NOR01 –Política de seguretat de la informació

Classificació de la Informació:

Nivell del Document	Normativa
Nom del Fitxer	NOR01 -Politica de Seguridad de la Informacion ca - copia.es.ca.docx
Tipus	Difusió pública
Àmbit de Difusió	Comitè de Seguretat de l'AJUNTAMENT DE PAIPORTA
Responsable	Responsable de Seguretat de l'AJUNTAMENT DE PAIPORTA

CONTROL DE SIGNATURES

	DATA	SIGNATURA
ELABORAT PER MARIA SANCHIS	22/02/2024	
APROVAT PER JUNTA DE GOVERN LOCAL	15/3/2024	

CONTROL DE VERSIONS

VERSIÓ	DATA	AUTOR	CANVIS
1.0	26/03/2019	Maria Sanchis	Versió inicial del document Aprovació per la 1a reunió del Comitè de Seguretat de la Informació.
1.0	06/05/2019	Maria Sanchis	Primera aprovació per la Junta de Govern Local.
1.0	27/11/2019	Maria Sanchis	Primera publicació al BOP núm. 134.
2.0	04/05/2020	Maria Sanchis	Actualització de membres per la 3a reunió ordinària del Comitè de Seguretat de la Informació.
2.0	30/3/2021	Maria Sanchis	Segona aprovació per la Junta de Govern Local.
2.0	04/05/2021	Maria Sanchis	Segona publicació al BOP núm. 83.
	22/02/2024	Maria Sanchis	Diverses modificacions: S'elimina el llistat de normativa i es mantindrà actualitzat un document extern tota la gestió de requisits legals. S'elimina com a vocal del Comitè al Tècnic/Igualtat. Es revisen els rols i les funcions del Comitè. S'hi afegeixen les funcions del rol Responsable d'Informació i de Serveis.
3.0	15/03/2024	Maria Sanchis	Tercera aprovació per la Junta de Govern Local.

ÍNDEX DE CONTINGUT

1. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 15 de març del 2024 per la Junta de Govern Local.

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

2. INTRODUCCIÓ

L'Ajuntament de Paiporta depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per assolir els objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant de danys accidentals o deliberats que puguin afectar l'autenticitat, la traçabilitat, la disponibilitat, la integritat o la 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 incidir en la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, cal una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

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

Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents segons l'Esquema Nacional de Seguretat.

3. MISSIÓ DE L'AJUNTAMENT DE PAIPORTA

L'Ajuntament de Paiporta per assolir els seus objectius assumeix el seu compromís amb la seguretat de la informació, comprometent-se a la gestió adequada d'aquesta, per tal d'oferir a tota la seva ciutadania les garanties més grans al voltant de la seguretat de la informació utilitzada.

Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant de danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

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

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, cal una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació continuada dels serveis. Això implica que els departaments han d'aplicar les mesures de seguretat exigides per l'Esquema Nacional de, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els diferents departaments han d'assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la 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, tant per als productes que desenvolupa i els seus serveis associats, com pel que fa al programari base adquirit de tercers.

Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, segons l'article 8 de l'ENS (Article 8. Prevenció, detecció, resposta i conservació).

4. ABAST

Aquesta Política s'aplicarà als sistemes d'informació de l'Ajuntament de Paiporta, que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o procediment administratiu i que es troben dins de l´abast de l´Esquema Nacional de Seguretat (ENS).

5. MARC NORMATIU

El marc normatiu que afecta el desenvolupament de les activitats i competències de l'Ajuntament de Paiporta, està constituït per normes jurídiques estatals i autonòmiques, si escau, orientades a l'administració electrònica, a la seguretat de la informació i els serveis que la manegen, així com a la protecció de dades de naturalesa personal.

Les normes que constitueixen aquest marc, es troben recollides en un registre a aquest efecte, el qual es manté actualitzat segons assenyala el corresponent PRO026 - Procediment de gestió de requisits legals.

També podran formar part del marc esmentat, aquelles normes aplicables a l'Administració electrònica de l'Ajuntament, que siguin desenvolupament de les anteriors o estiguin relacionades, podent ser addicionalment publicades a les seus electròniques compreses dins l'àmbit d'aplicació d'aquesta política.

6. COMPLIMENT D'ARTICLES

L'Ajuntament de Paiporta, per assolir el compliment dels articles del Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, que recullen els principis bàsics i dels requisits mínims, ha implementat diverses mesures de seguretat proporcionals a la naturalesa de la informació i els serveis a protegir i tenint en compte la categoria dels sistemes afectats.

Seguretat com un procés integral i seguretat per defecte

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

Es prestarà la màxima atenció a la conscienciació de les persones que intervenen en el procés i als seus responsables jeràrquics perquè, ni la ignorància, ni la manca d'organització i coordinació, ni instruccions inadequades, siguin font de risc per a la seguretat.

Els sistemes es dissenyaran de manera que garanteixin la seguretat per defecte, de la manera següent:

a) El sistema proporcionarà la mínima funcionalitat requerida perquè l'organització assoleixi els objectius.

b) Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i sassegurarà que només són accessibles per les persones, o des d'emplaçaments o equips, autoritzats, podent exigir si escau restriccions d'horari i punts d'accés facultats.

c) En un sistema d'explotació s'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que no siguin d'interès, siguin innecessàries i, fins i tot, aquelles que siguin inadequades per tal que es persegueix.

d) L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari.

Reavaluació periòdica i integritat i actualització del sistema

L'Ajuntament de Paiporta, ha implementat controls i avaluacions regulars de la seguretat, (incloent-hi avaluacions dels canvis de configuració de forma rutinària), per conèixer en tot moment l'estat de la seguretat dels sistemes en relació amb les especificacions dels fabricants, a les vulnerabilitats ia les actualitzacions que els afectin, reaccionant amb diligència per gestionar el risc en vista de l'estat de seguretat dels mateixos. Abans de l'entrada de nous elements, ja siguin físics o lògics, aquests requeriran una autorització formal.

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

Gestió de personal i professionalitat

Tots els membres de l'Ajuntament de Paiporta, dins l'àmbit de l'ENS, atendran una sessió de conscienciació en matèria de seguretat almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per atendre tots els membres, en particular els 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 que la necessitin per fer la feina. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

Gestió de la seguretat basada en els riscos i anàlisi i gestió de riscos

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

- Regularment, almenys cada cop a l'any.
- Quan canviïn la informació manejada i/o els serveis prestats de manera significativa.
- Quan es produeixi un incident greu de seguretat o es detectin vulnerabilitats greus.

El Responsable de Seguretat ENS serà l'encarregat que es faci l'anàlisi de riscos, així com identificar carències i debilitats i posar-les en coneixement del Comitè de Seguretat de la Informació.

Incidents de seguretat, prevenció, reacció i recuperació

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

Perquè la informació i/o els serveis no es vegin perjudicats per incidents de seguretat, l'Ajuntament de Paiporta, implementa les mesures de seguretat establertes per l'ENS, així com qualsevol altre control addicional, que hagi identificat com a necessari, mitjançant una avaluació d'amenaces i riscs. Aquests controls, així com els rols i les responsabilitats de seguretat de tot el personal, estan clarament definits i documentats.

Quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals, s'establiran els mecanismes de detecció, anàlisi i reporti necessaris perquè arribin als responsables regularment.

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

- Mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).
- Per garantir la disponibilitat dels serveis, l'Ajuntament de Paiporta disposa dels mitjans i les tècniques necessàries que permeten garantir la recuperació dels serveis més crítics.

Línies de defensa i prevenció davant d'altres sistemes interconnectats

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

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

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

Funció diferenciada i organització i implantació del procés de seguretat

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

Autorització i control dels accessos

L'Ajuntament de Paiporta ha implementat mecanismes de control d'accés al sistema d'informació i els ha limitat als estrictament necessaris i degudament autoritzats.

Protecció de les instal·lacions

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

Adquisició de productes de seguretat i contractació de serveis de seguretat

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

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

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

Els sistemes han de disposar de còpies de seguretat i han d'establir els mecanismes necessaris per garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals de treball.

S'han desenvolupat procediments que asseguren la recuperació i la conservació a llarg termini dels documents electrònics produïts en l'àmbit de les competències d'Ajuntament de Paiporta. De la mateixa manera, s'han implementat mecanismes de seguretat sobre la base de la naturalesa del suport en què es trobin els documents, per garantir que tota informació

relacionada en suport no electrònic estigui protegida amb el mateix grau de seguretat que l'electrònica.

Registres d'activitat

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

Qualificació de la informació

Els criteris de qualificació que permetin ajustar els requisits de seguretat estaran establerts al document "PRO017 – Procediment de qualificació de la informació" que establirà qui és el responsable de cada informació manejada pel sistema.

7. ORGANITZACIÓ DE LA SEGURETAT

L'organització de la Seguretat de la Informació a l'Ajuntament de Paiporta s'estableix de la manera que s'indica a continuació.

7.1. ROLS O PERFILS DE SEGURETAT

Per garantir el compliment i l'adaptació de les mesures exigides reglamentàriament, s'han creat rols o perfils de seguretat i s'han designat els càrrecs o òrgans que els ocuparan, de la manera següent:

- Delegat de Protecció de Dades (DPD): AUDIDAT 3.0, SLU
- Responsable/s d'informació i serveis: secretari/ària.
- Responsable de Seguretat: Tècnic/a informàtic.
- Responsable del sistema: tècnic/a auxiliar informàtic.

7.2. COMITÈ DE SEGURETAT DE LA INFORMACIÓ

L'Ajuntament de Paiporta, ha constituït un Comitè de Seguretat de la Informació, com a òrgan col·legiat, i està format pels membres següents:

COMITÈ DE SEGURETAT DE LA INFORMACIÓ		
UNITAT	**DELEGAT/DA**	**FUNCIÓ**

ALCALDIA	Alcalde/sa	**President/a**
INNOVACIÓ	Responsable de seguretat	**Secretari/ària**
INNOVACIÓ	Responsable de sistemes	Vocal
SECRETARIA	Secretari/ària. Responsable de la informació i serveis.	Vocal
INNOVACIÓ	regidor/a.	Vocal
SEGURETAT CIUTADANA	Intendent de la Policia Local.	Vocal
DELEGAT DE PROTECCIÓ DE DADES	AUDIDAT 3.0, SLU	Vocal

El Responsable de la Informació i dels Serveis serà representat pel Secretari/ària de l'Ajuntament podent convocar algun altre Responsable d'Àrea en funció dels assumptes a tractar.

El Delegat de Protecció de Dades participarà amb veu, però sense vot a les reunions del Comitè de seguretat de la informació quan s'hi abordaran qüestions relacionades amb el tractament de dades de caràcter personal, així com sempre que es requereixi la seva participació. En tot cas, si un assumpte se sotmet a votació, s'ha de fer constar sempre en acta l'opinió del delegat de protecció de dades.

El Comitè de Seguretat de la Informació celebrarà les seves sessions a les dependències de l'Ajuntament de Paiporta, amb periodicitat anual, prèvia convocatòria a aquest efecte realitzada pel president del Comitè esmentat.

7.3. RESPONSABILITATS ASSOCIADES A L'ESQUEMA NACIONAL DE SEGURETAT

A continuació, es detallen i s'estableixen les funcions i les responsabilitats de cadascuna dels rols de seguretat ENS:

Funcions del Responsable de la Informació i dels Serveis

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

Funcions del Responsable de Seguretat

- Mantenir i verificar el nivell adequat de seguretat de la informació manejada i dels serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.

- Designar responsables de l'execució de l'anàlisi de riscos, de la declaració d'aplicabilitat, identificar mesures de seguretat, determinar les configuracions necessàries, elaborar documentació del sistema.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el Responsable del Sistema i/o el Comitè de Seguretat de la Informació de la Informació.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comitè de Seguretat l'aprovació de canvis i altres requisits del sistema.

Funcions del Responsable del Sistema

- Paralitzar o donar suspensió a l'accés a informació o prestació de servei si teniu el coneixement que aquests presenten deficiències greus de seguretat.
- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida.
- Elaborar els procediments operatius necessaris.
- Definir la topologia i la gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en aquest.
- Assegureu-vos que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Prestar al Responsable de Seguretat de la Informació i/o al Comitè de Seguretat assessorament per a la determinació de la categoria del sistema.
- Col·laborar, si així se'l requereix, en l'elaboració i la implantació dels plans de millora de la seguretat i, si s'escau, en els plans de continuïtat.

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

- La gestió, configuració i actualització, si escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat.
- La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la seva correspondència amb allò autoritzat.
- Aprovar els canvis a la configuració vigent del Sistema d'Informació.
- Assegurar que els controls de seguretat establerts són estrictament complerts.
- Assegurar que són aplicats els procediments aprovats per manejar el sistema d'informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.

- Monitoritzar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i els mecanismes d'auditoria tècnica.

Quan la complexitat del sistema ho justifiqui, el Responsable de Sistema podrà designar els responsables de sistema delegats que consideri necessaris, que tindran dependència funcional directa d'aquell i seran responsables en el seu àmbit de totes aquelles accions que els delegue. De la mateixa manera, també podrà delegar en altres funcions concretes de les responsabilitats que se li atribueixen.

7.4 FUNCIONS DEL COMITÈ DE SEGURETAT DE LA INFORMACIÓ

El Comitè de Seguretat tindrà les funcions següents:

- Atendre les sol·licituds, en matèria de Seguretat de la Informació, de l'Administració i dels diferents rols de seguretat i/o àrees informant regularment de l'estat de la Seguretat de la Informació.
- Assessorar en matèria de seguretat de la informació.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre les diferents unitats administratives.
- Promoure la millora contínua del sistema de gestió de la seguretat de la informació. Per això s'encarregarà de:
    - Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que aquests siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
    - Proposar plans de millora de la Seguretat de la Informació, amb la dotació pressupostària corresponent, i prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.
    - Vetllar perquè la Seguretat de la Informació es tingui en compte en tots els projectes des de la seva especificació inicial fins a la posada en operació. En particular haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.
    - Realitzar un seguiment dels principals riscos residuals assumits per l'Administració i recomanar-ne possibles actuacions.
    - Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'aquests.
    - Elaborar i revisar regularment la Política de Seguretat de la Informació per aprovar-la l'òrgan competent.
    - Elaborar la normativa de Seguretat de la Informació per aprovar-la en coordinació amb la Direcció General.
    - Verificar els procediments de seguretat de la informació i la resta de documentació per a la seva aprovació.
    - Elaborar programes de formació destinats a formar i sensibilitzar el personal en matèria de seguretat de la informació i en particular en matèria de protecció de dades de caràcter personal.

- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de Seguretat de la Informació.
- Promoure la realització de les auditories periòdiques ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l'Administració en matèria de seguretat de la Informació.

7.5. PROCEDIMENTS DE DESIGNACIÓ

La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants i la designació dels Responsables identificats en aquesta Política ha estat realitzada per Alcaldia de l'Ajuntament de Paiporta, i comunicada a les parts afectades per notificació electrònica.

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

7.6. RESOLUCIÓ DE CONFLICTES

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

8. DADES DE CARÀCTER PERSONAL

Només es recolliran dades de caràcter personal quan siguin adequades, pertinents i no excessives i aquestes es trobin en relació amb l'àmbit i les finalitats per als quals s'hagin obtingut. De la mateixa manera, adoptarà les mesures d'índole tècnica i organitzatives necessàries per al compliment de la normativa de protecció de dades vigent en cada cas.

A la vista de l'entrada en aplicació, el dia 25 de maig de 2018, del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en allò que respecte al tractament de dades personals ia la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) i la seva translació a la legislació espanyola amb la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, s'han anat adaptant les mesures oportunes com ara l'anàlisi de legitimitat jurídica de cadascuna de les dades tractaments de dades que es duguin a terme, l'anàlisi de riscos , l'avaluació d'impacte si el risc és alt, el registre d'activitats i el nomenament de qui exerceixi les funcions de Delegat de Protecció de Dades.

9. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El Comitè de Seguretat de la Informació ha aprovat el desenvolupament d'un sistema de gestió, que serà establert, implementat, mantingut i millorat, d'acord amb els estàndards de seguretat. Aquest sistema s"adequarà i servirà de gestió dels controls de l"Esquema Nacional de Seguretat. El sistema serà documentat i permetrà generar evidències dels controls i del compliment dels objectius marcats pel Comitè. Hi haurà un procediment de gestió documental que establirà les directrius per a l'estructuració de la documentació de seguretat del sistema, la gestió i l'accés.

Correspon al Comitè de Seguretat de la Informació la revisió anual de la present Política proposant, en cas que calgui millores de la mateixa, per a la seva aprovació per part de la Junta de Govern Local competent per raó de la matèria de l'Ajuntament de Paiporta.

10. TERCERES PARTS

Quan el presta serveis a altres organismes, o manegi informació d'altres organismes, se'ls farà partícip d'aquesta Política de Seguretat de la Informació. L'Ajuntament de Paiporta, definirà i aprovarà els canals per a la coordinació de la informació i els procediments d'actuació per a la reacció davant d'incidents de seguretat, així com la resta de les actuacions que l'Ajuntament de Paiporta, dugui a terme en matèria de Seguretat en relació amb altres organismes.

Quan l'Ajuntament de Paiporta, utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícip d'aquesta Política de Seguretat i de la Normativa de Seguretat existent que afecta aquests serveis o informació. Aquesta tercera part queda subjecta a les obligacions establertes en la normativa esmentada, i poden desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics de comunicació i resolució d'incidències. Es garantirà que el personal de tercers estigui adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que el que estableix aquesta Política de Seguretat. De la mateixa manera, tenint en compte l'obligació de complir el que disposen les instruccions tècniques de seguretat recollides a l'Esquema Nacional de Seguretat en l'àmbit de l'Administració. Hauran d'estar en condicions d'exhibir la corresponent Declaració de Conformitat amb l'Esquema Nacional de Seguretat quan es tracti de sistemes de categoria BÀSICA, o la Certificació de Conformitat amb l'Esquema Nacional de Seguretat, quan es tracti de sistemes de categories MITJANA o ALTA.

Quan algun aspecte d'aquesta Política de Seguretat no pugui ser satisfet per una tercera part segons es requereixi en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat ENS que necessiti 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 endavant.

NOR01 – Política de seguridad de la información

Clasificación de la Información:

Nivel del Documento	Normativa
Nombre del Fichero	NOR01 – Politica de seguridad de la informacion.docx
Tipo	Difusión pública
Ámbito de Difusión	Comité de Seguridad del AYUNTAMIENTO DE PAIPORTA
Responsable	Responsable de Seguridad del AYUNTAMIENTO DE PAIPORTA

CONTROL DE FIRMAS

	FECHA	FIRMA
ELABORADO POR MARIA SANCHIS	22/02/2024	
APROBADO POR JUNTA DE GOBIERNO LOCAL	15/3/2024	

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	26/03/2019	María Sanchis	Versión inicial del documento Aprobación por la 1ª reunión del Comité de Seguridad de la Información.
1.0	06/05/2019	María Sanchis	Primera aprobación por la Junta de Gobierno Local.
1.0	27/11/2019	María Sanchis	Primera publicación en el BOP nº 134.
2.0	04/05/2020	María Sanchis	Actualización de miembros por la 3ª reunión ordinaria del Comité de Seguridad de la Información.
2.0	30/3/2021	María Sanchis	Segunda aprobación por la Junta de Gobierno Local.
2.0	04/05/2021	María Sanchis	Segunda publicación en el BOP nº 83.
3.0	22/02/2024	María Sanchis	Diversas modificaciones: Se elimina el listado de normativa y se mantendrá actualizado un documento externo toda la gestión de requisitos legales. Se elimina como vocal del Comité al Técnico/ Igualdad. Se revisan los roles y las funciones del Comité. Se añaden las funciones del rol Responsable de Información y de Servicios.
3.0	15/03/2024	María Sanchis	Tercera aprobación por la Junta de Gobierno Local.

ÍNDICE DE CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 15 de marzo de 2024 por la Junta de Gobierno Local.

Esta "Política de Seguridad de la Información", en adelante Política, es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

El Ayuntamiento de Paiporta depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de acuerdo al Esquema Nacional de Seguridad.

3. MISIÓN DEL AYUNTAMIENTO DE PAIPORTA

El Ayuntamiento de Paiporta para alcanzar sus objetivos asume su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, con el fin de ofrecer a toda su ciudadanía las mayores garantías en torno a la seguridad de la información utilizada.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados, tanto para los productos que desarrolla y sus servicios asociados, cómo en lo que se refiere al software base adquirido de terceros.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación).

4. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Paiporta, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

5. MARCO NORMATIVO

El marco normativo que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Paiporta, está constituido por normas jurídicas estatales y autonómicas, si procede, orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco, se encuentran recogidas en un registro al efecto, el cual se mantiene actualizado según señala el correspondiente “PRO026 - Procedimiento de gestión de requisitos legales”.

También podrán formar parte del referido marco, aquellas normas aplicables a la Administración Electrónica del Ayuntamiento, que sean desarrollo de las anteriores o estén relacionadas, pudiendo ser adicionalmente publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

6. CUMPLIMIENTO DE ARTÍCULOS

El Ayuntamiento de Paiporta, para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, que recogen los principios básicos y de los requisitos mínimos,

ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral y seguridad por defecto

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Ayuntamiento de Paiporta, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica e integridad y actualización del sistema

El Ayuntamiento de Paiporta, ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal y profesionalidad

Todos los miembros del Ayuntamiento de Paiporta, dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Gestión de la seguridad basada en los riesgos y análisis y gestión de riesgos

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad, prevención, reacción y recuperación

El Ayuntamiento de Paiporta, ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el Ayuntamiento de Paiporta, implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

El Ayuntamiento de Paiporta, establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

- Para garantizar la disponibilidad de los servicios, el Ayuntamiento de Paiporta, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa y prevención ante otros sistemas interconectados

El Ayuntamiento de Paiporta, ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada y organización e implantación del proceso de seguridad

El Ayuntamiento de Paiporta, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos

El Ayuntamiento de Paiporta, ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones

El Ayuntamiento de Paiporta, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos, el Ayuntamiento de Paiporta, tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento de Paiporta, ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de Ayuntamiento de Paiporta. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad

El Ayuntamiento de Paiporta, ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

Calificación de la información

Los criterios de calificación que permitan ajustar los requisitos de seguridad estarán establecidos en el documento “PRO017 – Procedimiento de calificación de la información” que establecerá quién es el responsable de cada información manejada por el sistema.

7. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la Seguridad de la Información en el Ayuntamiento de Paiporta, se establece en la forma que se indica a continuación.

7.1. ROLES O PERFILES DE SEGURIDAD

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Delegado de Protección de Datos (DPD): AUDIDAT 3.0, S.L.U.

- Responsable/s de Información y Servicios: Secretario/a.
- Responsable de Seguridad: Técnico/a informático.
- Responsable del Sistema: Técnico/a auxiliar informático.

7.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Ayuntamiento de Paiporta, ha constituido un Comité de Seguridad de la Información, como órgano colegiado, y está formado por los siguientes miembros:

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN		
UNIDAD	**DELEGADO/A**	**FUNCIÓN**
ALCALDÍA	Alcalde/sa	**Presidente/a**
INNOVACIÓN	Responsable de seguridad	**Secretario/a**
INNOVACIÓN	Responsable de sistemas	Vocal
SECRETARÍA	Secretario/a. Responsable de la Información y Servicios.	Vocal
INNOVACIÓN	Concejal/a.	Vocal
SEGURIDAD CIUDADANA	Intendente de la Policía Local.	Vocal
DELEGADO DE PROTECCIÓN DE DATOS	AUDIDAT 3.0, S.L.U.	Vocal

El Responsable de la Información y de los Servicios será representado por el Secretario/a del Ayuntamiento pudiendo convocar a algún otro Responsable de Área en función de los asuntos a tratar.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias del Ayuntamiento de Paiporta, con periodicidad anual, previa convocatoria al efecto realizada por el Presidente de dicho Comité.

7.3. RESPONSABILIDADES ASOCIADAS AL ESQUEMA NACIONAL DE SEGURIDAD

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta al Responsable de Seguridad ENS, y/o Comité de Seguridad de la Información
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

Llevar a cabo las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

7.4 FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

7.5. PROCEDIMIENTOS DE DESIGNACIÓN

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política ha sido realizada por Alcaldía del Ayuntamiento de Paiporta, y comunicada a las partes afectadas por notificación electrónica.

Los miembros del Comité, así como los roles de seguridad serán revisados cada cuatro años o con ocasión de vacante.

7.6. RESOLUCIÓN DE CONFLICTOS

El Comité de Seguridad de la Información, se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

8. DATOS DE CARÁCTER PERSONAL

Solo se recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento

general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte de la Junta de Gobierno Local competente por razón de la materia del Ayuntamiento de Paiporta.

10. TERCERAS PARTES

Cuando el preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Ayuntamiento de Paiporta, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el Ayuntamiento de Paiporta, lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Ayuntamiento de Paiporta, utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad. De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogidas en el Esquema Nacional de Seguridad en el ámbito de la Administración. Deberán de estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

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

aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.