DECRET 1160/2020, de 29 de setembre de 2020
Aprovació de la Política de Seguretat de la Informació

En exercici de les facultats que la legalitat vigent confereix a l'Alcaldia i ateses les consideracions següents:

Antecedents

1. El dret de la ciutadania a relacionar-se amb les Administracions Públiques utilitzant mitjans electrònics per l'exercici de les seues pretensions, porta aparellat unes obligacions correlatives de l'Administració, la qual ha de crear les condicions de confiança en l'ús dels mitjans electrònics i establir les mesures necessàries per a que les tecnologies de la informació s'utilitzen respectant els drets que la ciutadania té reconeguts en la Constitució i la resta de l'ordenament jurídic, principalment, la preservació de la integritat dels drets fonamentals de les persones i en especial els relacionats amb la intimitat i protecció de dades personals.

2. El Real Decret 3/2010, de 8 de gener va aprovar l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració electrònica. La finalitat de l' ENS és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics mitjançant les mesures que garantitzen la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics que permeta a la ciutadania i a les Administracions Públiques l'exercici dels drets i compliment de les obligacions per mitjans electrònics.

3. 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 i han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, 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 garantir la continuïtat dels serveis prestats.

4. L'Ajuntament de Silla, ha implementat la seu electrònica pera a que la ciutadania realitze els seus tràmits telemàticament. L'establiment d'una seu electrònica comporta la responsabilitat del titular respecte de la integritat, veracitat i actualització de la informació i els serveis als que se puguen accedir.

5. L'Ajuntament de Silla, el funcionariat i resta d'empleades/ts públics han de realitzar un seguiment continu dels nivells de prestació dels serveis, seguir i analitzar les vulnerabilitats reportades i preparar una resposta efectiva a les incidències per garantir la continuïtat dels serveis prestats.

6. Les diferents unitats organitzatives de l'Ajuntament de Silla hauran de conscienciar-se de que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema i aplicar les mesures mínimes de seguretat exigides per l'ENS.

7. Per a realitzar l'adaptació a l'ENS de l'Ajuntament de Silla, la Junta de Govern local per acord de data 29 d'octubre de 2019 va adjudicar el contracte a GOVERTIS ADVISORY SERVICES, SL. CIF: B97637151.

8. L'empresa ha estat treballant junt al servei TIC per tal de redactar en un document de Política de Seguretat en la Informació de l'Ajuntament de Silla i adaptar-la a l'Esquema Nacional de Seguretat.

9. En aquest document se plasma l'obligació de l'Administració, de la designació diferenciada del responsable de la informació, del responsable del servei i el responsable de la seguritat i delegada de protecció de dades.

10. El Tècnic de gestió informàtica, adscrit al Servei TIC de l'Ajuntament ha redactat aquest document junt a la tècnica de l'empresa Govertis Advisory Services S.L. i ha realitzat la proposta d'aprovació d'aquest document que consta part d'aquesta Resolució com Annex I.

11. L'òrgan competent per l'aprovació és l'Alcaldia d'acord amb les atribucions que li atorga l'article 21.1. a) de la Llei 7/85, Reguladora de les Bases de Règim local.

12. La Vicesecretaria-Interventora ha realitzat informe jurídic ref.40/2020.

Fonaments

1. Resulta aplicable la normativa següent:

– Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades. Articles 5 i 32

- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals. Disposició addicional primera
- Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim local (LBRL). l'article 21.1. a)
- Llei 8/2010, de la Generalitat, de règim local de la CV (LRLCV).
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques. Articles 12, 13, 17 i 27.
- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic. Article 156
- Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica. Articles, 4,5,10, 11, 12,14 i 15.

Per tot l' anteriorment exposat:

DISPOSE:

Primer. Aprovar la Política de Seguretat de la Informació de l'Ajuntament de Silla, document que s'inclou com Annex I de la present Resolució.

Segon. Els criteris i instruccions contingudes en el document que s'aprova en la present resolució constitueixen directrius vinculants per a totes les Unitats administratives de l'Ajuntament de Silla i OOAA Conservatori de Música.

Tercer. Designar la funció diferenciada dels següents:
Responsable de la informació: Alcaldia o regidoria en la que delegue.
Responsable dels serveis: Els responsables de les unitats funcionals amb serveis en la seu electrònica
Responsable de la seguritat: El Tècnic de gestió d'informàtica

Quart. Designar, així mateix els següents rols:
Responsable del sistema: el Tècnic de sistemes informàtics,
Administrador de la Seguridad del Sistema: el Tècnic auxiliar de informàtica,
Responsable de Seguridad Física: al/la Comissari/a, i,
Responsable de Gestió de Personal: al/la Tècnic/a Responsable de Recursos Humans,

Cinquè. Se crea el Comitè de Seguretat de la Informació que estarà compost pels següents membres:
PRESIDENT: Alcaldia o regidoria en qui delegue.
SECRETARI: Responsable de Seguretat de la Informació.
VOCALS:

- Secretaria o persona en qui delegue.
- Responsable de TIC.
- Responsable del Sistema.
- Responsable de Gestió Documental.
- Responsable del Servei OAC.

Sisè. Traslladar aquesta Resolució a totes les àrees de l'organització municipal i del OOAA Conservatori de Música i a les persones a les quals se'ls ha designat com a responsables de l'organització de la seguretat així com als membres del Comitè de Seguretat de la Informació. (Annex I Punt 3)

Sete. Publicar el document de Política de Seguretat de la Informació al Portal de Transparència de l'Ajuntament de Silla així com totes les versions d'actualització.

I, perquè conste, Vicente Zaragozá Alberola, alcalde, signe davant la Secretària General de la Corporació, Paz Zaragozá Campos.

L'Alcalde

AJUNTAMENT de SILLA
Firmado digitalmente por VICENTE| ZARAGOZA|ALBEROLA
Nombre de reconocimiento (DN): cn=VICENTE|ZARAGOZA|ALBEROLA, serialNumber=73767443A, givenName=VICENTE, sn=ZARAGOZA ALBEROLA, title=ALCALDE., ou=ALCALDE, ou=CERTIFICADO ELECTRONICO DE EMPLEADO PÚBLICO, o=AYUNTAMIENTO DE SILLA, c=ES
Fecha: 2020.09.29 11:52:44 +02'00'

La Secretaria

ZARAGOZA CAMPOS MARIA DE LA PAZ - DNI 21479778D
Firmado digitalmente por ZARAGOZA CAMPOS MARIA DE LA PAZ - DNI 21479778D
Fecha: 2020.09.29 12:14:54 +02'00'

ÍNDEX

1 INTRODUCCIÓ

1.1 JUSTIFICACIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

L'Ajuntament de Silla depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per a aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguen afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant 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, 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. És per això que l'Esquema Nacional de Seguretat (Reial decret 3/2010 de 8 de Gener, d'ara en avant ENS), 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".

Això implica que les diferents àrees de l'Ajuntament han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, 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.

Totes les àrees 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 previndre, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'Article 7 de l'ENS.

1.2 MISSIÓ I SERVEIS PRESTATS

L'Ajuntament de Silla com a Òrgan de Govern Municipal, per a la gestió dels seus interessos, i en l'àmbit de les seues competències i com a Administració pública, serveix amb objectivitat els interessos generals i actua d'acord amb els principis d'eficàcia, jerarquia, descentralització i coordinació, promou tota classe d'activitats i presta els serveis públics que contribueixen a satisfer les necessitats i aspiracions dels habitants del municipi.

La present Política de Seguretat aplica a les diferents activitats en les quals participa l'Ajuntament a través de mitjans electrònics, en concret:

a. Les relacions de caràcter jurídic-econòmic entre els ciutadans i l'Ajuntament.
b. La consulta per part dels ciutadans de la informació pública administrativa i de les dades administratives que estiguen en poder de l'Ajuntament.
c. La realització dels tràmits i procediments administratius incorporats per a la seua tramitació en la seu electrònica de l'ajuntament, de conformitat amb el que es preveu en l'ordenança municipal reguladora de l'ús de l'administració electrònica.
d. El tractament de la informació obtinguda per l'ajuntament en l'exercici de les seues potestats.

2 MARC NORMATIU

Com a base normativa per a realitzar la present guia de seguretat, s'ha analitzat la legislació vigent, que afecta el desenvolupament de les activitats de l'Administració Local en el que a administració electrònica es refereix, i que implica la implantació de manera explícita de mesures de seguretat en els sistemes d'informació. El marc legal en matèria de seguretat de la informació ve establit per la següent legislació:

- Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, que assenyala en el seu art. 17.3 que els mitjans o suports en què s'emmagatzemen documents , hauran de comptar amb les mesures de seguretat que estableix l'Esquema Nacional de Seguretat, que garantisquen una sèrie de principis (com a integritat, autenticitat, confidencialitat, qualitat, protecció i conservació dels documents

emmagatzemats); i, estableix també, en el seu art. 27.3 que les Administracions Públiques hauran de complir amb l'Esquema Nacional de Seguretat per a garantir la identitat i contingut de les còpies electròniques o en paper, és a dir, el caràcter de còpies autèntiques. Finalment, disposa en la seua Disposició Addicional segona que, tant les Comunitats Autònomes, com les Entitats Locals, hauran de garantir la seua compatibilitat informàtica i interconnexió, així com la transmissió telemàtica de les sol•licituds, escrits i comunicacions que es realitzen en els seus corresponents registres i plataformes mitjançant el compliment, igualment, de l'Esquema Nacional de Seguretat. I que, a més, deroga la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

- 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, fixa els principis bàsics i requisits mínims, així com les mesures de protecció a implantar en els sistemes de l'Administració.
- Reial decret 951/2015, de 23 d'octubre, de modificació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica, la finalitat de la qual és la creació de les condicions necessàries per a garantir l'adequat nivell d'interoperabilitat tècnica, semàntica i organitzativa dels sistemes i aplicacions emprats per les Administracions públiques, que permeta l'exercici de drets i el compliment de deures a través de l'accés electrònic als serveis públics, alhora que redunda en benefici de l'eficàcia i l'eficiència.
- 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).
- Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

3 ORGANITZACIÓ DE LA SEGURETAT

3.1 DEFINICIÓ DE ROLS

Tal com indica l'article 12 de l'ENS, la seguretat haurà de comprometre a tots els membres de l'organització. La Política de Seguretat, segons detalla l'Annex II de l'ENS, en la seua secció 3.1, ha d'identificar uns clars responsables per a vetllar 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:

A RESPONSABLE DE LA INFORMACIÓ

Serà responsable de la Informació l'Alcaldia o òrgan en qui delegue, a qui li corresponen les següents funcions:

- Adoptar les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat dels tractaments de dades de caràcter personal i eviten la seua alteració, pèrdua, tractament o accés no autoritzat, tenint en compte de l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos al fet que estan exposats, ja provinguen de l'acció humana o del medi físic o natural.
- Té la responsabilitat última de l'ús que es faça d'una certa informació i, per tant, de la seua protecció.
- El Responsable de la Informació 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 establit en l'Annex I de l'Esquema Nacional de Seguretat.
- 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.

B. RESPONSABLES DEL SERVEI

Seran responsables del Servei cadascun dels responsables d'unitats funcionals amb serveis en la seu electrònica (Caps d'àrea, de servei) als que els correspon les següents funcions:

- Quant al RGPD, s'encomana al Responsable del Servei el desenvolupament de les tasques relacionades amb la gestió dels tractaments de dades personals que es realitzen en la seua àrea en concret.

- Estableix els requisits dels serveis en matèria de seguretat. En el marc del ENS, equival a la potestat de determinar els nivells de seguretat de la informació.
- Té la responsabilitat de l'ús que es faça de determinats serveis i, per tant, de la seua protecció.
- El Responsable del Servei serà responsable de qualsevol error o negligència que porte a un incident de disponibilitat dels serveis.
- Determinarà els nivells de seguretat en cada dimensió del servei dins del marc establert en l'Annex I de l'Esquema Nacional de Seguretat d'acord amb la proposta dels Responsables de Seguretat i del Sistema.
- Encara que l'aprovació formal dels nivells corresponga al Responsable del Servei, podrà recaptar una proposta al Responsable de la Seguretat i del Responsable del Sistema.
- La prestació d'un servei sempre ha d'atendre els requisits de seguretat de la informació que maneja, de manera que poden heretar-se els requisits de seguretat d'aquesta, afegint requisits de disponibilitat, així com uns altres com a accessibilitat, interoperabilitat, etc.

Responsables dels serveis:

- Alcaldia:Alcaldia
- Àrea Técnica: Caps d' àrea.
- Àrea d'administració i serveis interns: Cap d'àrea.
- Àrea d'animació ciutadana: Cap d'àrea.
- Àrea de salut pública i benestar: Cap d'àrea
- Àrea econòmica: Cap d'àrea.
- Àrea seguretat ciutadana: Cap d'àrea.

C RESPONSABLE DE LA SEGURETAT DE LA INFORMACIÓ

Serà responsable de Seguretat de la Informació al Tècnic de gestió d'informàtica, a qui li correspondran les següents funcions:

- Coordinarà i controlarà les mesures definides en el Registre d'activitats del tractament i en general s'encarregarà del compliment de les mesures de seguretat que detalla l'informe d'avaluació d'impacte en la protecció de dades.
- Reportarà 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.
- Mantindrà la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb el que s'estableix 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 de l'ENS i del resultat de l'Anàlisi de Riscos.
- Facilitarà als Responsable d'Informació i als Responsables de Servei o Àrea 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 per l'ENS.
- Coordinarà l'elaboració de la Documentació de Seguretat del Sistema.
- Participarà en l'elaboració, en el marc del Comité de Seguretat de la Informació, la Política de Seguretat de la Informació, per a la seua aprovació per Direcció.
- 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 qual està exposat el sistema).
- Elaborarà, al costat dels Responsables de Sistemes, Plans de Millora de la Seguretat, per a la seua aprovació pel Comitè de Seguretat de la Informació.
- Elaborarà els Plans 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 Plans 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.

Com a Secretari del Comitè de Seguretat de la Informació li correspon:

- Convocar les reunions del Comitè de Seguretat de la Informació.
- Preparar els temes a tractar en les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elaborar l'acta de les reunions.
- És responsable de l'execució directa o delegada de les decisions del Comitè.

D RESPONSABLE DEL SISTEMA

Serà a responsable del Sistema al Tècnic de Sistemes Informàtics, al qual li corresponen les següents funcions:

- Desenvolupar, operar i mantindre el Sistema d'Informació 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 del Sistema d'Informació 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.
- 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 la satisfacció dels requisits establits. 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.
- Monitorar l'estat de la seguretat del Sistema d'Informació i reportar-lo periòdicament o davant incidents de seguretat rellevants al Responsable de Seguretat de la Informació.
- Elaborar els Plans 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 Plans de Continuïtat del Sistema per a mantindre'ls 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.

E ADMINISTRADOR DE LA SEGURETAT DEL SISTEMA

Serà Administrador de la Seguretat del Sistema a l'Informàtic i al Tècnic auxiliar d'informàtica, als quals, com a tal, li corresponen les següents funcions:

- La implementació, gestió i manteniment de les mesures de seguretat aplicables al Sistema d'Informació.
- Assegurar que els controls de seguretat establits 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 aquest, tant interns com 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, en el seu cas, 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 continuen operatius els mecanismes i serveis de seguretat habilitats.
- Informar els Responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Monitorar 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 tindre conseqüències greus (aquestes actuacions haurien d'estar reflectides en un procediment documentat 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 reflectides en un procediment documentat per a reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Mantindre 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.

F RESPONSABLE DE SEGURETAT FÍSICA

Serà responsable de Seguretat Física al/la Comissari/a, al qual li correspondrà implantar les mesures de seguretat que li competisquen dins de les determinades pel responsable de la Seguretat de la Informació, i informarà a aquest del seu grau d'implantació, eficàcia i incidents.

G RESPONSABLE DE GESTIÓ DE PERSONAL

Serà responsable de Gestió de Personal al/la Tècnic/a Responsable de Recursos Humans, al qual li correspon implantar les mesures de seguretat que li competisquen dins de les determinades pel Responsable de Seguretat de la Informació, i informarà a aquest del seu grau d'implantació, eficàcia i incidents.

3.2 COMITÈ DE SEGURIDAD DE LA INFORMACIÓ

Se crea el Comitè de Seguretat de la Informació que estarà compost pels següents membres:

PRESIDENT: Alcaldia o regidoria en qui delegue.

SECRETARI: Responsable de Seguretat de la Informació.

VOCALS:

Secretaria o persona en qui delegue.

Responsable de TIC.

Responsable del Sistema.

Responsable de Gestió Documental.

Responsable del Servei OAC.

Podran acudir a requeriment del Comitè qualssevol altres Caps de Servei o Àrea i responsables la intervenció de les quals siga precisa per ser afectats per l'Esquema Nacional de Seguretat i pel RGPD.

Les funcions del Comitè de Seguretat de la Informació són les següents:

- Atendre les inquietuds de l'Alta Direcció i dels diferents departaments.
- Informar regularment de l'estat de la seguretat de la informació a l'Alta Direcció.
- Promoure la millora contínua del Sistema de Gestió de la Seguretat de la Informació.
- Elaborar l'estratègia d'evolució de l'Ajuntament 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 la Direcció.
- 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.
- Monitorar els principals riscos residuals assumits per l'Ajuntament i recomanar possibles actuacions respecte d'ells.
- Monitorar 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'Ajuntament. En particular, vetllarà per la coordinació de diferents plans que puguen realitzar-se en diferents àrees.
- Vetllar perquè la seguretat de la informació es tinga en compte en tots els projectes TIC des de la seua especificació inicial fins a la seua posada en operació. En particular, haurà de vetllar per la creació i utilització de serveis horitzontals que reduïsquen duplicitats en pro d'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.
- Recaptarà regularment del personal tècnic propi o extern, la informació pertinent per a prendre decisions.
- S'assessorarà dels temes que 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 mixtos.
    - Assessoria interna i/o externa.
    - Assistència a cursos o un altre tipus d'entorns formatius o d'intercanvi d'experiències.

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

- Aprovarà el Pla de Millora de la Seguretat, amb la seua dotació pressupostària corresponent.

3.3 JERARQUÍA EN EL PROCES 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 dona 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 el que s'estableix en la política de seguretat aprovada per a l'Organització.

L'Administrador de la Seguretat del Sistema reporta al Responsable del Sistema:

- Incidents relatius a la seguretat del sistema.
- Accions de configuració, actualització o correcció.

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

El Responsable del Sistema informa el 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 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 el 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.
- Resum consolidat d'incidents relatius a la seguretat de la informació.
- Estat de la seguretat del sistema, en particular del risc residual al qual el sistema està exposat.

El Responsable de la Seguretat informa la Direcció de l'Organització, segons els acords en el Comitè de Seguretat de la Informació.

Quan no existisca un Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta directament a la Direcció 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 qual el sistema està exposat.

3.4 PROCEDIMIENTS DE DESIGNACIÓ DE PERSONES

La Direcció de l'Organització nomenarà formalment:

- Al Responsable de la Informació; pot ser un càrrec unipersonal o un òrgan col•legiat (típicament, el Comitè de Seguretat de la Informació).
- Als Responsables del Servei; pot ser el mateix que el Responsable de la Informació; pot ser un càrrec unipersonal o un òrgan col•legiat (típicament, el Comitè de Seguretat de la Informació).
- Al Responsable de la Seguretat, que ha de reportar directament a la Direcció o, quan existisca, al Comitè de Seguretat de la Informació.
- Al Responsable del Sistema, que ha de reportar directament a la Direcció o, quan existisca, al Comitè de Seguretat de la Informació.

La Direcció de l'Organització designa 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 Direcció de l'Organització designa a l'Administrador de Seguretat del Sistema a proposta del Responsable del Sistema o del Responsable de Seguretat de la Informació.

4 DADES DE CARÀCTER PERSONAL

Per a la prestació dels serveis previstos han de ser tractades dades de caràcter personal. el registre d'activitats del tractament detalla els tractaments afectats i els responsables corresponents, així com les mesures adoptades derivades de l'anàlisi de riscos realitzat sobre els diferents tractaments de dades. 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 registre d'activitats del tractament.

4.1 FIGURES VINCULADES A PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

4.1.1 FUNCIONS I OBLIGACIONS DEL RESPONSABLE DEL TRACTAMENT

El Responsable del tractament és la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideix sobre la finalitat, contingut i ús del tractament.

A l'efecte de l'entitat local s'ha atribuït la condició de Responsable de Tractament a la persona jurídic-pública, és a dir, al propi Ajuntament de Silla. De manera que, s'ha entés que l'Ajuntament és Responsable del Tractament de les dades de caràcter personal, que obren en els seus sistemes d'informació, i que deriven de la prestació dels serveis públics atribuïts a nivell de competències.

Al seu torn, cal dir que la consideració de Responsable de Tractament no ha de ser associada a persona física representant de l'Ajuntament, en qualitat del càrrec o lloc (com, per exemple, l'Alcalde o Secretari).

Les funcions del Responsable del tractament són:

- Adoptar les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat de les dades de caràcter personal i eviten la seua alteració, pèrdua, tractament o accés no autoritzat.
- Haurà d'informar els titulars de les dades els drets que els assisteixen i en els termes en els quals poden exercir-los.
- Haurà d'excloure del tractament les dades relatives a l'afectat que s'opose al tractament d'aquests.
- Haurà de cessar en la utilització o cessió il·lícita de les dades quan així ho requerisca l'interessat.
- Obligació de fer efectiu el dret de rectificació o supressió de l'interessat en el termini màxim d'1 mes.
- Notificar les rectificacions o cancel·lacions efectuades en les dades personals a qui s'haja comunicat aquestes dades, en el cas que es mantinga el tractament per aquest últim, que deurà també procedir a la cancel·lació.

4.1.2 FUNCIONS I OBLIGACIONS DE LA/EL DELEGADA/T DE PROTECCIÓ DE DADES

La/El DPD pot ser una persona física o un òrgan col•legiat, les funcions del qual s'assenyalen en l'article 39 del Reglament (UE) 679/2016, així com els articles 36 i 37 de la Llei orgànica 3/2018, i s'ocupa de l'aplicació de la legislació sobre privacitat i protecció de dades en l'entitat en la qual desenvolupa les seues funcions.

L'Ajuntament de Silla ha nomenat com a Delegat de Protecció de Dades a Govertis Advisory Services S.L.

La/El delegada/t de protecció de dades tindrà com a mínim les següents funcions:

a) informar i assessorar el responsable o a l'encarregat del tractament i als empleats que s'ocupen del tractament de les obligacions que els incumbeixen en virtut del present Reglament i d'altres disposicions de protecció de dades de la Unió o dels Estats membres;

b) supervisar el compliment del que es disposa en el present Reglament, d'altres disposicions de protecció de dades de la Unió o dels Estats membres i de les polítiques del responsable o de l'encarregat del tractament en

matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents;

c) 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;

d) cooperar amb l'autoritat de control;

e) actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36, i realitzar consultes, en el seu cas, sobre qualsevol altre assumpte.

El delegat de protecció de dades exercirà les seues funcions prestant la deguda atenció als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i finalitats del tractament.

Per a això haurà de ser capaç de:

a) Recaptar informació per a determinar les activitats de tractament,

b) analitzar i comprovar la conformitat de les activitats de tractament,

c) informar, assessorar i emetre recomanacions al responsable o l'encarregat del tractament.

d) Recaptar informació per a supervisar el registre de les operacions de tractament.

e) Assessorar en l'aplicació del principi de la protecció de dades per disseny i per defecte.

f) Assessorar sobre:

- Si s'ha de dur a terme o no una avaluació d'impacte de la protecció de dades
- Quina metodologia ha de seguir-se en efectuar una avaluació d'impacte de la protecció de dades.
- Si s'ha de dur a terme l'avaluació d'impacte de la protecció de dades amb recursos propis o amb contractació externa.
- Quines salvaguardes (incloses mesures tècniques i organitzatives) aplicar per a mitigar qualsevol risc per als drets d'interessos dels afectats.
- Si s'ha dut a terme correctament o no l'avaluació d'impacte de la protecció de dades i
- Si les seues conclusions (si seguir avant o no amb el tractament i quines salvaguardes aplicar) són conformes al Reglament.

g) Prioritzar les seues activitats i centrar els seus esforços en aquelles qüestions que presenten majors riscos relacionats amb la protecció de dades.

h) Assessorar el responsable del tractament sobre:

- Quina metodologia emprar en dur a terme una avaluació d'impacte de la protecció de dades,
- quines àrees han de sotmetre's a auditoria de protecció de dades interna o externa,
- quines activitats de formació internes proporcionar al personal o als directors responsables de les activitats de tractament de dades i a quines operacions de tractament dedicar més temps i recursos.

La/El DPD haurà de reunir coneixements especialitzats del Dret i la pràctica en matèria de protecció de dades. S'han identificat, en conseqüència, aquells coneixements, habilitats o destreses necessàries que ha de saber o posseir la/el Delegada/t de Protecció de Dades per a dur a terme una de les funcions pròpies del seu lloc.

Aquestes funcions genèriques de la/del DPD es poden concretar en tasques d'assessorament i supervisió, entre altres, en les següents àrees:

1. Compliment de principis relatius al tractament, com els de limitació de finalitat, minimització o exactitud de les dades.
2. Identificació de les bases jurídiques dels tractaments.
3. Valoració de compatibilitat de finalitats diferents de les que van originar la recollida inicial de les dades.
4. Determinació de l'existència de normativa sectorial que puga determinar condicions de tractament específiques diferents de les establides per la normativa general de protecció de dades.
5. Disseny i implantació de mesures d'informació als afectats pels tractaments de dades.
6. Establiment de mecanismes de recepció i gestió de les sol•licituds d'exercici de drets per part dels interessats.

7. Valoració de les sol•licituds d'exercici de drets per part dels interessats.
8. Contractació d'encarregats de tractament, inclòs el contingut dels contractes o actes jurídics que regulen la relació responsable-encarregat.
9. Identificació dels instruments de transferència internacional de dades adequades a les necessitats i característiques de l'organització i de les raons que justifiquen la transferència.
10. Disseny i implantació de polítiques de protecció de dades.
11. Auditoria de protecció de dades.
12. Establiment i gestió dels registres d'activitats de tractament.
13. Anàlisi de riscos dels tractaments realitzats.
14. Implantació de les mesures de protecció de dades des del disseny i protecció de dades per defecte adequades als riscos i naturalesa dels tractaments.
15. Implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments.
16. Establiment de procediments de gestió de violacions de seguretat de les dades, inclosa l'avaluació del risc per als drets i llibertats dels afectats i els procediments de notificació a les autoritats de supervisió i als afectats.
17. Determinació de la necessitat de realització d'avaluacions d'impacte sobre la protecció de dades.
18. Realització d'avaluacions d'impacte sobre la protecció de dades
19. Relacions amb les autoritats de supervisió
20. Implantació de programes de formació i sensibilització del personal en matèria de protecció de dades.

4.1.3 FUNCIONS I OBLIGACIONS D'USUARIS AMB ACCES A DADES

Tots els empleats de l'entitat estan subjectes a funcions i obligacions. Tot el personal de l'entitat que dispose d'accés a les dades de caràcter personal ha de complir amb les següents obligacions:

- No es permet la difusió de dades de caràcter personal ni confidencial pertanyent a l'entitat. Estant obligat a guardar secret de la informació fins i tot acabada la relació laboral.
- L'usuari es responsabilitzarà de notificar tota incidència segons el procediment de gestió d'incidències, no notificar una incidència serà considerada una omissió del deure del treballador.
- L'usuari es responsabilitzarà de tots els accessos que es realitzen sota el seu identificador i contrasenya, per tant, no haurà de revelar la contrasenya.
- L'usuari es responsabilitzarà sempre que abandone el lloc de treball de tancar la seua sessió o bloquejar l'equip amb contrasenya.
- No es podran instal•lar aplicacions en els sistemes de l'entitat sense el consentiment del delegat de protecció de dades.
- No es permet la còpia de dades de caràcter personal, en suports, sense l'autorització expressa del delegat de protecció de dades.
- L'usuari es responsabilitzarà de guardar còpies de tots els correus que incloguen annexos amb dades personals vinculades a l'entitat.

4.1.4 FUNCIONS I OBLIGACIONS DE L'ENCARREGAT/DA DEL TRACTAMENT

Els encarregats del tractament tenen com a missió fer les tasques ordinàries per al desenvolupament efectiu de les funcions per a les quals ha sigut creat el tractament per compte del Responsable del tractament.

En aquest sentit, l'**apartat 8 de l'article 4 del RGPD** defineix a l'Encarregat de Tractament com <<la persona física o jurídica, autoritat pública, servei o un altre organisme que tracte dades personals per compte del responsable del tractament>>.

L'Encarregat del Tractament haurà d'aplicar les mesures d'índole tècnica i organitzatives necessàries que garantisquen la seguretat de les dades de caràcter personal i eviten la seua alteració, pèrdua, tractament o accés no autoritzat.

Igualment haurà d'implementar les mesures de seguretat a què es refereix el paràgraf anterior i que apareixeran estipulades en el contracte amb el Responsable del Tractament.

En concret, les seues funcions són les de:

- Tractar les dades del tractament.
- Realitzar el control de tractament, qualitat i seguretat de les dades.
- Controlar la forma i requisits per a procedir a les addicions i cancel•lacions.
- Controlar els suports de seguretat.
- Control i accés de contrasenyes.
- Manteniment del registre d'incidències.
- Crear una llista per a les situacions en la qual un afectat no desitge que les seues dades personals s'emmagatzemen en el tractament.
- Donar trasllat al responsable del tractament d'aquelles sol•licituds d'exercici de dret que es reben per part dels interessats.

En conseqüència, l'Ajuntament de Silla haurà de dur a terme un document actualitzat on s'identificaran els encarregats de tractament que estan prestant serveis en l'entitat local, així com la indicació de la formalització del pertinent contracte amb aquests prestadors de serveis amb accés a dades.

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 establits per l'Esquema Nacional de Seguretat, segons el que es preveu en l'Article 6 de l'ENS.

5.2 CRITERIS D'AVALUACIÓ DE RISCOS

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat de la Informació 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.

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 manera 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 de la Informació dinamitzarà la disponibilitat de recursos per a atendre 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 després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II de l'ENS) hauran de ser acceptats prèviament pel seu Responsable d'aqueixa Informació.

Els nivells de Risc residuals esperats sobre cada Servei després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II de l'ENS) hauran de ser acceptats prèviament pel seu Responsable d'aqueix Servei.

Els nivells de risc residuals seran presentats pel Responsable de Seguretat de la Informació al Comité 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 el que s'estableix en l'Article 9 de l'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 ocòrrega 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 previndre en la mesura que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. L'ENS mitjançant l'article 19 estableix que els sistemes han de dissenyar-se i configurar-se de manera que garantisquen la seguretat per defecte. D'igual forma, l'article 17 de l'esmentat ENS defineix que els sistemes s'instal·laran en àrees separades, dotades d'un procediment de control d'accés.

Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'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 hauran:

- Establir àrees segures per als sistemes d'informació crítica o confidencial.
- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent 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.

6.2 MONITORITZACIÓ I DETECCIÓ D'INCIDENTS

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 reporte que arriben als responsables regularment i quan es produïsca una desviació significativa dels paràmetres que s'hagen preestablert com a normals.

Els sistemes de detecció d'intrusos compleixen fonamentalment amb una labor de supervisió i auditoria sobre els recursos de l'Organització, verificant que la política de seguretat no és violada i intentant identificar qualsevol tipus d'activitat maliciosa d'una forma primerenca i eficaç.

S'hauran d'establir, en funció de les necessitats, les següents classificacions:

- Sistemes de detecció d'intrusos a nivell de xarxa.
- Sistemes de detecció d'intrusos a nivell sistema.

6.3 RESPOSTA DAVANT INCIDENTS

Els departaments han de:

- Establir mecanismes per a respondre eficaçment als incidents de seguretat.
- Designar punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).

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

Tots els membres de l'organització tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, és responsabilitat del Comité de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribe als afectats.

Tots els membres de l'organització atendran 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.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura en què la necessiten per a fer el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seua primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

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 es presten serveis o es gestione informació d'altres organitzacions, se'ls farà partícip d'aquesta Política de Seguretat de la Informació, s'establiran canals per a reporte i coordinació dels respectius Comités de Seguretat de la Informació i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan s'utilitzen serveis de tercers o cedisca informació a tercers, 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 aquesta 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 de tercers 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 manera de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir avant.

9 REVISIÓ I APROVACIÓ DE LA POLÍTICA DE SEGURETAT

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 duració, 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 de l'ENS.

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

10 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 això 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 busquen ajudar els 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. Les guies ajuden a previndre 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.

ANNEX. 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.

Gestió d'incidències

Pla d'acció per a atendre 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 riscs

Activitats coordinades per a dirigir i controlar una organització respecte als riscos.

Incident de seguretat

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

Informació

Cas concret d'un cert 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 consideren 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 recollir, emmagatzemar, processar o tractar, mantindre, usar, compartir, distribuir, posar a disposició, presentar o transmetre.