NOR01 – Política de seguretat de la informació

Classificació de la informació:

Nivell del document	Normativa
Nom del fitxer	NOR01 – Política de seguretat de la informació.docx
Tipus	Difussió pública
Àmbit de difusió	Comité de Seguretat de l'AJUNTAMENT DE PAIPORTA
Responsable	Responsable de seguretat de l'AJUNTAMENT DE PAIPORTA

CONTROL DE MODIFICACIONS		
Descripció	**Versió**	**Data**
Primera aprovació per la Junta de Govern Local	1.0	06/05/2019
Primera publicació en el BOP nº 134	1.0	27/11/2019
Actualització de membres por la 3a reunió ordinària del Comité de Seguretat de la Informació	1.1	04/05/2021
Segona aprovació per la Junta de Govern Local	1.1	30/3/2021
Segona publicació en el BOP nº 83	1.1	4/5/2021

ÍNDEX DE CONTINGUT

1. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 30 de març de 2021 per la Junta de Govern Local.

Aquesta "Política de Seguretat de la Informació", d'ara en avant Política, és efectiva des d'aquesta data i fins que siga reemplaçada per una nova Política.

2. INTRODUCCIÓ

L'Ajuntament de Paiporta 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, actuar preventivament, supervisar l'activitat diària i reaccionar 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. Això implica que els departaments 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.

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

Els departaments han d'estar preparats per a prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'Article 7 de l'Esquema Nacional de Seguretat.

3. PRINCIPIS I DIRECTRIUS

3.1. PREVENCIÓ

L'Ajuntament de Paiporta ha d'evitar, o almenys prevenir en la mesura que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'Esquema Nacional de Seguretat, 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, l'Ajuntament de Paiporta deu:

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

3.2. DETECCIÓ

Atès 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'Esquema Nacional de Seguretat.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'Article 8 de l'Esquema Nacional de Seguretat. S'establiran mecanismes de detecció, anàlisi i reporte que arriben a les persones responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagen preestablit com a normals.

3.3. RESPOSTA

L'Ajuntament de Paiporta deu:

- 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).

3.4. RECUPERACIÓ

Per a garantir la disponibilitat dels serveis crítics, l'Ajuntament de Paiporta ha de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

4. ASSOLIMENT

Aquesta Política s'aplicarà als sistemes d'informació de l'Ajuntament de Paiporta i a totes les persones membres de l'organització, sense excepcions, que estan relacionades amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu i que es troben dins de l'abast de l'Esquema Nacional de Seguretat (ENS). També s'aplica sobre personal en pràctiques i personal extern que puguen participar en els processos municipals de manera directa o indirecta.

La Política de Seguretat és d'obligat compliment i s'estructura en els següents nivells relacionats jeràrquicament:

1. Primer nivell: Política de Seguretat de la Informació.

Constitueix el primer nivell la Política de Seguretat de la Informació, arreplegat en el present text. La Política de Seguretat requereix l'aprovació per part de la Junta de Govern.

2. Segon nivell: Normativa de Seguretat de la Informació.

El segon nivell desenvolupa la Política de Seguretat de la Informació mitjançant instruccions específiques que abasten una àrea o aspecte determinat de la seguretat de la informació. Les instruccions s'estructuraran en normatives i seran aprovades pel Comité de Seguretat de la Informació.

3. Tercer nivell: Procediments de Seguretat de la Informació.

El tercer nivell està constituït per directrius de caràcter tècnic o procedimental que s'han d'observar en tasques o activitats relacionades amb la seguretat de la informació i la protecció de la informació i dels serveis.

Els procediments seran aprovats per la persona responsable de seguretat de la informació o per les persones responsables de la informació o dels serveis, segons el seu àmbit de competència.

Aquesta estructura jeràrquica permetrà a l'Ajuntament de Paiporta adaptar amb eficiència els seus entorns operatius i garantir la seguretat en els seus processos de negoci.

El personal de l'Ajuntament de Paiporta tindrà l'obligació de conèixer i complir, a més de la Política de Seguretat de la Informació, totes les instruccions i procediments de seguretat de la informació que puguen afectar les seues funcions.

La Política, les normatives i els procediments de seguretat de la informació estaran disponibles en la Intranet de l'organització.

5. MISSIÓ

L'Ajuntament de Paiporta és l'Administració Local del municipi de Paiporta (província de València). L'organització té com a missió servir a la seua ciutadania complint el marc de legalitat vigent.

6. MARC NORMATIU

La base normativa que afecta al desenvolupament de les activitats i competències de l'Ajuntament de Paiporta, en el que a administració electrònica es refereix, i que implica la implantació de forma explícita de mesures de seguretat en els sistemes d'informació, està constituïda per la següent legislació:

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, modificat per Reial decret 951/2015, de 23 d'octubre.
- Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat.
- Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció tècnica de seguretat d'informe de l'estat de la seguretat.
- Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció tècnica de seguretat d'auditoria de la seguretat dels sistemes d'informació.
- Resolució de 13 d'abril de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció tècnica de seguretat de notificació d'incidents de seguretat.
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.
- Reial decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades, RGPD).
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.
- Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.
- Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació.
- Llei 9/2014, de 9 de maig, general de telecomunicacions.
- Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, modificada per la Llei 11/1999, de 21 d'abril.
- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual.
- Reial decret legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat públic.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Reial decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.
- Text refós de la Llei de contractes del sector públic, aprovat per Reial decret legislatiu 3/2011, de 14 de novembre, i la seua normativa de desenvolupament.
- Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions.
- Reglament regulador del registre electrònic de l'Ajuntament de Paiporta.
- Reglament orgànic d'utilització de mitjans electrònics de l'Ajuntament de Paiporta.

També formen part del marc normatiu les restants normes aplicables a l'Administració Electrònica de l'Ajuntament de Paiporta, derivades de les anteriors i publicades en les seus electròniques compreses dins de l'àmbit d'aplicació de la present Política.

El manteniment del marc normatiu serà responsabilitat de l'Ajuntament de Paiporta, i es mantindrà en un Annex a aquest document. Inclòs les instruccions tècniques de seguretat d'obligat compliment, publicades mitjançant resolució de la Secretaria d'Estat d'Administracions Públiques i aprovades pel Ministeri d'Hisenda i Administracions Públiques, a proposta del Comité Sectorial d'Administració Electrònica i a iniciativa del Centre Criptològic Nacional (CCN) tal com s'estableix en l' "Article 29. Instruccions tècniques de seguretat i guies de seguretat".

Així mateix, l'Ajuntament de Paiporta, també serà responsable d'identificar les guies de seguretat del CCN, referenciades en l'esmentat article, que seran aplicable per a millorar el compliment del que s'estableix en l'Esquema Nacional de Seguretat.

7. ORGANITZACIÓ DE LA SEGURETAT

7.1. COMITÉ DE SEGURETAT DE LA INFORMACIÓ

7.1.1. CONSTITUCIÓ

El **Comité de Seguretat de la Informació**, d'ara en avant el "Comité", assumeix els **rols de responsable de la informació i responsable del servei.**

El Comité presenta estructura orgànica i està format per delegats i delegades de les parts interessades en l'òptima gestió de la seguretat de la informació. La postura oficial del Comité davant qüestions sotmeses a votació serà delimitada per majoria simple.

Les persones integrants del Comité de Seguretat de la Informació es detallen en la següent taula.

COMITÉ DE SEGURETAT DE LA INFORMACIÓ		
UNITAT	**PERSONA DELEGADA**	**FUNCIÓ**
ALCALDIA	Alcalde/alcaldessa	**President/presidenta**
INNOVACIÓ	Responsable de seguretat	**Secretari/secretària**
INNOVACIÓ	Responsable de sistemas	Vocal
SECRETARIA	Secretari/secretària	Vocal
INNOVACIÓ	Regidor/regidora	Vocal
SEGURETAT CIUTADANA	Intendent de la Policia Local	Vocal
IGUALTAT	Tècnic/tècnica d'Igualtat	Vocal
DELEGAT DE PROTECCIÓ DE DADES	AUDIDAT 3.0, SLU	Vocal

El **secretari o la secretària del Comité** és la persona responsable de seguretat i té com a funcions del càrrec:

- Convocar les reunions del Comité.
- Preparar els temes a tractar en les reunions del Comité, aportant informació puntual per a la presa de decisions.
- Elaborar l'acta de reunió.
- Impulsar l'execució directa o delegada de les decisions del Comité.

El p**resident o la presidenta del Comité** és l'alcalde-president o alcaldessa-presidenta de l'Ajuntament de Paiporta i és responsable de presidir les reunions. Així mateix, serà responsable de revisar les actes derReunió i aprovar-les formalment amb la seua signatura.

7.1.2. FUNCIONS i RESPONSABILITATS

El **Comité de Seguretat de la Informació** reportarà a la Junta de Govern les seues propostes i decisions en aquelles àrees que li competeixen. El Comité tindrà les següents funcions:

- 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'Organització pel que fa a 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 Junta de Govern.
- Aprovar la normativa de seguretat de la informació.
- Elaborar i aprovar els requisits de formació i qualificació de persones administradores, operadores i usuàries des del punt de vista de seguretat de la informació.
- Monitorar els principals riscos residuals assumits per l'organització 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'organització. En particular vetlarà per la coordinació de diferents plans que puguen realitzar-se en diferents àrees.
- Prioritzar les actuacions en matèria de seguretat quan els recursos siguen limitats.
- Vetlar perquè la seguretat de la informació es té en compte en tots els projectes TIC des de la seua especificació inicial fins a la seua posada en operació. En particular haurà de vetlar per la creació i utilització de serveis horitzontals que reduïsquen duplicitats i donen suport a un funcionament homogeni de tots els sistemes TIC.
- Resoldre els conflictes de responsabilitat que puguen aparèixer entre les diferents persones responsables i/o entre diferents àrees de l'organització, elevant aquells casos en els quals no tinga suficient autoritat per a decidir.

7.2. ROLS

7.2.1. ESTRUCTURA

A l'Ajuntament de Paiporta els rols de l'Esquema Nacional de Seguretat s'assignen de la següent forma:

FIGURA RESPONSABLE	ROL	FUNCIONS I RESPONSABILITATS
COMITÉ DE SEGURETAT DE LA INFORMACIÓ	Responsable de la informació	Tractament/protecció de la informació
	Responsable del servei	Definir requisits de seguretat dels serveis
RESPONSABLE DE SEGURETAT	Responsable de la seguretat	Responsable del compliment ENS
ADMINISTRADOR/ ADMINISTRADORA DEL SISTEMA	Responsable del sistema	Manteniment i continuitat dels sistemes
	Administrador/administradora de la seguretat	Aplicació de mesures de seguretat

Els rols nominatius de l'Esquema Nacional de Seguretat són exercits pel següent personal:

FIGURA RESPONSABLE	NOMENAMENT	CONTACTE
Responsable de seguretat	María Sanchis Valero	ens@paiporta.es
Administrador del sistema	Rafael Tortosa Vila	ens@paiporta.es

Relatiu al compliment de la normativa en protecció de dades, es realitza la designació de la figura de delegat de protecció de dades que col·laborarà activament en el Comité de Seguretat de la Informació.

FIGURA RESPONSABLE	NOMENAMENT	CONTACTE
Delegat de protecció de dades	Francisco Ricardo Gómez Sancho (AUDIDAT 3.0, S.L.U.)	fgomez@audidat.com

7.2.2. FUNCIONS I RESPONSABILITATS

La figura de **responsable de Seguretat** té com a principals funcions i responsabilitats:

- Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes TIC en el seu àmbit de responsabilitat.
- Realitzar o promoure les auditories periòdiques que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.

- Promoure la formació i conscienciació de la Unitat d'Informàtica dins del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establides són adequades per a la protecció de la informació manejada i els serveis prestats.
- Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat del sistema.
- Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria implementats en el sistema.
- Donar suport i supervisar la investigació dels incidents de seguretat des de la seua notificació fins a la seua resolució.
- Elaborar l'informe periòdic de seguretat per al propietari del sistema, incloent els incidents més rellevants del període.
- Aprovació dels procediments de seguretat elaborats per la persona administradora del sistema.
- Elaboració de la normativa de seguretat de l'entitat.

Per part seua, **la persona administradora del Sistema** tindrà com a principals funcions i responsabilitats:

- Desenvolupar, operar i mantenir el Sistema durant tot el seu cicle de vida, incloent les especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i els procediments de gestió del Sistema i establir els criteris d'ús i els serveis disponibles en aquest.
- Definir la política de connexió o desconnexió d'equips i usuaris nous en el Sistema.
- Aprovar els canvis que afecten la seguretat de la manera d'operació del Sistema.
- Decidir les mesures de seguretat que aplicaran els subministradors de components del Sistema durant les etapes de desenvolupament, instal·lació i prova d'aquest.
- Implantar i controlar les mesures específiques de seguretat del Sistema i cerciorar-se que aquestes s'integren adequadament dins del marc general de seguretat.
- Determinar la configuració autoritzada de maquinari i programari a utilitzar en el Sistema.
- Aprovar tota modificació substancial de la configuració de qualsevol element del Sistema.
- Dur a terme el preceptiu procés d'anàlisi i gestió de riscos en el Sistema.
- Determinar la categoria del sistema segons el procediment descrit en l'Annex I de l'ENS i determinar les mesures de seguretat que han d'aplicar-se segons es descriu en l'Annex II de l'ENS.
- Elaborar la documentació de seguretat del Sistema.
- Delimitar les responsabilitats de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del Sistema.
- Investigar els incidents de seguretat que afecten el Sistema, i si escau, comunicació a la persona responsable de Seguretat o a qui aquest determine.
- Establir plans de contingència i emergència, duent a terme freqüents exercicis perquè el personal es familiaritze amb ells.
- Detenir el 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 les persones responsables de la informació afectada, del servei afectat i la persona responsable de Seguretat, abans de ser executada.

- Elaboració dels procediments de seguretat necessaris per a l'operativa en el sistema.

Les funcions i les responsabilitats llistades en aquest apartat podran ser delegades tal com estipula la Guia d'Adequació 801 sobre Responsabilitats i Funcions en l'Esquema Nacional de Seguretat.

7.3. PROCEDIMENTS DE DESIGNACIÓ

La persona responsable de Seguretat de la Informació serà nomenada per la Junta de Govern a proposta del Comité de Seguretat de la Informació. El nomenament es revisarà cada 2 anys o quan el lloc quede vacant.
El departament responsable d'un servei que es preste electrònicament designarà la perona responsable del Sistema, i precisarà les seues funcions i responsabilitats dins del marc establit per aquesta Política.
Cada àrea proposarà cada dos anys al seu delegat o delegada en el Comité de Seguretat de la Informació, que serà triat per consens entre els membres de l'àrea. Les persones representants nomenaran al president o presidenta del Comité, mentre que la figura de secretari o secretària correspondrà a la persona responsable de la Seguretat de l'Esquema Nacional de Seguretat.

7.4. POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Serà missió del Comité de Seguretat de la Informació la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment d'aquesta. La Política serà aprovada per la Junta de Govern i difosa perquè la coneguen totes les parts afectades.

8. DADES DE CARÀCTER PERSONAL

L'Ajuntament de Paiporta tracta dades de caràcter personal. El document **"Registre d'activitats de tractament"** arreplega els fitxers afectats, les persones responsables corresponents i les activitats de tractament realitzades. Només arreplegarà dades de caràcter personal quan siguen adequats, pertinents i no excessius i aquests es troben en relació amb l'àmbit i les finalitats per als quals s'hagen obtingut. D'igual manera, adoptarà les mesures d'índole tècnica i organitzatives necessàries per al compliment de la normativa de Protecció de Dades vigent en cada cas.
Tots els sistemes d'informació de l'Ajuntament de Paiporta 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 de Tractament".
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 pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) i la seua 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 tals com, l'anàlisi de legitimitat jurídica de cadascuna de les dades i tractaments de dades que es duguen a terme, l'anàlisi de riscos, l'avaluació d'impacte si el risc és alt, el registre d'activitats i el nomenament de qui vaja a exercir les funcions de delegat o delegada de Protecció de Dades.

9. GESTIÓ DE RISCOS

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

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

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

10. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta Política de Seguretat de la Informació complementa les polítiques de seguretat de l'Ajuntament de Paiporta aplicades en matèria de protecció de dades de caràcter personal.

El Comité de Seguretat de la Informació de l'Ajuntament de Paiporta ha aprovat el desenvolupament d'un sistema de gestió, que serà establit, implementat, mantingut i millorat, conforme als 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 Comité. Existirà un procediment de gestió documental que establirà les directrius per a l'estructuració de la documentació de seguretat del sistema, la seua gestió i accés.

Aquesta Política es desenvoluparà per mitjà de la Normativa de Seguretat que afronte aspectes específics. La Normativa de Seguretat estarà a la disposició de tots els membres de l'organització que necessiten conèixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.
Correspon al Comité de Seguretat de la Informació la revisió anual de la present Política proposant, en cas que siga necessari, millores d'aquesta per a la seua aprovació per part de la Junta de Govern Local competent per raó de la matèria de l'Ajuntament de Paiporta.

La normativa de seguretat estarà disponible en la Intranet i en format imprès en l'àrea d'Innovació.

11. OBLIGACIONS DEL PERSONAL

Tots els membres de l'Ajuntament de Paiporta tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribe a les persones afectades.

Tots els membres de l'Ajuntament de Paiporta atendran una sessió de conscienciació en matèria de seguretat TIC almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per a atendre a tots els membres, 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.

12. TERCERES PARTS

Quan l'Ajuntament de Paiporta preste serveis a altres organismes o manege informació d'altres organismes, se'ls farà partícips 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 incidents de seguretat, així com la resta d'actuacions que l'Ajuntament de Paiporta duga a terme en matèria de seguretat en relació amb altres organismes.

Quan l'Ajuntament de Paiporta utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícip d'aquesta Política de Seguretat i de la Normativa de Seguretat existent 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'establit en aquesta Política.

Quan algun aspecte de la Política no puga ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe a ell o a la responsable de Seguretat que precise els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe per les persones responsables de la informació i els serveis afectats abans de seguir avant.

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 MODIFICACIONES		
Descripción	**Versión**	**Fecha**
Primera aprobación por la Junta de Gobierno Local.	1.0	06/05/2019
Primera publicación en el BOP nº 134.	1.0	27/11/2019
Actualización de miembros por la 3ª reunión ordinaria del Comité de Seguridad de la Información.	1.1	04/05/2021
Segunda aprobación por la Junta de Gobierno Local.	1.1	30/3/2021
Segunda publicación en el BOP nº 83.	1.1	04/05/2021

ÍNDICE DE CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 30 de marzo de 2021<día> de <mes> de <año> 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 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 Artículo 7 del Esquema Nacional de Seguridad.

3. PRINCIPIOS Y DIRECTRICES

3.1. PREVENCIÓN

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

Para garantizar el cumplimiento de la política, el Ayuntamiento de Paiporta debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

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

3.2. DETECCIÓN

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

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

3.3. RESPUESTA

El Ayuntamiento de Paiporta debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar 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).

3.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, el Ayuntamiento de Paiporta debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Paiporta y a todas las personas miembros de la organización, sin excepciones, 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). También se aplica sobre personal en prácticas y personal externo que puedan participar en los procesos municipales de manera directa o indirecta.

La Política de Seguridad es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

1. Primer nivel: Política de Seguridad de la Información.

Constituye el primer nivel la Política de Seguridad de la Información, recogido en el presente texto. La Política de Seguridad requiere la aprobación por parte de la Junta de Gobierno.

2. Segundo nivel: Normativa de Seguridad de la Información.

El segundo nivel desarrolla la Política de Seguridad de la Información mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de la información. Las Instrucciones se estructurarán en normativas y serán aprobadas por el Comité de Seguridad de la Información.

3. Tercer nivel: Procedimientos de Seguridad de la Información.

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios.

Los procedimientos serán aprobados por el Responsable de Seguridad de la Información o por los y las Responsables de la Información o los de los Servicios, según su ámbito de competencia.

Esta estructura jerárquica permitirá al Ayuntamiento de Paiporta adaptar con eficiencia sus entornos operativos y garantizar la seguridad en sus procesos de negocio.

El personal del Ayuntamiento de Paiporta tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Normativas y los Procedimientos de Seguridad de la información estarán disponibles en la Intranet de la organización.

5. MISIÓN

El Ayuntamiento de Paiporta es la Administración Local del municipio de Paiporta (Provincia de Valencia). La organización tiene como misión servir a su ciudadanía cumpliendo el marco de legalidad vigente.

6. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Paiporta, en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado por Real Decreto 951/2015, de 23 de octubre.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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, RGPD).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, y su normativa de desarrollo.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Reglamento regulador del registro electrónico del Ayuntamiento de Paiporta.
- Reglamento orgánico de utilización de medios electrónicos del Ayuntamiento de Paiporta.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de Paiporta, derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad del Ayuntamiento de Paiporta, y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el "Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad".

Así mismo, el Ayuntamiento de Paiporta, también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

7.1.1. CONSTITUCIÓN

El **Comité de Seguridad de la Información**, en adelante el "Comité", asume los **roles de Responsable de la Información y Responsable del Servicio.**

El Comité presenta estructura orgánica y está formado por delegados y delegadas de las partes interesadas en la óptima gestión de la Seguridad de la Información. La postura oficial del Comité ante cuestiones sometidas a votación será delimitada por mayoría simple.

Los y las integrantes del Comité de Seguridad de la Información se detallan en la siguiente tabla.

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	Vocal
SEGURIDAD CIUDADANA	Intendente de la Policía Local	Vocal
IGUALDAD	Técnico/a de Igualdad	Vocal
DELEGADO DE PROTECCIÓN DE DATOS	AUDIDAT 3.0, S.L.U.	Vocal

El/la **Secretario/a del Comité** es el/la Responsable de Seguridad y tiene como funciones del cargo:

- Convocar las reuniones del Comité.

- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el Acta de Reunión.
- Impulsar la ejecución directa o delegada de las decisiones del Comité.

El/la **Presidente/a del Comité** es el/la Alcalde/sa-Presidente/a del Ayuntamiento de Paiporta y es responsable de presidir las reuniones. Así mismo, será responsable de revisar las Actas de Reunión y aprobarlas formalmente con su firma.

7.1.2. FUNCIONES Y RESPONSABILIDADES

El **Comité de Seguridad de la Información** reportará a la Junta de Gobierno sus propuestas y decisiones en aquellas áreas que le competen. El Comité tendrá las siguientes funciones:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Junta de Gobierno.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores/as, operadores/as y usuarios/as desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar 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 TIC 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los y las diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

7.2. ROLES

7.2.1. ESTRUCTURA

En el Ayuntamiento de Paiporta los roles del Esquema Nacional de Seguridad se asignan de la siguiente forma:

FIGURA RESPONSABLE	ROL	FUNCIONES Y RESPONSABILIDADES
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Responsable de la información	Tratamiento / Protección de la información
	Responsable del servicio	Definir requisitos de seguridad de los servicios
RESPONSABLE DE SEGURIDAD	Responsable de la Seguridad	Responsable del Cumplimiento ENS
ADMINISTRADOR/A DEL SISTEMA	Responsable del sistema	Mantenimiento y continuidad de los Sistemas
	Administrador/a de la Seguridad	Aplicación de medidas de Seguridad

Los roles nominativos del Esquema Nacional de Seguridad son ejercidos por el siguiente personal:

FIGURA RESPONSABLE	NOMBRAMIENTO	CONTACTO
Responsable de Seguridad	María Sanchis Valero	ens@paiporta.es
Administrador/a del Sistema	Rafael Tortosa Vila	ens@paiporta.es

Relativo al Cumplimiento de la normativa en Protección de Datos, se realiza la designación de la figura de Delegado de Protección de Datos que colaborará activamente en el Comité de Seguridad de la Información.

FIGURA RESPONSABLE	NOMBRAMIENTO	CONTACTO
Delegado de Protección de Datos	Francisco Ricardo Gómez Sancho (AUDIDAT 3.0, S.L.U.)	fgomez@audidat.com

7.2.2. FUNCIONES Y RESPONSABILIDADES

La figura de **Responsable de Seguridad** tiene como principales funciones y responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.

- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación de la Unidad de Informática dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario del sistema, incluyendo los incidentes más relevantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por el Administrador del Sistema.
- Elaboración de la normativa de seguridad de la entidad.

Por su parte, el **Administrador/a del Sistema** tendrá como principales funciones y responsabilidades:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

- Detener el manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los y las responsables de la información afectada, del servicio afectado y el o la Responsable de Seguridad, antes de ser ejecutada.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.

Las funciones y responsabilidades listadas en este apartado podrán ser delegadas tal como estipula la Guía de Adecuación 801 sobre Responsabilidades y Funciones en el Esquema Nacional de Seguridad.

7.3. PROCEDIMIENTOS DE DESIGNACIÓN

El/la Responsable de Seguridad de la Información será nombrado/a por la Junta de Gobierno a propuesta del Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente designará al/la Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

Cada Área propondrá cada dos años a su delegado/a en el Comité de Seguridad de la Información, que será elegido por consenso entre los miembros del Área. Los representantes nombrarán al Presidente/a del Comité, mientras que la figura de Secretario/a corresponderá a la persona Responsable de la Seguridad del Esquema Nacional de Seguridad.

7.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Junta de Gobierno y difundida para que la conozcan todas las partes afectadas.

8. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Paiporta trata datos de carácter personal. El documento "**Registro de Actividades de Tratamiento**" recoge los ficheros afectados, los/ las responsables correspondientes y las actividades de tratamiento realizadas. Solo 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.

Todos los sistemas de información del Ayuntamiento de Paiporta se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado "Registro de Actividades de Tratamiento".

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. GESTIÓN DE RIESGOS

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

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

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad del Ayuntamiento de Paiporta aplicadas en materia de Protección de Datos de Carácter Personal.

El Comité de Seguridad de la Información del Ayuntamiento de Paiporta 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.

Esta Política se desarrollará por medio de Normativa de Seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

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.

La Normativa de Seguridad estará disponible en la Intranet y en formato impreso en el Área de Innovación.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento de Paiporta tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados o afectadas.

Todos los miembros de Ayuntamiento de Paiporta atenderán a una sesión de concienciación en materia de seguridad TIC 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.

12. TERCERAS PARTES

Cuando el Ayuntamiento de Paiporta preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes 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 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 dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe a él o la Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los y las responsables de la información y los servicios afectados antes de seguir adelante.