POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

1. INTRODUCCIÓ.

1.1. Missió i serveis prestats.

La Diputació d'Alacant, el naixement de la qual data del 15 de maig de 1822, és un ens local bolcat en l'assistència als municipis per a facilitar la gestió de les seues competències. Serveix a les corporacions locals, i a través d'elles a tots els habitants de la província d'Alacant.

Entre unes altres, són competències pròpies de la Diputació les següents:

1. 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 de competència municipal.

2. L'assistència i la cooperació jurídica, econòmica i tècnica als Municipis, especialment als de menor capacitat econòmica i de gestió.

3. La prestació de serveis públics de caràcter supramunicipal i, si escau, supracomarcal.

4. 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.

5. En general, el foment i l'administració dels interessos peculiars de la província.

2. JUSTIFICACIÓ POLÍTICA DE SEGURETAT DE LA INFORMACIÓ.

2.1. Necessitat de seguretat en els sistemes.

Per al compliment de la seua Missió, la prestació dels Serveis identificats i el compliment dels seus objectius, la Diputació d'Alacant depèn dels anomenats sistemes TIC (Tecnologies de la Informació i Comunicacions).

Aquests sistemes han de ser administrats amb diligència, adoptant les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguen afectar a 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 de la informació 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 de ràpida evolució 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. Açò implica s'han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (d'ara endavant ENS), així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats

Per açò el ENS (Reial decret 3/2010, de 8 de gener), en el seu article 11 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".

2.2. Requisits de seguretat en els Departaments.

Totes les Àrees de la Diputació han d'aplicar les mesures mínimes de seguretat exigides pel ENS, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

Els diferents departaments han de cerciorar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seua concepció fins a la seua retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

Els departaments han d'estar preparats per a prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 del ENS.

3. MARC NORMATIU.

3.1. Responsabilitats derivades de normatives.

La Llei 11/2007, de 22 de juny, d'accés dels ciutadans als serveis públics, en el seu article 42.2, estableix sobre el ENS, com un dels seus principis, que s'ha de disposar d'un marc de referència que establisca les condicions necessàries de confiança en l'ús dels mitjans electrònics.

La Llei 3/2010, de 5 de maig, de la Generalitat, d'Administració Electrònica de la Comunitat Valenciana, estableix en el seu article 37 que la utilització de tècniques electròniques, informàtiques i telemàtiques per part de les administracions públiques de la Comunitat Valenciana haurà d'incorporar les mesures de seguretat, qualitat i de control necessàries que garantisquen l'autenticitat, confidencialitat, integritat, disponibilitat i conservació de la informació.

El Reial decret 3/2010, de 8 de gener, de desenvolupament del ENS, fixa els principis bàsics i requisits mínims, així com les mesures de protecció a implantar en els sistemes de l'Administració.

Així mateix, la Llei 15/1999, de 13 de desembre, de Protecció de dades de caràcter personal, té per objecte garantir i protegir, en el que concerneix al tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i intimitat personal i familiar.

El Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, la dota de coherència en tot el relacionat amb la transposició de la directiva 95/46/CE del Parlament Europeu i desenvolupa aquells aspectes nous o en què l'experiència ha aconsellat un cert grau de precisió.

4. ORGANITZACIÓ DE LA SEGURETAT.

4.1. Comitè: funcions i responsabilitats.

El Comitè de Seguretat de la Informació, és l'òrgan que coordina la Seguretat de la Informació a nivell de la Diputació d'Alacant.

Estarà constituït pel Cap del departament d'Informàtica, el Cap de la Unitat de Sistemes, l'Administrador de Seguretat Informàtica i per representants de les àrees afectades pel ENS

Els membres del Comitè de Seguretat de la Informació, seran nomenats per la Presidència d'aquesta Corporació.

Les seues funcions són les següents:

- Responsabilitats derivades del tractament de dades de caràcter personal.

- Atendre les inquietuds de la Corporació i dels diferents departaments.

- Informar regularment de l'estat de la seguretat de la informació a l'Alta Adreça.

- Promoure la millora contínua del Sistema de Gestió de la Seguretat de la Informació.

- Elaborar l'estratègia d'evolució de la Diputació d'Alacant pel que fa a la seguretat de la informació.

- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

- Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè siga aprovada per l'Adreça.

- Aprovar la normativa de seguretat de la informació.

- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.

- Monitoritzar els principals riscos residuals assumits per l'Organització i recomanar possibles actuacions respecte d'ells.

- Monitoritzar l'acompliment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'ells. En particular, vetlar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.

- Promoure la realització de les auditories periòdiques que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.

- Aprovar plans de millora de la seguretat de la informació de l'Organització. En particular, vetlarà per la coordinació de diferents plans que puguen realitzar-se en diferents àrees.

- Vetlar perquè la seguretat de la informació es té en compte en tots els projectes TIC des de la seua especificació inicial fins a la seua posada en operació. En particular, haurà de vetlar per la creació i utilització de serveis horitzontals que reduïsquen duplicitats i recolzen un funcionament homogeni de tots els sistemes TIC.

- Resoldre els conflictes de responsabilitat que puguen aparèixer entre els diferents responsables i/o entre diferents àrees de l'Organització, elevant aquells casos en els quals no tinga suficient autoritat per a decidir.

En cas d'ocurrència d'incidents de seguretat de la informació aprovarà el Pla de Millora de la Seguretat.

El Comitè de Seguretat de la Informació no és un comitè tècnic, però recaptarà regularment del personal tècnic propi o extern, la informació pertinent per a prendre decisions. El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els quals haja de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, podent materialitzar-se de diferents formes i maneres:

- Grups de treball especialitzats interns, externs o mixts.

- Assessoria externa.

- Assistència a cursos o un altre tipus d'entorns formatius o d'intercanvi d'experiències.

El Responsable de la Seguretat de la Informació és el secretari del Comitè de Seguretat de la Informació i com a tal:

- Convoca les reunions del Comitè de Seguretat de la Informació.

- Prepara els temes a tractar en les reunions del Comitè, aportant informació puntual per a la presa de decisions.

- Elabora l'acta de les reunions.

- És responsable de l'execució directa o delegada de les decisions del Comitè.

4.2. Rols: funcions i responsabilitats.

La Política de Seguretat, segons requereix l'Annex II del ENS en la seua secció 3.1, ha d'identificar uns clars responsables per a vetlar pel seu compliment i ser coneguda per tots els membres de l'organització administrativa.

S'estableixen els següents rols en l'organització relacionats amb la Seguretat de la Informació.

4.2.1. Responsable de la Informació.

Aquestes funcions seran assumides per, la Presidència o diputat en qui delegue, que entén la missió de la Diputació d'Alacant., determina els objectius que es proposa aconseguir i respon que s'aconseguisquen.

- *Funcions associades.*

Les seues funcions seran les següents:

- Té la responsabilitat última de l'ús que es faça d'una certa informació i, per tant, de la seua protecció.

- És el responsable últim de qualsevol error o negligència que porte a un incident de confidencialitat o d'integritat.

- Estableix els requisits de la informació en matèria de seguretat. En el marc del ENS, equival a la potestat de determinar els nivells de seguretat de la informació.

- Determinarà els nivells de seguretat en cada dimensió dins del marc establert en l'Annex I del ENS.

- Encara que l'aprovació formal dels nivells corresponga al Responsable de la Informació, podrà recaptar una proposta al Responsable de la Seguretat i convé que escolte l'opinió del Responsable del Sistema.

- *Compatibilitat amb altres responsables.*

Aquest rol podrà coincidir:

- amb el de Responsable de Servei,

- i amb el de Responsable de Fitxer requerit per la Llei 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

Aquest rol no podrà coincidir:

- amb el de Responsable de Seguretat,

- ni amb el de Responsable de Sistema,

- ni amb el d'Administrador de la Seguretat del Sistema.

4.2.2. Responsable del Servei.

Aquestes funcions seran assumides per, la Presidència o diputat en qui delegue, que entén què fa cada departament, i com els departaments es coordinen entre si per a aconseguir els objectius marcats per l'Adreça.

- *Funcions associades.*

Les seues funcions seran les següents:

- Té la potestat de determinar els nivells de seguretat dels serveis dins del marc establert en l'Annex I del ENS.

- Té la responsabilitat última de l'ús que es faça de determinats serveis i, per tant, de la seua protecció.

- És el responsable últim de qualsevol error o negligència que porte a un incident de disponibilitat dels serveis que gestiona.

- Encara que l'aprovació formal dels nivells corresponga al Responsable del Servei, podrà recaptar una proposta al Responsable de la Seguretat i convé que escolte l'opinió del Responsable del Sistema.

- La prestació d'un servei sempre ha d'atendre als requisits de seguretat de la informació que maneja, de manera que aquests podran heretar-se, afegint requisits de disponibilitat, així com uns altres com a accessibilitat, interoperabilitat, etc.

- *Compatibilitat amb altres responsables.*

Aquest rol podrà coincidir:

- amb el del Responsable de la Informació,

- i amb el de Responsable de Fitxer requerit per la Llei 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

Aquest rol no podrà coincidir:

- amb el de Responsable de Seguretat,

- amb el de Responsable de Sistema,

- ni amb el d'Administrador de la Seguretat del Sistema.

4.2.3. Responsable de Seguretat de la Informació.

El rol de Responsable de Seguretat de la Informació, serà exercit pel Cap del Departament d'Informàtica.

Es nomenarà formalment com a tal a una única persona en l'organització.

Es podrà delegar part de les seues funcions en altres persones.

- *Funcions associades.*

Les seues funcions seran les següents:

- Informarà directament al Comitè de Seguretat de la Informació.

- Actuarà com a Secretari del Comitè de Seguretat de la Informació.

- Convocarà al Comitè de Seguretat de la Informació, recopilant la informació pertinent.

- Pertanyerà al Comitè de Seguretat de la informació, per a coordinar les necessitats de Seguretat de la Informació en el marc de la resta de necessitats de Seguretat Corporativa.

- Mantindrà la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord a l'establert en la Política de Seguretat de l'Organització.

- Promourà la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.

- Recopilarà els requisits de seguretat dels Responsables d'Informació i Servei i determinarà la categoria del Sistema.

- Realitzarà l'Anàlisi de Riscos.

- Elaborarà una Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides conforme a l'Annex II del ENS i del resultat de l'Anàlisi de Riscos.

- Facilitarà als Responsable d'Informació i als Responsables de Servei informació sobre el nivell de risc residual esperat després d'implementar les opcions de tractament seleccionades en l'anàlisi de riscos i les mesures de seguretat requerides pel ENS.

- Coordinarà l'elaboració de la Documentació de Seguretat del Sistema.

- Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per a la seua aprovació per Adreça.

- Participarà en l'elaboració i aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de Seguretat de la Informació.

- Elaborarà i aprovarà els Procediments Operatius de Seguretat de la Informació.

- Facilitarà periòdicament al Comitè de Seguretat un resum d'actuacions en matèria de seguretat, d'incidents relatius a seguretat de la informació i de l'estat de la seguretat del sistema (en particular del nivell de risc residual al que està exposat el sistema).

- Elaborarà, al costat dels Responsables de Sistemes, Planes de Millora de la Seguretat, per a la seua aprovació pel Comitè de Seguretat de la Informació.

- Elaborarà els Planes de Formació i Conscienciació del personal en Seguretat de la Informació, que hauran de ser aprovats pel Comitè de Seguretat de la Informació.

- Validarà els Planes de Continuïtat de Sistemes que elabore el Responsable de Sistemes, que hauran de ser aprovats pel Comitè de Seguretat de la Informació i provats periòdicament pel Responsable de Sistemes.

- Aprovarà les directrius proposades pels Responsables de Sistemes per a considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis.

- En cas d'ocurrència d'incidents de seguretat de la informació analitzarà i proposarà salvaguardes que previnguen incidents similars en un futur.

- *Compatibilitat amb altres rols.*

Aquest rol no podrà coincidir:

- amb el de Responsable de la Informació,

- amb el de Responsable del Servei,

- amb el de Responsable del Sistema,

- i amb el d'Administrador de Seguretat del Sistema.

- *Delegació de funcions.*

Per a determinats Sistemes d'Informació en els quals per la seua complexitat, distribució, separació física dels seus elements o nombre d'usuaris es necessite de personal addicional per a dur a terme les funcions del Responsable de la Seguretat, es podran designar els Responsables de Seguretat Delegats que es consideren necessaris.

La designació correspon al Responsable de la Seguretat. Per mitjà de la designació de Delegats, es deleguen funcions. La responsabilitat final seguirà recaient sobre el Responsable de la Seguretat.

Els Responsables de Seguretat Delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegue el Responsable de la Seguretat, podent ser, per exemple, la seguretat de sistemes d'informació concrets o de sistemes d'informació horitzontals.

Cada Responsable de Seguretat Delegat tindrà una dependència funcional directa del Responsable de la Seguretat, que és a qui reporten.

4.2.4. Responsable del Sistema.

El rol de Responsable del Sistema serà exercit pel Cap de la Unitat de Sistemes.

Es nomenarà formalment com a tal a una única persona en l'organització.

Es podrà delegar part de les seues funcions en altres persones

- *Funciones associades.*

Les seues funcions seran les següents:

- Desenvolupar, operar i mantenir el Sistema d'Informació durant tot el seu cicle de vida, les seues especificacions, instal·lació i verificació del seu correcte funcionament.

- Definir la topologia i sistema de gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en el mateix.

- Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.

- El Responsable del Sistema pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que pogueren afectar a la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els Responsables de la Informació afectada, del Servei afectat i amb el Responsable de la Seguretat abans de ser executada.

- Aplicar els procediments operatius de seguretat elaborats i aprovats pel Responsable de Seguretat.

- Monitoritzar l'estat de la seguretat del Sistema d'Informació i reportar-ho periòdicament o davant incidents de seguretat rellevants al Responsable de Seguretat de la Informació.

- Elaborar els Planes de Continuïtat del Sistema perquè siguen validats pel Responsable de Seguretat de la Informació, i coordinats i aprovats pel Comitè de Seguretat de la Informació.

- Realitzar exercicis i proves periòdiques dels Planes de Continuïtat del Sistema per a mantenir-los actualitzats i verificar que són efectius.

- Elaborarà les directrius per a considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos (especificació, arquitectura, desenvolupament, operació i canvis) i les facilitarà al Responsable de Seguretat de la Informació per a la seua aprovació.

En cas d'ocurrència d'incidents de seguretat de la informació:

- Planificarà la implantació de les salvaguardes en el sistema.

- Executarà el pla de seguretat aprovat.

- *Compatibilitat amb altres responsables.*

Aquest rol no podrà coincidir:

- amb el de Responsable d'Informació,

- amb el de Responsable de Servei,

- amb el de Responsable de Seguretat de la Informació,

- ni amb d'Administrador de Seguretat del Sistema.

4.2.5. Administrador de la seguretat del Sistema.

Correspon al nivell d'un funcionari qualificat en seguretat informàtica de sistemes.

Podrà nomenar-se formalment com tal diverses persones per a cada Sistema.

Serà proposat pel Responsable del Sistema, a qui reportarà en tot el relacionat amb seguretat de la informació.

- *Funcions associades.*

Les seues funcions seran les següents:

- La implementació, gestió i manteniment de les mesures de seguretat aplicables al Sistema d'Informació.

- Assegurar que els controls de seguretat establerts són complits estrictament.

- Assegurar que la traçabilitat , pistes d'auditoria i altres registres de seguretat requerits es troben habilitats i registren amb la freqüència desitjada, d'acord amb la Política de Seguretat establida per l'Organització.

- Aplicar als Sistemes, usuaris i altres actius i recursos relacionats amb el mateix, tant interns com a externs, els Procediments Operatius de Seguretat i els mecanismes i serveis de seguretat requerits.

- Assegurar que són aplicats els procediments aprovats per a manejar el Sistema d'informació i els mecanismes i serveis de seguretat requerits.

- La gestió, configuració i actualització, si escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat del Sistema d'Informació.

- Supervisar les instal·lacions de maquinari i programari, les seues modificacions i millores per a assegurar que la seguretat no està compromesa.

- Aprovar els canvis en la configuració vigent del Sistema d'Informació, garantint que seguisquen operatius els mecanismes i serveis de seguretat habilitats.

- Informar als Responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.

- Monitoritzar l'estat de la seguretat del sistema.

En cas d'ocurrència d'incidents de seguretat de la informació:

- Dur a terme el registre, comptabilitat i gestió dels incidents de seguretat en els Sistemes sota la seua responsabilitat.

- Executar el pla de seguretat aprovat.

- Aïllar l'incident per a evitar la propagació a elements aliens a la situació de risc.

- Prendre decisions a curt termini si la informació s'ha vist compromesa de tal forma que poguera tenir conseqüències greus (aquestes actuacions haurien d'estar procedimentades per a reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).

- Assegurar la integritat dels elements crítics del Sistema si s'ha vist afectada la disponibilitat dels mateixos (aquestes actuacions haurien d'estar procedimentades per a reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).

- Mantenir i recuperar la informació emmagatzemada pel Sistema i els seus serveis associats.

- Investigar l'incident: Determinar la manera, els mitjans, els motius i l'origen de l'incident.

- *Compatibilitat amb altres responsables.*

Aquest rol no podrà coincidir:

- amb el de Responsable d'Informació,

- amb el de Responsable de Servei,

- ni amb el de Responsable de Seguretat Corporativa o de la Informació.

Aquest rol podrà coincidir amb el de Responsable del Sistema.

- *Delegació de funcions.*

En determinats sistemes d'informació que per la seua complexitat, distribució, separació física dels seus elements o nombre d'usuaris es necessite de personal addicional per a dur a terme les seues funcions, es podran designar Administradors de Seguretat del Sistema Delegats.

Els Administradors de Seguretat del Sistema Delegats seran responsables, en el seu àmbit, d'aquelles accions que delegue l'Administrador de Seguretat del Sistema relacionades amb la implantació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació.

L'Administrador de Seguretat del Sistema Delegat serà designat a sol·licitud de l'Administrador de Seguretat del Sistema, del que dependrà funcionalment.

La seua identitat apareixerà reflectida en la documentació de seguretat del sistema d'informació.

4.2.6. Gestió de personal.

Els responsables de gestió del personal s'ajustaran a l'establert pel ENS en matèria de personal de forma anàloga a l'establert en els punts anteriors.

Els responsables de personal implantaran les mesures de seguretat que els competisquen dins de les determinades pel Responsable de Seguretat de la Informació, i informaran a aquest del seu grau d'implantació, eficàcia i incidents.

4.3. Jerarquia en el procés de decisions i mecanismes de coordinació.

Els diferents rols de seguretat de la informació (autoritat principal i possibles delegades) es limiten a una jerarquia simple: el Comitè de Seguretat de la Informació dóna instruccions al Responsable de la Seguretat de la Informació que s'encarrega d'emplenar, supervisant que administradors i operadors implementen les mesures de seguretat segons l'establert en la Política de Seguretat aprovada per a l'Organització.

L'Administrador de Seguretat reporta al Responsable del Sistema:

- Incidents relatius a la seguretat del sistema.

- Accions de configuració, actualització o correcció.

El Responsable del Sistema informa al Responsable de la Informació de les incidències funcionals relatives a la informació que li competeix.

El Responsable del Sistema informa al Responsable del Servei de les incidències funcionals relatives al servei que li competeix.

El Responsable del Sistema reporta al Responsable de la Seguretat:

- Actuacions en matèria de seguretat, en particular quant a decisions d'arquitectura del sistema.

- Resum consolidat dels incidents de seguretat.

- Mesures de l'eficàcia de les mesures de protecció que s'han d'implantar.

El Responsable de la Seguretat informa al Responsable de la Informació de les decisions i incidents en matèria de seguretat que afecten a la informació que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

El Responsable de la Seguretat informa al Responsable del Servei de les decisions i incidents en matèria de seguretat que afecten al servei que li competeix, en particular de

l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

Quan existisca un Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta a aquest Comitè com a secretari:

- Resum consolidat d'actuacions en matèria de seguretat

- Resumeixen consolidat d'incidents relatius a la seguretat de la informació

- Estat de la seguretat del sistema, en particular del risc residual al que el sistema està exposat

Quan no existisca un Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta directament a l'Adreça de l'Organització:

- Resum consolidat d'actuacions en matèria de seguretat.

- Resum consolidat d'incidents relatius a la seguretat de la informació.

- Estat de la seguretat del sistema, en particular del risc residual al que el sistema està exposat.

4.4. Procediments de designació de persones.

La Presidència de la Diputació d'Alacant designarà formalment mitjançant la seua publicació en el Butlletí Oficial corresponent:

- Al Responsable de la Informació, en cas de no assumir directament aquest rol.

- Al Responsable del Servei, en cas de no assumir directament aquest rol.

- Al Responsable de la Seguretat, que ha de reportar directament a l'Adreça o, quan existisquen, als Comitès de Seguretat de la Informació i Seguretat Corporativa.

- Al Responsable del Sistema, que ha de reportar directament a l'Adreça o, quan existisquen, als Comitès de Seguretat de la Informació i Seguretat Corporativa.

La Presidència de la Diputació d'Alacant designarà a la persona Responsable del Sistema:

- A proposta del Responsable de la Informació tractada, quan el Sistema d'informació tracte una única informació.

- A proposta del Responsable del Servei prestat, quan el Sistema d'informació preste un únic servei.

- Directament, quan el Sistema d'informació tracta diferents informacions o presta diferents serveis, sentits els responsables de les informacions i els serveis afectats.

La Presidència de la Diputació d'Alacant designarà a l'Administrador de Seguretat del Sistema a proposta del Responsable del Sistema.

4.5. Relació amb el document de seguretat i protecció de dades personals.

Per a la prestació dels serveis previstos han de ser tractats dades de caràcter personal. El Document de Seguretat de la Diputació d'Alacant detalla els fitxers afectats i els responsables corresponents, així com les mesures adoptades en el marc del Reial decret 1720/2007 i normativa complementària. Tots els sistemes d'informació s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollits en l'esmentat Document de Seguretat.

5. GESTIÓ DE RISCOS.

5.1. Justificació.

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats.

L'anàlisi de riscos serà la base per a determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establerts pel ENS, segons el previst en l'article 6 del mateix.

5.2. Criteris d'avaluació de riscos.

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

Els criteris d'avaluació de riscos detallats s'especificaran en la metodologia d'avaluació de riscos que elaborarà l'organització, basant-se en estàndards i bones pràctiques reconegudes. En concret, la Diputació efectuarà una anàlisi i avaluació de riscos basant-se en la metodologia MAGERIT V.2 elaborat pel Ministeri de Política Territorial i Administració Pública.

Hauran de tractar-se, com a mínim, tots els riscos que puguen impedir la prestació dels serveis o el compliment de la missió de l'organització de forma greu.

Es prioritzaran especialment els riscos que impliquen un cessament en la prestació de serveis als ciutadans.

5.3. Directrius de tractament.

El Comitè de Seguretat TIC dinamitzarà la disponibilitat de recursos per a atendre a les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

5.4. Procés d'acceptació del risc residual.

Els riscos residuals seran determinats pel Responsable de Seguretat de la Informació.

Els nivells de Risc residuals esperats sobre cada Informació o Servei després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II del ENS) hauran de ser acceptats prèviament pels responsables corresponents.

Els nivells de risc residuals seran presentats pel Responsable de Seguretat de la Informació al Comitè de Seguretat de la Informació, perquè aquest procedisca, si escau, a avaluar, aprovar o rectificar les opcions de tractament proposades.

5.5. Necessitat de realitzar o actualitzar les avaluacions de riscos.

L'anàlisi dels riscos i el seu tractament han de ser una activitat repetida regularment, segons l'establert en l'article 9 del ENS. Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada a l'any.

- Quan es produïsquen canvis significatius en la informació manejada.

- Quan es produïsquen canvis significatius en els serveis prestats.

- Quan es produïsquen canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.

- Quan ocórrega un incident greu de seguretat.

- Quan es reporten vulnerabilitats greus.

6. GESTIÓ D'INCIDENTS DE SEGURETAT.

6.1. Prevenció d'incidents.

Els departaments han d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per a açò els departaments han d'implementar les mesures mínimes de seguretat determinades pel ENS, així com qualsevol control addicional identificat a través d'una 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 Política, els departaments han de:

- Autoritzar els sistemes abans d'entrar en operació.

- Avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració realitzats de forma rutinària.

6.2. Monitoratge i detecció d'incidents.

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una disminució fins al cessament del nivell de prestació, els serveis han de Monitoritzar l'operació de manera contínua per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons l'establert en l'article 9 del ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 del ENS. S'establiran mecanismes de detecció, anàlisi i reporte que puguen informar als responsables tant regularment com quan es produïsca una desviació significativa dels paràmetres que s'hagen preestablert com a normals.

6.3. Resposta davant incidents.

Les diferents Àrees d'aquesta Diputació han de:

- Establir mecanismes per a respondre eficaçment als incidents de seguretat.

- Designar punts de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o en altres organismes.

- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Açò inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).

6.4. Recuperació davant incidents i plans de continuïtat.

Per a garantir la disponibilitat dels serveis crítics, els departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

7. OBLIGACIONS DEL PERSONAL.

Tot el personal de la Diputació d'Alacant, tant empleats públics com a polítics, té l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribe als mateixos.

Tot el personal de la Diputació d'Alacant atendrà a una sessió de conscienciació en matèria de seguretat TIC almenys una vegada cada dos anys. S'establirà un programa de conscienciació contínua per a atendre a tots els membres de l'organització, en particular als de nova incorporació.

El personal amb responsabilitat en l'ús, operació o administració de sistemes TIC rebrà formació per al maneig segur dels sistemes en la mesura en què la necessite per a realitzar 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 de treball o de responsabilitats en el mateix.

El compliment de la present Política de Seguretat és obligatori per part de tot el personal intern o extern que intervinga en els processos l'organització, constituint el seu incompliment infracció greu a efectes laborals.

8. TERCERES PARTS.

Quan la Diputació d'Alacant preste serveis o manipule informació d'altres entitats, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals para reporte i coordinació dels respectius Comitès de Seguretat TIC i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan s'utilitzen serveis externs o se cedisca informació a entitats o empreses, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que concernisca a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establides en la citada normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la.

S'establiran procediments específics de reporte i resolució d'incidències.

Es garantirà que el personal aliè a aquesta Diputació d'Alacant que vaja a manejar la informació està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert 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 requerirà un informe del Responsable de Seguretat que precise els riscos en què s'incorre i la forma de tractar-los.

Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir avant.

9. DOCUMENTACIÓ COMPLEMENTÀRIA.

La Política de Seguretat de la Informació s'emplenarà amb documents més precisos que ajuden a dur a terme el proposat. Per a açò s'utilitzaran:

- Normes de seguretat (security standards).

- Guies de seguretat (security guides).

- Procediments de seguretat (security procedures).

Les normes uniformitzen l'ús d'aspectes concrets del sistema. Indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori.

Les guies tenen un caràcter formatiu i cerquen ajudar als usuaris a aplicar correctament les mesures de seguretat proporcionant raonaments on no existeixen procediments precisos. Per exemple, sol haver-hi una guia sobre com escriure procediments de seguretat. D'igual manera, les guies ajuden a prevenir que es passen per alt aspectes importants de seguretat que poden materialitzar-se de diverses formes.

Els procediments [operatius] de seguretat afronten tasques concretes, indicant el que cal fer, pas a pas. Són útils en tasques repetitives.

10. REVISIÓ I APROVACIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ.

La Política de Seguretat de la Informació serà revisada pel Comitè de Seguretat de la Informació a intervals planificats, que no podran excedir l'any de durada, o sempre que es produïsquen canvis significatius, a fi d'assegurar que es mantinga la seua idoneïtat, adequació i eficàcia.

Els canvis sobre la Política de Seguretat de la Informació hauran de ser aprovats per l'òrgan superior competent que corresponga, d'acord amb l'article 11 del ENS.

Qualsevol canvi sobre la mateixa haurà de ser difós a totes les parts afectades.

11. POLÍTIQUES RELACIONADES.

Aquesta Política de Seguretat de la Informació complementa les Polítiques de Seguretat corporatives, detallant les mesures a adoptar sobre Sistemes d'Informació.

Aquesta Política es desenvoluparà per mitjà de normativa de seguretat que afronte aspectes específics. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conèixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

ANNEX A. GLOSSARI DE TERMES.

Anàlisi de riscos

Utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos.

Dades de caràcter personal

Qualsevol informació concernent a persones físiques identificades o identificables. Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

Gestió d'incidents

Pla d'acció per a atendre a les incidències que es donen. A més de resoldre-les ha d'incorporar mesures d'acompliment que permeten conèixer la qualitat del sistema de protecció i detectar tendències abans que es convertisquen en grans problemes.

Gestió de riscos

Activitats coordinades per a dirigir i controlar una organització pel que fa als riscos.

Incident de seguretat

Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del Sistema d'Informació.

Informació

És qualsevol conjunt de dades que tenen significat. L'Esquema Nacional de Seguretat es limita a valorar aquells tipus d'informació que són rellevants per al procés administratiu i poden ser tractats en algun servei afecte a la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics. Per exemple, dades mèdiques, fiscals, administratius, contractacions, resolucions, notificacions, etc. En general, cal esperar que aquests tipus d'informació estiguen identificats en algun tipus d'ordenament general o particular de l'organisme, la qual cosa els confereix entitat pròpia i implica uns deures de l'administració respecte del tractament d'aquest tipus d'informació.

Política de seguretat

Conjunt de directrius plasmades en document escrit, que regeixen la forma en què una organització gestiona i protegeix la informació i els serveis que considera crítics.

Principis bàsics de seguretat

Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis.

Responsable de la informació

Persona que té la potestat d'establir els requisits d'una informació en matèria de seguretat.

Responsable de la seguretat

El responsable de seguretat determinarà les decisions per a satisfer els requisits de seguretat de la informació i dels serveis.

Responsable del servei

Persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.

Responsable del sistema

Persona que s'encarrega de l'explotació del sistema d'informació.

Servei

Funció o prestació exercida per alguna entitat oficial destinada a cuidar interessos o satisfer necessitats dels ciutadans.

Sistema d'informació

Conjunt organitzat de recursos perquè la informació es puga arreplegar, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

ANNEXE B. GLOSSARI D'ABREVIATURES.

ENS Esquema Nacional de Seguretat

TIC Tecnologies de la Informació i les Comunicacions

ANNEXE C. REFERÈNCIES

CCN-STIC-402

Organització i Gestió per a la Seguretat dels Sistemes TIC. Desembre 2006.

CCN-STIC-801

ENS - Responsables i Funcions. 2010.

Llei 11/2007

Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics. BOE de 23 de juny de 2007.

Llei 15/1999

Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. BOE de 14 de desembre de 1999.

RD 1720/2007

Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. BOE de 19 de gener de 2008.

RD 3/2010

Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica. BOE de 29 de gener de 2010.