plazo de dos meses a contar desde el día siguiente a la publicación del presente anuncio, de conformidad con el artículo 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción contencioso-administrativa.

València, a 27 de junio de 2022.—El secretario general, Vicente Rafael Boquera Matarredona.

Reglamento por el cual se regula la política de seguridad y de la protección de datos de carácter personal en la Diputación Provincial de València

Índice

Para el cumplimiento de su misión, la prestación de los servicios identificados y el cumplimiento de sus objetivos, la Diputación de Valencia depende de los sistemas TIC (Tecnologías de la Información y Comunicaciones). Estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada o de los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de ésta y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas se requiere una estrategia que se adapte a los cambios en las condiciones del entorno, para garantizar la prestación continua de los servicios.

A mayor abundamiento, en el específico marco de la administración electrónica, la antigua Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, proclamaba como uno de sus fines crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos. La actual norma de aplicación en la materia, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas recuerda además que el desarrollo de las TIC también ha venido afectando profundamente a la forma y al contenido de las relaciones de la Administración con los ciudadanos y las empresas.

Es por ello que el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, establece que Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.

Por su parte, la aplicación de la normativa sobre protección de datos de carácter personal supone para esta Corporación, en tanto responsable y encargada de tratamientos de esta naturaleza, la necesaria adopción de una serie de medidas de carácter técnico y organizativo tendentes a garantizar los derechos de los titulares de dichos datos personales. En este sentido, la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, determina que los responsables enumerados en el artículo 77.1 de esta ley orgánica –sector público- deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad. En consecuencia, la convergencia de los requisitos de seguridad sobre los sistemas de información TIC y de los reclamados por la protección de datos de carácter personal en una misma norma (ENS) hace aconsejable no acometer acciones desagregadas, que atiendan a cada dimensión por separado, pues ello podría provocar duplicidades, antinomias, confusión y descoordinación internas, además de resultar más oneroso desde el punto de vista de la inversión de recursos humanos, económicos, técnicos y organizativos.

En su virtud, y para dar respuesta a las necesidades expuestas anteriormente, el Pleno de la Diputación de Valencia aprobó el Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia -BOP N.º 159, de 6-VII-2013-, el cual fue desarrollado mediante el Decreto nº 6353, de 3 de julio de 2015, del Diputado de Modernización, por el que se aprueban las Normas de Seguridad para el Personal Técnico de los Sistemas de Información TIC; el Decreto nº 6111, de 26 de junio de 2015, del Diputado de Modernización, por el que se aprueban las Normas de Seguridad para los Usuarios de los Sistemas de Información; el Decreto nº5448, de 12 de junio de 2015, del Diputado de Modernización, por el que se aprueba Normativa de Protección de Datos de Carácter Personal; y el Decreto nº 6110, de 26 de junio de 2015, del Diputado de Modernización, por el que se aprueban los Procedimientos de Protección de Datos de Carácter Personal. Tras la aprobación de las normas citadas anteriormente se han producido cambios importantes. Dichos cambios son de diferente naturaleza: Avances tecnológicos, nuevas amenazas cibernéticas, cambios geopolíticos, modificación de hábitos sociales, alteración de la organización administrativa de la Corporación, incidencia de pandemias y nueva producción legislativa tanto del entorno europeo como nacional. La suma de dichos cambios nos sitúa en un escenario diferente al existente en el momento en que se elaboraron las normativas internas expuestas.

Precisamente la nueva producción legislativa ha tenido una incidencia notable en los dos ámbitos de referencia, la protección de datos personales y la seguridad de la información. El régimen normativo en materia de protección de datos personales vigente durante los casi 20 últimos años ha sido desplazado por sendas normas, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos -en adelante RGPD- y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los

derechos digitales (LOPDGDD). Por lo que se refiere al ENS, en el momento actual se ha elaborado un proyecto legislativo que habrá de sustituir el texto del RD 3/2010, obedeciendo el mismo a la directriz contenida en el Plan de Digitalización de las Administraciones Públicas, uno de los instrumentos principales para la ejecución de los fondos del Componente 11 «Modernización de las Administraciones Públicas» del Plan de Recuperación, Transformación y Resiliencia, así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025, la cual contempla la actualización del ENS entre las reformas normativas a abordar con el fin de evolucionar la política de seguridad de las Administraciones Públicas españolas, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información.

En conclusión, resulta necesario aprobar una nueva normativa que, en el ámbito interno de la Diputación de Valencia, sustituya a la anterior, incorporando esta nueva realidad tecnológica, social, organizativa interna y legislativa y proporcionando la debida actualidad a la regulación de la actividad propia de la Corporación.

Para la elaboración de la presente disposición se ha tenido en consideración la siguiente legislación: Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (con su modificación por Real Decreto 951/2015, de 23 de octubre), el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como las denominadas instrucciones técnicas de seguridad y las guías de seguridad de las tecnologías de la información y las comunicaciones (serie CCN-STIC) elaboradas por el Centro Criptológico Nacional para el mejor cumplimiento de lo establecido en el ENS –artículo 29 ENS-, además de las resoluciones, informes y guías de la Agencia Española de Protección de Datos, adecuando todo ello a la realidad orgánica y funcional de la Diputación de Valencia.

Titulo preliminar

Ámbito de aplicación y disposiciones generales

Capítulo Primero

Disposiciones comunes

Artículo 1. Objeto

El presente reglamento tiene por objeto definir y regular, en el ámbito de la Diputación de Valencia, la Política de seguridad y de protección de datos de carácter personal aplicable a los sistemas de información que intervengan en el tratamiento de la información que resulte necesaria para el ejercicio de sus competencias.

Artículo 2. Definiciones

A efectos de la presente disposición se entenderá por:

• Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

• Análisis de riesgos. Estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en el organismo (en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

• Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de dichos controles, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

• Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

• Ciberincidente. Incidente de seguridad el ámbito de los Sistemas de Información y las Comunicaciones.

• Ciberseguridad. La protección de las redes y sistemas de información, sus usuarios y otras personas frente a las ciberamenazas.

• Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

• Datos personales. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

• Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

• Encargado del tratamiento o encargado. La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

• Incidente de seguridad. Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información.

• Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

• Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

• Responsable del tratamiento o responsable: La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

• Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

• Riesgo residual. Es el riesgo resultante de la aplicación de contramedidas y, por tanto, constituye el riesgo a asumir.

• Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

• Sistema de información TIC. Sistema de información que emplea tecnologías de la información y de las comunicaciones.

• Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Artículo 3. Alcance

Esta Política se aplica a todos los sistemas de información TIC, así como a aquellos sistemas de información de cualquier naturaleza que traten datos de carácter personal, que sean de la titularidad de la Diputación de Valencia o cuya gestión o responsabilidad tenga encomendada.

Cuando la información cuya titularidad, gestión o responsabilidad corresponda a la Diputación de Valencia se encuentre o trate en entornos ajenos, la Diputación exigirá las mismas garantías y requisitos que las determinadas en la presente Política.

Sin perjuicio de lo anterior, la Diputación aplicará la presente Política en el marco de sus relaciones con las entidades locales de su territorio, respetando en cualquier caso la autonomía de aquéllas y sus facultades de gestión y control sobre la información y los servicios que les son propios. La Diputación promoverá acuerdos con dichas entidades locales para el intercambio de la información necesaria que facilite las garantías y el cumplimiento legal en materia de seguridad y de protección de datos personales en los sistemas de información afectados.

Queda excluida de forma específica de la aplicación de la presente Política la información tratada por los grupos políticos y/o sus miembros, las centrales sindicales y/o miembros representantes de los trabajadores, siempre que dicha información no forme parte de los activos de información titularidad de la Corporación.

La normativa que desarrolle el presente Reglamento establecerá las condiciones de uso de los activos de los sistemas de información corporativos y de los dispositivos puestos a disposición de estos colectivos.

Artículo 4. Ámbito subjetivo de aplicación

Las presentes disposiciones son de aplicación a todos los departamentos y unidades de la Diputación de Valencia. Los entes u organismos públicos vinculados o dependientes de la Diputación de Valencia adoptarán su propia Política de seguridad y de protección de datos de carácter personal, que deberá adecuarse en la medida de lo posible a las presentes prescripciones.

Capítulo Segundo

Misión y marco legal

Artículo 5. Misión

La Diputación de Valencia es una entidad local de ámbito provincial que tiene las siguientes competencias:

a. La coordinación de los servicios municipales entre sí para la garantía de la prestación integral y adecuada en la totalidad del territorio provincial de los servicios mínimos de competencia municipal.

b. La asistencia y la cooperación jurídica, económica y técnica a los Municipios, especialmente los de menor capacidad económica y de gestión.

c. La prestación de servicios públicos de carácter supramunicipal y, en su caso, supracomarcal.

d. La cooperación en el fomento del desarrollo económico y social y en la planificación en el territorio provincial, de acuerdo con las competencias de las demás Administraciones Públicas en este ámbito.

e. En general, el fomento y la administración de los intereses peculiares de la provincia.

f. Cualesquiera otras que les sean atribuidas por las leyes del Estado y de la Comunidad Autónoma en los diferentes sectores de acción pública.

Artículo 6. Marco legal

En su calidad de administración pública, la Diputación de Valencia lleva a cabo las competencias que le son propias con pleno sometimiento al Ordenamiento Jurídico, en general, y en especial:

a. A la normativa sobre régimen jurídico local - Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local; Real Decreto Legislativo 781/1986, de 18 de abril, por el que se aprueba el texto refundido de las disposiciones legales vigentes en materia de Régimen Local; Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales; Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales; y Ley 8/2010, de 23 de junio, de la Generalitat, de Régimen Local de la Comunitat Valenciana-

b. A la normativa sobre procedimiento administrativo y contratación - Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público-

De igual forma, en la utilización de medios tecnológicos para el desarrollo de sus actividades, le son de especial aplicación:

a. La normativa sobre administración electrónica -Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público; Decreto 220/2014, del Consell, por el que se aprueba el Reglamento de administración electrónica de la Comunidad Valenciana; Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica; Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica; Real Decreto 203/2021, de 30 de marzo (BOE 31/03/2021) por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos; Reglamento de desarrollo de la Administración Electrónica de la Diputación de Valencia (BOP 30/09/2013)-

b. La normativa sobre firma electrónica - Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza-

c. La normativa sobre protección de datos de carácter personal - el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Título primero

Principios de seguridad TIC y de la protección de datos de carácter personal

Capítulo Primero

Principios comunes

Artículo 7. Seguridad coordinada y estructurada

La seguridad de los sistemas de información se abordará aplicando de forma coherente y coordinada esta Política, las normas que la desarrollen y el referente legislativo del ENS a cualquier tipo de información tratada en dichos sistemas, atendiendo a la previsión que en materia de seguridad de los datos personales contiene la Disposición adicional primera de la Ley 3/2018 LOPD-GDD.

De igual forma, a la hora de ejecutar las actividades de la seguridad de la información se respetarán los principios de competencia y separación de funciones establecidos en el presente Reglamento, conforme a las atribuciones conferidas a cada componente de la estructura de organización de la seguridad y de la protección de datos personales.

Artículo 8. Acceso a la información

Los derechos de acceso de los usuarios a la información se regirán por los siguientes principios:

a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Artículo 9. Ciclo vital de la información

La seguridad y la protección de los datos de carácter personal estarán presentes durante todo el ciclo de vida de la información.

La normativa que desarrolle la presente Política deberá establecer los criterios y requisitos que deberá cumplir la recogida, utilización, publicación, transferencia e intercambio de la información, así como su destrucción o destino final tras cumplir su ciclo de vida útil, con el objetivo de garantizar los anteriores principios de seguridad y de protección de datos de carácter personal.

Artículo 10. Deber de secreto

Todos los usuarios están obligados a guardar secreto profesional de toda aquella información de la que tengan conocimiento con ocasión del ejercicio de su cargo o actividad profesional. Esta obligación se mantendrá incluso después de haber finalizado la relación con la Diputación de Valencia.

El deber de confidencialidad y secreto profesional se establecerá de forma expresa en todo tipo de relaciones –administrativas, civiles o mercantiles - que impliquen o supongan acceso o tratamiento de la información, incluidos los servicios de simple alojamiento, transporte o soporte técnico.

Capítulo Segundo

Principios de seguridad TIC

Artículo 11. Proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema de información.

En su virtud, cualquier acción dirigida al objetivo de la seguridad debe considerar la interacción de todos los elementos citados, lo cual excluye cualquier actuación puntual o tratamiento coyuntural.

Para evitar que la ignorancia, la falta de organización y coordinación, o instrucciones inadecuadas, sean fuentes de riesgo para la seguridad deberá procederse, en especial, a la concienciación y formación adecuada de las personas que intervienen en el proceso y a sus responsables jerárquicos.

Artículo 12. Gestión basada en riesgos

La gestión de la seguridad se apoyará en un proceso continuo de análisis y tratamiento de riesgos. Este proceso deberá mantenerse actualizado de modo permanente.

La gestión de riesgos debe permitir el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Todos los sistemas de información sujetos a esta Política de seguridad deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el ENS.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC podrá establecer una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Artículo 13. Prevención

Los departamentos internos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de la evaluación de amenazas y riesgos. Estos controles y los roles y responsabilidades de seguridad de todo el personal deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la presente Política, se deberá:

▪ Autorizar los sistemas antes de entrar en operación.

▪ Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

▪ Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Artículo 14. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte, que lleguen a los responsables regularmente, y cuándo se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Artículo 15. Respuesta

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

Deberán establecerse mecanismos para responder eficazmente a los incidentes de seguridad, designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en los departamentos y establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

En el ámbito de la Diputación de Valencia deberá crearse un Grupo de Respuesta a Incidentes TIC (Grupo RITIC), cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos de la Corporación. El Grupo RITIC estará formado por miembros designados por el Comité de Seguridad TIC.

Artículo 16. Conservación

Los sistemas de información garantizarán la conservación de los datos e informaciones en soporte electrónico. De igual modo, los sistemas mantendrán disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Capítulo Tercero

Principios de la protección de datos de carácter personal

Artículo 17. Licitud, transparencia y lealtad.

Los datos deben ser tratados de manera lícita, leal y transparente para el interesado.

Todos los medios que sean utilizados para recabar datos de carácter personal deberán guardar la transparencia y proporcionar al interesado la información a que hace referencia el artículo 11 de la LOPDGDD, con las excepciones legalmente contempladas.

Tanto la sede electrónica de la Diputación de Valencia, como cualquier espacio en Internet o tecnologías similares de cuyos contenidos sea responsable la Corporación, contendrá referencia al Registro de Actividades de Tratamiento, las políticas y normativas internas sobre protección de datos de carácter personal y, en particular, de los derechos que asisten a los titulares de los datos.

Mediante procedimientos internos se garantizará, previamente a su activación, que los medios y espacios anteriormente citados cumplen debidamente los requisitos establecidos.

Artículo 18. Protección de datos desde el diseño

Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que estén basados en el tratamiento de datos personales o que traten datos personales para cumplir su función, ha de inclinarse por aquellos que tengan en cuenta el derecho a la protección de datos cuando se desarrollan y diseñan estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.

Todos los departamentos de la Corporación deberán tener en cuenta a la hora de incorporar nuevos tratamientos de datos personales que, previamente a su ejecución, se consideran en su diseño y desarrollo las acciones que garanticen el cumplimiento de las garantías de protección de datos personales.

Artículo 19. Derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad.

Deberá establecerse un procedimiento interno que asegure el ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad a los titulares de los datos de carácter personal. Este procedimiento deberá ser común a todos los tratamientos de los que sea responsable la Corporación, salvo que las leyes aplicables a determinados tratamientos establezcan un procedimiento especial para la rectificación o supresión de los datos tratados.

Se adoptarán las medidas oportunas para garantizar que el personal de la Corporación que tiene acceso a datos de carácter personal pueda informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

En sede electrónica se habilitará un espacio para ofrecer información a los afectados sobre el contenido de dichos derechos y el procedimiento a seguir para ejercitarlos, así como un canal electrónico para su ejercicio, preferentemente a través de la misma sede electrónica de la Corporación.

Artículo 20. Comunicación de datos

Sólo con el consentimiento del interesado, siempre que una norma no lo impida, o al amparo de alguno de los supuestos recogidos expresamente en la normativa sobre protección de datos personales podrá procederse a la comunicación o cesión de los datos.

Cuando, con soporte legal y sin ser preceptivo el consentimiento del interesado, deba publicarse información considerada como dato de carácter personal, el contenido de dicha publicación será el estrictamente necesario para cumplir el objetivo perseguido, preservando lo máximo posible la intimidad del afectado. De igual forma, se optará por aquellos medios de publicidad que comporten menor nivel de injerencia en el derecho a la intimidad y a la protección de datos de carácter personal.

Siempre que sea posible se disociarán los datos aplicando, según proceda, técnicas de seudonimización o anonimización, y el cifrado de los datos.

Artículo 21. Acceso a datos por cuenta de terceros

Cuando la Diputación vaya a encomendar a un tercero la realización de un tratamiento por su cuenta, elegirá únicamente un encargado

que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos de la legislación de protección de datos, del presente Reglamento y sus normas de desarrollo, garantizando la protección de los derechos de los titulares de los datos.

Para que la Diputación de Valencia otorgue a terceros el acceso a datos de carácter personal, cuando el citado acceso sea necesario para que dichos terceros presten un servicio a la Diputación, deberá formalizarse previamente a dicho acceso a datos un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable, con el contenido mínimo regulado en el art. 28.3 RGPD. Dicho contrato o acto jurídico estipulará, en particular, que el encargado deberá ofrecerlas garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido denle el RGPD.

De igual forma, la Diputación de Valencia se abstendrá de actuar en calidad de encargado del tratamiento cuando dicha prestación requiera el acceso a datos de carácter personal si no se llevan a cabo las previsiones anteriores, aunque el responsable del tratamiento no le exigiera el cumplimiento de las mismas.

Artículo 22. Responsabilidad proactiva

Se aplicarán las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con la normativa legal e interna en la materia.

Cuando resulte preceptivo recabar el consentimiento del interesado para la recogida, tratamiento o cesión de sus datos, se utilizarán medios que permitan dejar constancia fehaciente del mismo.

Título segundo

Organización de la seguridad y de la protección de datos personales

Capítulo Primero

Principios comunes

Artículo 23. Responsabilidad general y específica

Todos y cada uno de los usuarios de los sistemas de información de la Diputación de Valencia son responsables de la seguridad de los activos tecnológicos puestos a su disposición mediante un uso correcto de los mismos, así como de la seguridad de la información y de los datos de carácter personal que manejan, siempre de acuerdo con sus atribuciones profesionales.

No obstante, el mantenimiento y gestión de la seguridad de los sistemas de información y de la protección de datos personales van íntimamente ligados al establecimiento de una organización. Dicha organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas de información y de la protección de datos personales, y la implantación de una estructura que las soporte.

Artículo 24. Estructura organizativa

En los siguientes apartados se especifica la estructura básica de la organización de la seguridad y de la protección de datos personales en los sistemas de información que regirá en la Diputación de Valencia. Las figuras y las responsabilidades a ellas asociadas tienen carácter de mínimos, pudiéndose desarrollar los contenidos a través de la normativa interna de seguridad y de la protección de datos personales, que respetará, en cualquier caso, lo establecido en la presente disposición.

Artículo 25. Resolución de conflictos

En caso de conflicto entre las diferentes figuras que componen la estructura organizativa, prevalecerá la decisión del Comité de Seguridad TIC siempre que el conflicto no afecte a la aplicación de la normativa legal o interna en materia de protección de datos personales. Para decidir sobre el conflicto, el Comité tomará como referencia el marco de competencias y responsabilidades de las citadas figuras establecido por la presente Política y sus normas de desarrollo.

Cuando el conflicto afecte a la aplicación de normativa legal o interna en materia de protección de datos personales, prevalecerá el criterio del Delegado de Protección de Datos.

Capítulo Segundo

Figuras y responsabilidades

Artículo 26. Responsable del servicio

El responsable del servicio es quien tiene la potestad de establecer las características de un servicio, a los efectos de determinar los requisitos en materia de seguridad y de protección de datos personales.

Al responsable del servicio le corresponde:

- la valoración del servicio en todas las dimensiones de seguridad –disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad- teniendo en cuenta la naturaleza del servicio y la normativa que pudiera serle de aplicación.
- la propiedad de los riesgos sobre los servicios.
- aceptar el riesgo residual sobre los servicios que le competen.

Artículo 27. Responsable de la información

El responsable de la información es quien tiene la potestad de establecer las características de una información, a los efectos de determinar los requisitos en materia de seguridad y de protección de datos personales.

Sin perjuicio de lo que se disponga en procedimientos o disposiciones en desarrollo del presente Reglamento sobre cada una de las figuras contempladas en este Capítulo, al responsable de la información le corresponde:

- la valoración de la información en todas las dimensiones de seguridad –disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad- teniendo en cuenta la naturaleza de dicha información y la normativa que pudiera serle de aplicación.
- adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de la información y de los tratamientos de datos de carácter personal de que resulte responsable establecidas por la normativa interna.
- la responsabilidad última de la protección de la información respecto al uso que de ella hagan las personas a su cargo, o las que dependan de su dirección, o, en general, aquellas que sean autorizadas por él para acceder a la información.
- la propiedad de los riesgos sobre la información.
- aceptar el riesgo residual sobre la información que le compete.
- autorizar los accesos de los usuarios a la información, respetando los principios de mínimo privilegio y necesidad de conocer establecidos en la presente Política.
- la responsabilidad última del cumplimiento de todas las garantías establecidas por la legislación y la normativa interna de la Corporación, especialmente cuando la información consista en datos de carácter personal.
- la responsabilidad última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad de la información, cuando no haya atendido debidamente el deber de velar por el cumplimiento de las garantías aludidas en el apartado anterior.

Artículo 28. Disposiciones comunes al responsable del servicio y al responsable de la información

Serán responsables del servicio y de la información el personal directivo –Jefes/as de Servicio, Jefes/as de Oficina, Directores/as, Coordinadores/as, etc- bajo cuya dirección técnica se encuentre el correspondiente servicio y la información.

En los supuestos de información y servicios bajo la dirección exclusiva del personal eventual a que se refiere el artículo 12 del EBEP, será este personal el considerado responsable del servicio y de la información.

La responsabilidad de la valoración de la información y de los servicios es exclusivamente del responsable correspondiente. La valoración podrá ser propuesta por el Responsable de Seguridad de los Sistemas de Información, y aprobada por el responsable de la información y del servicio correspondiente si éste la considera adecuada.

La normativa que desarrolle la presente Política establecerá los criterios y los instrumentos que permitan una adecuada valoración de los servicios e informaciones por parte de sus correspondientes responsables.

Artículo 29. Responsable de seguridad de los sistemas de información

El Responsable de Seguridad es quien determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

Para el mejor cumplimiento de las funciones relacionadas con las medidas de seguridad implantadas y, especialmente, por razones de complejidad o inmediatez, el Responsable de Seguridad de los Sistemas de Información podrá delegar determinados aspectos de dichos cometidos en otras personas de la organización. En estos supuestos, los diferentes responsables de seguridad delegados actuarán ajustándose estrictamente al contenido de la delegación, la cual recogerá el alcance material y temporal, las obligaciones y responsabilidades de las tareas delegadas. De las posibles delegaciones deberá darse cuenta al Comité de Seguridad TIC.

Serán funciones del Responsable de Seguridad de los Sistemas de Información:

- Actuar como Secretario del Comité de Seguridad TIC.

- Convocar al Comité de Seguridad TIC, recopilando la información pertinente.

- Ser responsable, junto con los diferentes responsables de seguridad delegados, en su caso, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que puedan afectar directa o indirectamente a la seguridad de los sistemas de información de la Corporación, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad TIC y proponiendo las acciones oportunas de adecuación al nuevo marco normativo.

- Elaborar y firmar las pertinentes Declaraciones de Aplicabilidad de los sistemas de información.

- Ser el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad TIC. Estas decisiones estarán presididas por los principios de unidad de acción y coordinación de actuaciones en general y, en especial, en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.

- En caso de desastre se incorporará al Grupo RITIC y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de los sistemas de información.

- Coordinar sus actuaciones con el Departamento de Protección de Datos y Seguridad de la Información y colaborar con este en todos aquellos aspectos que puedan incidir en las competencias atribuidas a dicho Departamento.

Y cualesquiera otros cometidos que le sean encargados por la presente Política y por la Dirección de la Corporación.

Será Responsable de Seguridad de los Sistemas de Información en el ámbito de la Diputación de Valencia quien designe el Comité de Seguridad TIC.

Artículo 30. Responsable de los sistemas de información TIC

Corresponderá al Responsable de los Sistemas de Información TIC:

- Desarrollar, operar y mantener los Sistemas de Información TIC durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y sistema de gestión de los Sistemas de Información TIC estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- Acordar la suspensión del manejo de una cierta información o la prestación de un determinado servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con el Responsable de la Información afectada, del Servicio afectado y el Responsable de Seguridad de los Sistemas de Información antes de ser ejecutada.

Será Responsable de los Sistemas de Información TIC en el ámbito de la Diputación de Valencia el Jefe de Servicio de informática.

Considerando la complejidad, distribución, separación física de sus elementos o número de usuarios que habitualmente comporta la gestión de los actuales sistemas de información, así como la realidad funcional de quienes han de compaginar las responsabilidades derivadas de la presente disposición con sus competencias habituales, el Responsable de los Sistemas de Información TIC podrá delegar determinados aspectos de sus cometidos en otras personas de la organización. En estos supuestos, los diferentes responsables de sistemas de información delegados actuarán ajustándose estrictamente al contenido de la delegación, la cual recogerá el alcance material y temporal, las obligaciones y responsabilidades de las tareas delegadas. De las posibles delegaciones deberá darse cuenta al Comité de Seguridad TIC.

En ningún caso podrá ser objeto de delegación la competencia para acordar la suspensión del manejo de cierta información o la prestación de un determinado servicio, en los términos citados en el presente artículo.

Artículo 31. Administrador de seguridad de los sistemas de información TIC

El Administrador de Seguridad es el responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables a los Sistemas de Información TIC.

Será Administrador de Seguridad de los sistemas de información TIC en el ámbito de la Diputación de Valencia el Jefe de Servicio de informática.

El Administrador de Seguridad de los Sistemas de Información TIC podrá delegar determinados aspectos de sus cometidos en otras personas de la organización. En estos supuestos, los diferentes administradores de seguridad delegados actuarán ajustándose estrictamente al contenido de la delegación, la cual recogerá el alcance material y temporal, las obligaciones y responsabilidades de las tareas delegadas. De las posibles delegaciones deberá darse cuenta al Comité de Seguridad TIC.

Artículo 32. Comité de seguridad TIC

Es el órgano que gestiona y coordina la Seguridad de los sistemas de información TIC a nivel de organización.

Se crea el Comité de Seguridad TIC de la Diputación de Valencia, como un órgano colegiado de carácter horizontal, que se regirá en su funcionamiento por esta disposición y, en lo no previsto en ella, será de aplicación supletoria la normativa reguladora de los órganos colegiados contenida en la Subsección 2ª de la Sección 3ª del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El Comité de Seguridad TIC se reunirá con carácter ordinario, al menos, una vez por semestre. Por razones de urgencia podrá reunirse siempre que la Presidencia del Comité lo estime conveniente. Las reuniones tendrán lugar dentro de la jornada de trabajo establecida reglamentariamente.

El Comité podrá acordar la constitución de comisiones delegadas de trabajo, para tratar temas, elaborar estudios o informes, o llevar a cabo cualquier otra gestión que por su especificidad o complejidad técnica así se considere.

El Comité podrá regular su propio régimen de funcionamiento, el cual deberá respetar, en cualquier caso, lo dispuesto en la presente disposición y la normativa que resulte de aplicación.

El Comité está compuesto por:

- El Jefe de Servicio de Informática, que asumirá la Presidencia del Comité.

- El Secretario general de la Corporación, que ostentará la Vicepresidencia del Comité.

- El Responsable de Seguridad de los Sistemas de Información, que actuará como Secretario del Comité.

- Los diferentes Responsables de Sistemas de Información, Responsables de seguridad y Administradores de seguridad delegados.

- Una persona designada por el Departamento de Protección de Datos y Seguridad de la Información, que actuará con voz pero sin voto.

- El Delegado de protección de datos de la Corporación, que actuará en funciones de información y asesoramiento en materia de protección de datos pero no participará en la toma de decisiones.

El Comité desempeñará las siguientes funciones:

• Coordinar todas las funciones de seguridad de los sistemas de información TIC de la Corporación.

• Velar por el cumplimiento de la legislación y normativa interna de aplicación.

• Recabar del Responsable de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes. Estos informes se consolidan y resumen para la Dirección de la Corporación.

• Atender las peticiones de información que pueda requerir el Departamento de Protección de Datos y Seguridad de la Información,

así como las recomendaciones y propuestas efectuadas por dicho Departamento.

• Coordinar y dar respuesta a las inquietudes transmitidas a través del Responsable de Seguridad.

• Dinamizar la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas de información, promoviendo inversiones de carácter horizontal.

• Designar a los componentes del Grupo RITIC indicado en el artículo 15 de la presente disposición.

Y cualesquiera otros cometidos que les sean encargados por la presente Política y por la Dirección de la Corporación.

El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones.

Artículo 33. Delegado de protección de datos

El delegado de protección de datos es el garante en el seno de la Corporación del cumplimiento de la legislación europea y nacional sobre protección de datos de carácter personal, así como de la normativa interna en la materia.

La regulación de esta figura está recogida en los artículos 36 a 38 de la presente Política.

Será delegado de protección de datos en el ámbito de la Diputación de Valencia el funcionario designado por el/la Presidente/a de la Diputación.

Artículo 34. Centro gestor del tratamiento

Es la unidad administrativa responsable de un tratamiento de datos personales, en atención a criterios como:

a) Ser la unidad que presta el servicio o tiene la competencia para cuyo fin se tratan los datos personales

b) Ser la unidad que decide sobre la creación, finalidad y/o tipo de datos del tratamiento o el uso de los datos personales

c) Ser la principal o mayor usuaria de los datos personales

En cualquier caso, será competencia del Delegado de Protección de Datos el estudio, valoración y determinación de las unidades que deben ser Centro Gestor del Tratamiento en cada supuesto concreto.

En relación con el tratamiento de datos del que es responsable, a cada centro gestor del tratamiento le corresponde:

• Comunicar al Delegado de Protección de Datos la intención de proceder a un nuevo tratamiento, previamente a su iniciación, así como las variaciones y ceses en los tratamientos ya iniciados.

• Mantener actualizada la información en el Registro de Actividades de Tratamiento de la Corporación de los tratamientos que sea responsable.

Artículo 35. Departamento de protección de datos y seguridad de la información

Al departamento de Protección de Datos y Seguridad de la Información le corresponde:

a) Proporcionar apoyo técnico, humano y organizativo al Delegado de Protección de Datos, asistiéndole en el ejercicio de sus competencias.

b) Elaborar el Plan general Auditor de Protección de Datos personales y Seguridad de la Información de la Diputación y llevar a cabo las actuaciones auditoras en él comprendidas que le correspondan.

c) Ejecutar la Auditoría de la seguridad de los sistemas de información a la que se refiere el Esquema Nacional de Seguridad.

d) Supervisar el cumplimiento de la normativa legal e interna en materia de seguridad de la información.

e) Llevar a cabo investigaciones sobre hechos e incidentes de seguridad de la información.

f) Elaborar estudios, propuestas de regulación, documentos para facilitar el cumplimiento normativo y evacuar consultas e informes en la materia.

g) La difusión de todo tipo de información y la organización de actividades que fomenten el conocimiento, el cumplimiento normativo y las buenas prácticas en materia de protección de datos personales y de seguridad de la información, tanto en el entorno corporativo como en la sociedad en general.

En el ejercicio de las competencias recogidas en los apartados b, c, d, e, el departamento de Protección de Datos y Seguridad de la Información actuará con la debida independencia para asegurar la objetividad en sus actuaciones. Cuando actúe asistiendo al Delegado de Protección de Datos, se garantizará las notas de independencia, no conflicto de intereses y confidencialidad que resultan consustanciales a la figura del Delegado.

Todos los empleados de la Corporación están obligados a facilitar cuanta información le sea requerida por el departamento de Protección de Datos y Seguridad de la Información, así como el acceso a locales, instalaciones, equipos, archivos, soportes de almacenamiento, programas, procesos y procedimientos.

Capítulo Tercero

El Delegado de Protección de Datos

Artículo 36. Designación y remoción

En cumplimiento del artículo 37.5 del RGPD el Delegado de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 del RGPD.

En el ámbito de la Diputación de Valencia, el Delegado de Protección de Datos es designado por resolución del/a Presidente/a de la Corporación, recayendo el nombramiento en el/la funcionario/a que reúna los requisitos anteriormente citados.

La designación ha de ser comunicada en el plazo de diez días a la Agencia Española de Protección de Datos.

Una vez designado, el Delegado de Protección de Datos no podrá ser removido ni sancionado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio.

Artículo 37. Funciones del delegado

Serán funciones del Delegado de Protección de Datos, como mínimo:

a) informar y asesorar a los Servicios internos y miembros de la Corporación de la normativa legal e interna sobre protección de datos

b) supervisar el cumplimiento de la normativa legal e interna sobre protección de datos

c) supervisar la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes

d) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD

e) cooperar con la Agencia Española de Protección de Datos y, en su caso, la autoridad de control autonómica

f) actuar como punto de contacto de la Agencia Española de Protección de Datos y, en su caso, la autoridad de control autonómica, para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas sobre cualquier otro asunto

g) ser el contacto de los interesados para las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos

h) intervenir en caso de reclamaciones ante las autoridades de protección de datos en los términos del artículo 37 de la LOPDGDD

Y todas aquellas que le puedan ser encomendadas por las normas de desarrollo de la presente Política, respetando la legislación de protección de datos y, en todo caso, la normativa de función pública. De igual modo, las normas de desarrollo de la presente Política podrán concretar y especificar con mayor detalle las funciones mínimas anteriores, así como los correspondientes procedimientos de trabajo asociados.

Artículo 38. Actuaciones y posición del delegado en la organización

El Delegado de Protección de Datos actuará como interlocutor de la Diputación ante la Agencia Española de Protección de Datos y, en su caso, las autoridades autonómicas de protección de datos.

En el ejercicio de sus funciones el Delegado de Protección de Datos tendrá acceso a todos los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso la existencia de cualquier deber de confidencialidad o secreto.

Todos los empleados de la Corporación están obligados a facilitar cuanta información le sea requerida por el Delegado de Protección de Datos, así como el acceso a locales, instalaciones, equipos,

archivos, soportes de almacenamiento, programas, procesos y procedimientos.

Se considerará una obstrucción a la labor del Delegado no atender a las obligaciones expuestas en los dos párrafos anteriores, incurrir en dilaciones injustificadas, establecer limitaciones y, en general, entorpecer las actuaciones del Delegado.

Cuando el Delegado de Protección de Datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a la Presidencia de la Corporación. Procederá de igual forma cuando en el ejercicio de sus competencias el Delegado apreciase o tuviese conocimiento de hechos que puedan ser constitutivos de una infracción penal, ello sin perjuicio del deber de denunciar recogido en el artículo 262 de la Ley de Enjuiciamiento Criminal.

El Delegado de Protección de Datos podrá solicitar al Responsable de los Sistemas de Información TIC la suspensión temporal del tratamiento de informaciones, prestación de servicios o la total operación en aquellos supuestos en los que aprecie situaciones que:

- puedan ser graves para la seguridad de los datos de carácter personal, o

- puedan causar un daño irreparable a los titulares de los datos personales, o

- supongan una violación de la normativa de protección de datos que esté considerada una infracción muy grave según el artículo 72 LOPDGDD

Se garantizará la independencia del Delegado de Protección de Datos dentro de la organización:

a) evitando cualquier conflicto de intereses

b) prohibiendo que se le den instrucciones en lo que respecta al desempeño de sus funciones

c) estableciendo las condiciones necesarias para que no se interfiera en sus actuaciones o menoscabe su competencia

d) removiendo cualquier actuación que pueda implicar un perjuicio para los derechos o condiciones laborales del Delegado, o que le discriminen frente al resto de funcionarios de la organización o, en general, pueda suponer una presión o influencia en su toma de decisiones.

En cumplimiento del artículo 38.2 del RGPD, la Presidencia de la Corporación respaldará al Delegado de Protección de Datos en el desempeño de sus funciones, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, así como para el mantenimiento de sus conocimientos especializados.

El Delegado de Protección de Datos rendirá cuentas directamente ante la Presidencia de la Corporación. En todo caso, el Delegado presentará una memoria anual donde informará de las actuaciones llevadas a cabo en dicho periodo.

Se garantizará que el Delegado de Protección de Datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales. Se establecerán instrucciones y procedimientos internos para asegurar dicha participación.

Se habilitarán canales, preferiblemente telemáticos, para que los titulares de los datos, los empleados públicos, los encargados de tratamientos y los miembros de la Corporación puedan ponerse en contacto con el Delegado de Protección de Datos por lo que respecta a todas las cuestiones relativas al tratamiento de datos personales.

El Delegado de Protección de Datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.

Título tercero

Disposiciones relativas al personal

Capítulo Primero

Obligaciones y responsabilidades

Artículo 39. Obligaciones del personal

Todo el personal de la Diputación de Valencia tiene la obligación de conocer y cumplir esta Política de seguridad y de protección de datos de carácter personal y la normativa que la desarrolle, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

La normativa interna que desarrolle la presente Política contendrá las especificaciones necesarias para que todo el personal conozca perfectamente las obligaciones que, en atención a las funciones que desempeña, le son exigibles en el marco de la presente disposición.

Artículo 40. Terceras partes

Cuando la Diputación de Valencia preste servicios a otros organismos o maneje información de otros organismos, se les hará participes de esta Política, estableciéndose canales para reporte y coordinación de los respectivos Comités de Seguridad TIC, en su caso, y procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Diputación de Valencia utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política y de la normativa de seguridad y de protección de datos personales que ataña a dichos servicios o información. Dichos terceros quedarán sujetos a las obligaciones establecidas en la citada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad y protección de datos personales, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se recabará un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

Todos los instrumentos mediante los que se regulen las relaciones entre la Diputación de Valencia y terceros –convenios, contratos, pliegos técnicos, etc- contendrán cumplida referencia de esta Política y de las obligaciones y responsabilidades de las partes en materia de seguridad de la información y protección de datos de carácter personal.

Artículo 41. Incumplimientos

A los incumplimientos de la presente Política, así como de la normativa que la desarrolle, cometidos por el personal al servicio de la Diputación de Valencia les será de aplicación el régimen disciplinario legalmente establecido por la normativa vigente.

Cuando los incumplimientos fuesen cometidos por terceros, sobre los que recaiga la obligación de cumplimiento en virtud de contrato o cualquier otro tipo de relación acordada, la responsabilidad les será exigida en los términos previstos en los instrumentos que regulen dichas relaciones y por la normativa legal que pueda resultar de aplicación.

Capítulo Segundo

Recursos formativos

Artículo 42. Formación y concienciación

La Diputación de Valencia garantizará la formación y concienciación a todos sus empleados públicos a través del Servicio de Formación incluyendo las acciones formativas necesarias en los planes de formación interna. Las personas con responsabilidad en el uso, operación o administración de los sistemas de información recibirán la formación adecuada para el manejo seguro de los sistemas y para un adecuado tratamiento de los datos de carácter personal, en la medida en que la necesite para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto o de responsabilidad del mismo.

La asistencia y cumplimentación de estas acciones formativas tiene carácter obligatorio, salvo circunstancias excepcionales debidamente acreditadas. El personal que no pueda concurrir a las mismas por estos supuestos será incluido con carácter preferente en siguientes convocatorias.

Al personal con responsabilidades muy específicas en materia de seguridad o de protección de datos de carácter personal, se les facilitará de modo preferente la asistencia a actividades formativas que tengan relación directa con dichas responsabilidades.

El Departamento de Protección de Datos y Seguridad de la Información diseñará y pondrá en práctica actividades dirigidas a la concienciación en ciberseguridad y protección de datos, así como al fomento del cumplimiento de la normativa legal, interna y de buenas prácticas en ambas materias.

El Delegado de Protección de Datos, en el ejercicio de su competencia de supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento, participará en la planificación

de los programas formativos internos en la materia, proponiendo las acciones formativas que considere necesarias en atención a la situación que en cada momento presente la organización.

El Servicio de Informática y el Servicio de Formación colaborarán estrechamente con el Delegado y el Departamento de Protección de Datos y Seguridad de la Información para el cumplimiento efectivo de lo dispuesto en el presente artículo.

TÍTULO CUARTO

Desarrollo y modificación de la Política de Seguridad y de Protección de Datos de Carácter Personal

Capítulo Primero

Instrumentos de desarrollo

Artículo 43. DESARROLLO NORMATIVO

El desarrollo de la presente Política se llevará a cabo mediante instrumentos pertenecientes a tres niveles, denominados A, B y C. Cuando se apruebe un instrumento de desarrollo deberá especificarse el nivel al que pertenece.

Artículo 43.1. NIVEL A

Pertenecen al nivel A las denominadas Normas de Seguridad y de Protección de Datos de Carácter Personal.

Están conformadas por el conjunto de reglas y directrices de carácter obligatorio que desarrollan directamente el contenido de la presente Política o trasladan al orden interno, mediante las correspondientes normas, el cumplimiento de la normativa legal aplicable en la materia.

Se integran en este nivel:

- Las Normativas de Seguridad (apartado 3.2 org.2 del ENS).
- Las Políticas de Protección de Datos (artículo 24.2 del RGPD).

De igual modo, se integrará en este nivel cualquier otra normativa interna que el órgano o autoridad competente, según lo establecido en el artículo 44.1 de la presente disposición, considere necesaria para cumplir los objetivos expuestos en el presente artículo.

Artículo 43.2. NIVEL B

Pertenecen al nivel B los denominados Procedimientos de Seguridad y de Protección de Datos de Carácter Personal.

Están constituidos por el conjunto de procedimientos técnicos de carácter obligatorio orientados a resolver las tareas, procesos de trabajo o modos de actuación considerados más relevantes atendiendo al perjuicio que causaría una actuación inadecuada de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información, o de protección de datos de carácter personal, o por venir impuestos por la legislación aplicable.

Se integran en este nivel:

- Los Procedimientos de Seguridad (apartado 3.3 org.3 del ENS)
- El Procedimiento para el control del acceso físico a instalaciones (artículo 17 del ENS).
- El Procedimiento para asegurar la recuperación y conservación a largo plazo de los documentos electrónicos (artículo 21.2 del ENS).
- El Procedimiento del Registro de Actividades de Tratamiento.
- El Procedimiento de realización de copias de respaldo y de recuperación de los datos (ex art. 32 del RGPD).
- Los Procedimientos para el archivo de soportes y documentos.
- El Procedimiento para atender el ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad (artículos 15 a 22 del RGPD).
- El Procedimiento de notificación, gestión y respuesta ante las incidencias y en su caso brechas o violaciones de seguridad (art. 33-34 del RGPD y 4.3.7 op.exp.7 del ENS).
- El Procedimiento de asignación, distribución y almacenamiento de contraseñas (ex art. 32 del RGPD).
- Los Procedimientos para el control de las medidas de seguridad y de auditoría (ex art. 32 del RGPD y anexo III del ENS).

De igual modo, se integrará en este nivel cualquier otro procedimiento que el órgano o autoridad competente, según lo establecido en el artículo 44.1 de la presente disposición, considere necesario para cumplir los objetivos expuestos en el presente artículo.

Artículo 43.3. Nivel C

Pertenecen al nivel C las denominadas Guías de Seguridad y de Protección de Datos de Carácter Personal.

Están conformadas por el conjunto de recomendaciones y especificaciones técnicas y jurídicas, de carácter esclarecedor u orientativo, tendentes a ilustrar con mayor detalle aspectos concretos de la seguridad y la protección de datos personales. Su objetivo último es ayudar a la correcta aplicación de las normas y procedimientos recogidos en los niveles A y B, o complementar su contenido, así como contribuir a una mejor información y difusión de las mismas.

Se integran en este nivel:

- Las Guías técnicas de seguridad.
- Los Manuales, informes, monografías, cuadernos, estudios técnicos y recomendaciones y cualquier tipo de publicaciones.

Capítulo Segundo

Competencias de desarrollo

Artículo 44. Asignación de competencias de desarrollo

Las competencias para la elaboración y aprobación de los instrumentos de desarrollo de la presente Política se asignan en función de los diferentes niveles en que se encuadran, de conformidad con el artículo 43 de la presente disposición.

Artículo 44.1. Instrumentos de nivel A y B

La competencia para la aprobación de las Normas de Seguridad y de Protección de Datos de Carácter Personal, así como de los Procedimientos de Seguridad y de Protección de Datos de Carácter Personal corresponde al Presidente/a de la Diputación de Valencia o Diputado/a en quien delegue.

El Comité de Seguridad TIC, el Departamento de protección de Datos y Seguridad de la Información y el Delegado de Protección de Datos, cada cual en el marco de sus competencias, formularán las propuestas que consideren adecuadas.

Artículo 44.2. Instrumentos de nivel C

Corresponde al Comité de Seguridad TIC, al Departamento de protección de Datos y Seguridad de la Información y al Delegado de Protección de Datos, cada cual en el marco de sus competencias, la elaboración de las Guías de Seguridad y de Protección de Datos de Carácter Personal.

Capítulo Tercero

Modificación de la Política

Artículo 45. Actualización permanente

La presente Política deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a las previsiones legales que pudiesen afectarle.

Artículo 46. Procedimiento para la modificación

Las propuestas de las sucesivas revisiones de la presente Política se elaborarán por el Comité de Seguridad TIC y por el Departamento de Protección de Datos y Seguridad de la Información, y se trasladarán, a través del Presidente/a al Pleno de la Corporación, único órgano competente para acordar cualquier modificación de dicha Política.

Disposicion derogatoria

Única. Derogación normativa

1. Queda derogado el Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia, aprobado por el Pleno de la Corporación en sesión de 18 de junio de 2013, Bop nº 159 de 6 de julio.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en la presente disposición.

Disposicion transitoria

Única. Normativa interna vigente

La normativa interna aprobada en desarrollo del Reglamento que se cita en la Disposición Derogatoria seguirá siendo de aplicación mientras se aprueban las normativas de desarrollo de la presente disposición que las sustituyan, en la medida en que no incurran en los supuestos a los que se refiere el apartado 2 de la Disposición Derogatoria.

Disposiciones finales

Primera. Constitución del comité de seguridad TIC

El nuevo Comité de Seguridad TIC deberá quedar constituido en un plazo no superior a tres meses desde la entrada en vigor de la presente disposición.

Las actas, acuerdos y cualquier otra documentación referida al período de actuación del Comité de Seguridad TIC constituido al amparo del Reglamento anterior, deberán ser transferidos al nuevo Comité en el momento se constituya.

Segunda. Desarrollo normativo

El desarrollo de la presente Política, a través de los instrumentos establecidos en el artículo 43.1, deberá llevarse a cabo en un plazo máximo de seis meses desde la entrada en vigor de la misma.

Cuando se trate de los instrumentos contemplados en el artículo 43.2, se deberá tener aprobados dentro del plazo citado anteriormente aquellos procedimientos considerados como críticos para la seguridad de los sistemas de información afectados.

Tercera. Politicas de ámbito municipal

La Diputación de Valencia podrá elaborar, al amparo del párrafo segundo del artículo 11.2 ENS, Políticas de Seguridad y de Protección de Datos Personales comunes para los municipios de la provincia que deseen adherirse a ellas.

En la configuración de dichas Políticas se tendrán en consideración aquellos elementos que resulten homogéneos a la hora de determinar el conjunto de sus destinatarios, tales como la población, el nivel de infraestructuras y servicios TIC, los recursos organizativos, el grado de dependencia de la asistencia de la Diputación o la posible transferencia de competencias del ámbito municipal al provincial.

Cuarta. Entrada en vigor

La presente disposición entrará en vigor a los 15 días hábiles desde la fecha de su publicación en el BOP.

2022/7768