AJUNTAMENT
DE RIUDOMS

POLÍTICA DE SEGURETAT I LA INFORMACIÓ

1. INTRODUCCIÓ 2
2. MISSIÓ DE L'AJUNTAMEMT 2
3. ABAST 2
4. MARC NORMATIU 3
5. COMPLIMENT DELS REQUISITS MÍNIMS DE SEGURETAT 5
6. MODEL DE GOVERNANÇA 10
6.1 PROCEDIMENTS DE DESIGNACIÓ I FUNCIONS DE SEGURETAT 10
6.2 RESPONSABILITATS ASSOCIADES A L'ESQUEMA NACIONAL DE SEGURETAT 11
6.3 FUNCIONS DEL COMITÉ DE SEGURETAT DE LA INFORMACIÓ 12
6.4 RESOLUCIÓ DE CONFLICTES 13
7. DADES DE CARÀCTER PERSONAL 13
8. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ 13
9. TERCERES PARTS 13
10. APROVACIÓ I ENTRADA EN VIGOR .....

INTRODUCCIÓ

L'Ajuntament depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per aconseguir els seus objectius, exercir les seves competències i prestar els serveis que té atribuïts. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los enfront 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 confidencialitat, integritat, autenticitat i traçabilitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb rapidesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir a 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'adapti 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 (ENS), així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per 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 seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i la valoració del seu cost, 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.

MISSIÓ DE L'AJUNTAMENT

L'Ajuntament, per a la gestió dels seus interessos i de les funcions i competències que té atribuïdes en diferents normes o convenis, promou activitats i presta serveis públics que contribueixen a satisfer les necessitats i aspiracions de la població. Per això posa a disposició d'aquesta la realització de tràmits en línia amb l'objectiu d'impulsar la tramitació electrònica dels procediments administratius, la millora en la prestació dels serveis i la participació de la ciutadania en els assumptes públics establint, d'aquesta manera, noves vies de participació que garanteixin el desenvolupament de la democràcia participativa i la millora de l'eficàcia i eficiència de l'acció pública.

Es desitja potenciar d'altra banda l'ús de les noves tecnologies a l'Ajuntament i en la pròpia ciutadania. Els principals objectius que es persegueixen entre altres són: fomentar la relació electrònica de la ciutadania amb l'Ajuntament, crear la confiança necessària entre ciutadà i Ajuntament en aquesta relació.

ABAST

Aquesta Política s'aplicarà als sistemes d'informació de l'Ajuntament, 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 al procediment administratiu i que es troben dins de l'àmbit d'aplicació de l'ENS.

MARC NORMATIU

La base normativa que afecta el desenvolupament de les activitats i competències de l'Ajuntament, en el que a administració electrònica es refereix, i que implica la implantació de manera explícita de mesures de seguretat en els sistemes d'informació, 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 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional 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.
- 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.
- 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 36/2015, de 28 de setembre, de Seguretat Nacional.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- El Reglament (UE) Núm. 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014 (enllaç a https://www.boe.es/doue/2014/257/l00073-00114.pdf), relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE (reglament eIDAS).
- Reial decret 1308/1992, de 23 d'octubre, pel qual es declara al Laboratori del Real Institut i Observatori de l'Armada, com a Laboratori dipositari del patró nacional de Temps i Laboratori associat al Centre Espanyol de Metrologia.
- 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 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic
- Reial decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.
- 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.
- Reial decret 1494/2007, de 12 de novembre, pel qual s'aprova el Reglament sobre les condicions bàsiques per a l'accés de les persones amb discapacitat a les tecnologies, productes i serveis relacionats amb la societat de la informació i mitjans de comunicació social.
- Reial decret 1495/2011, de 24 d'octubre, pel qual es desenvolupa la Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic, per a l'àmbit del sector públic estatal.
- Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
- Llei 25/2013, de 27 de desembre, d'Impuls de la factura electrònica i creació del Registre electrònic de factures en el sector públic.
- Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local, modificada per la llei 11/1999, de 21 d'abril.
- Llei 16/1985, de 25 de juny, del Patrimoni Històric Espanyol (arxiu).
- 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 9/2017, de 8 de novembre, de Contractes del Sector Públic, per la qual es transposen a l'ordenament jurídic espanyol les Directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.
- Llei 9/2014, de 9 de maig, General de Telecomunicacions (Vigent en els apartats assenyalats en la Disposició Derogatòria Única de la Llei 11/2022, de 28 de juny).
- Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- Llei 11/2022, de 28 de juny, General de Telecomunicacions (segons terminis entrada en vigor de Disposició d'aquesta Llei).
- Normes tècniques d'interoperabilitat (NTI), de desenvolupament de l'Esquema Nacional d'Interoperabilitat les quals són de compliment obligatori per a les Administracions públiques.
- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya.
- Llei 18/2020, de 28 de desembre, de facilitació de l'activitat econòmica.
- Acord de 27 de novembre de 2007, sobre l'impuls de la interoperabilitat a la Generalitat de Catalunya.
- Acord GOV/92/2015, de 16 de juny, pel qual s'aprova el sistema d'identificació electrònica idCAT-SMS i l'ús del Validador de credencials d'identitat (VALid).
- Acord 1/2010, de 17 de juny, de la Comissió Nacional, d'Accés, Avaluació i Tria Documental sobre les condicions de substitució de documents en suports físics per còpies electròniques de documents amb validesa d'originals.

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

El manteniment del marc normatiu serà responsabilitat de l'Ajuntament, i es mantindrà en un Annex a aquest document. Incloses 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 Comitè Sectorial d'Administració Electrònica i a iniciativa del Centre Cristològic Nacional (CCN) tal com s'estableix en el Reial decret.

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

COMPLIMENT DELS REQUISITS MÍNIMS DE SEGURETAT

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

La seguretat com un procés integral i mínim privilegi.

La seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials, jurídics i organitzatius, relacionats amb el sistema. L'aplicació de l'ENS a l'Ajuntament 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, per a evitar que, la ignorància, la falta d'organització i coordinació, o d'instruccions inadequades, constitueixin fonts de risc per a la seguretat.

Els sistemes d'informació han de dissenyar-se i configurar-se atorgant els mínims privilegis necessaris per al seu correcte acompliment, la qual cosa implica incorporar els següents aspectes:

a) El sistema proporcionarà la funcionalitat imprescindible perquè l'organització aconsegueixi els seus objectius competencials o contractuals.

b) Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'assegurarà que només siguin desenvolupades per les persones autoritzades, ja sigui des d'emplaçaments o equips autoritzats; podent-se exigir, en el seu cas, 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 siguin innecessàries o inadequades per a la finalitat que es persegueix. L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi d'un acte conscient per part de l'usuari.

d) S'aplicaran guies de configuració de seguretat per a les diferents tecnologies, adaptades a la categorització del sistema, a aquest efecte d'eliminar o desactivar les funcions que siguin innecessàries o inadequades.

Vigilància contínua, re-avaluació periòdica i Integritat, actualització del sistema i millora contínua del procés de seguretat.

La vigilància contínua per part de l'Ajuntament permetrà la detecció d'activitats o comportaments anòmals i la seva oportuna resposta.

L'avaluació permanent de l'estat de la seguretat dels actius permetrà mesurar la seva evolució, detectant vulnerabilitats i identificant deficiències de configuració.

Les mesures de seguretat es re-avaluaran i actualitzaran periòdicament, adequant la seva eficàcia a l'evolució dels riscos i els sistemes de protecció, podent arribar a un replantejament de la seguretat, si fos necessari.

La inclusió de qualsevol element físic o lògic en el catàleg actualitzat d'actius del sistema, o la seva modificació, requerirà autorització formal prèvia.

L'avaluació i monitoratge permanents permetran adequar l'estat de seguretat dels sistemes ateses les deficiències de configuració, les vulnerabilitats identificades i les actualitzacions que els afectin, així com la detecció precoç de qualsevol incident que tingui lloc sobre els mateixos.

El procés integral de seguretat implantat haurà de ser actualitzat i millorat de manera contínua. Per a això, s'aplicaran els criteris i mètodes reconeguts en la pràctica nacional i internacional relatius a la gestió de la seguretat de les tecnologies de la informació.

Gestió de personal i professionalitat.

Tot el personal, propi o aliè relacionat amb els sistemes d'informació de l'Ajuntament, dins de l'àmbit de l'ENS, seran formats i informats dels seus deures, obligacions i responsabilitats en matèria de seguretat. La seva actuació serà supervisada per a verificar que se segueixen els procediments establerts.

El significat i abast de l'ús segur del sistema es concretarà i plasmarà en unes normes de seguretat que seran aprovades per la direcció o l'òrgan superior corresponent. D'igual manera, es determinaran els requisits de formació i experiència necessària del personal per al desenvolupament del seu lloc de treball.

La seguretat dels sistemes d'informació estarà atesa i serà revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del seu cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament.

De manera objectiva i no discriminatòria s'exigirà que les organitzacions que proporcionin serveis comptin amb professionals qualificats i amb uns nivells idonis de gestió i maduresa dels serveis prestats.

Gestió de la seguretat basada en els riscos, anàlisis i gestió de riscos L'anàlisi i la gestió dels riscos serà part essencial del procés de seguretat i serà una activitat contínua i permanentment actualitzada.

La gestió dels riscos permetrà el manteniment d'un entorn controlat, minimitzant els riscos a nivells acceptables. La reducció a aquests nivells es realitzarà mitjançant una apropiada aplicació de mesures de seguretat, de manera equilibrada i proporcionada a la naturalesa de la informació tractada, dels serveis a prestar i dels riscos als quals estiguin exposats.

Aquesta gestió es realitzarà per mitjà de l'anàlisi i tractament dels riscos als quals està exposat el sistema. Sense perjudici del que es disposa en l'annex II, s'emprarà alguna metodologia reconeguda internacionalment. Les mesures adoptades per a mitigar o suprimir els riscos hauran d'estar justificades i, en tot cas, existirà una proporcionalitat entre elles i els riscos.

Incidents de seguretat, prevenció, detecció, reacció i recuperació.

L'Ajuntament disposa de procediments de gestió d'incidents de seguretat d'acord amb el que es preveu en l'article 33, la Instrucció Tècnica de Seguretat corresponent, i de mecanismes de detecció, criteris de classificació, procediments d'anàlisis i resolució, així com de les vies de comunicació a les parts interessades.

La seguretat del sistema contemplarà les accions relatives als aspectes de prevenció, detecció i resposta, a fi de minimitzar les seves vulnerabilitats i aconseguir que les amenaces sobre el mateix no es materialitzin o que, en el cas de fer-lo, no afectin greument la informació que tracta o als serveis que presta.

Les mesures de prevenció podran incorporar components orientats a la dissuasió o a la reducció de la superfície d'exposició, han d'eliminar o reduir la possibilitat de que les amenaces s'arribin a materialitzar.

Les mesures de detecció aniran adreçades a descobrir la presència d'un ciber incident.

Les mesures de resposta es gestionaran en temps oportú, estaran orientades a la restauració de la informació i els serveis que poguessin haver-se vist afectats per un incident de seguretat.

El sistema d'informació garantirà la conservació de les dades i informació en suport electrònic.

D'igual manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital, a través d'una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

Existència de línies de defensa i prevenció davant altres sistemes d'informació interconnectats.

L'Ajuntament ha implementat una estratègia de protecció del sistema d'informació constituïda per múltiples capes de seguretat, constituïdes per mesures organitzatives, físiques i lògiques, de tal forma que quan una capa ha estat

compromesa permeti desenvolupar una reacció adequada enfront dels incidents que no han pogut evitar-se, reduint la probabilitat que el sistema sigui compromès en el seu conjunt i minimitzar l'impacte final sobre aquest.

Es protegirà el perímetre del sistema d'informació, especialment, quan el sistema de l'Ajuntament es connecta a xarxes públiques, tal com es defineixen en la legislació vigent en matèria de telecomunicacions, reforçant-se les tasques de prevenció, detecció i resposta a incidents de seguretat.

En tot cas, s'analitzaran els riscos derivats de la interconnexió del sistema amb altres sistemes i es controlarà el seu punt d'unió. Per a l'adequada interconnexió entre sistemes s'estarà al que es disposa en la Instrucció Tècnica de Seguretat corresponent.

Diferenciació de responsabilitats, organització i implantació del procés de seguretat.

L'Ajuntament 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 en l'apartat de "MODEL DE GOVERNANÇA" del present document.

Autorització i control dels accessos.

L'Ajuntament ha implementat mecanismes de control d'accés al sistema d'informació, limitant-lo als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats, i exclusivament a les funcions permeses.

Protecció de les instal·lacions.

L'Ajuntament ha implementat mecanismes de control d'accés físic, prevenint 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 o contractació de serveis de seguretat l'Ajuntament tindrà en compte la utilització de forma proporcionada a la categoria del sistema i el nivell de seguretat determinat, aquells que tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició.

Per a la contractació de serveis de seguretat s'atendrà a l'assenyalat quant a la professionalitat.

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

L'Ajuntament prestarà especial atenció a la informació emmagatzemada o en trànsit a través dels equips o dispositius portàtils o mòbils, els dispositius perifèrics, els suports d'informació i les comunicacions sobre xarxes obertes, que hauran d'analitzar-se especialment per a aconseguir una adequada protecció.

S'aplicaran procediments que garanteixin la recuperació i conservació a llarg termini dels documents electrònics produïts pels sistemes d'informació compresos en l'àmbit d'aplicació d'aquest reial decret, quan això sigui exigible.

Tota informació en suport no electrònic que hagi estat causa o conseqüència directa de la informació electrònica a la qual es refereix aquest reial decret, haurà d'estar protegida amb el mateix grau de seguretat que aquesta. Per a això, s'aplicaran les mesures que corresponguin a la naturalesa del suport, de conformitat amb les normes que resultin d'aplicació.

Els sistemes disposaran de còpies de seguretat i s'establiran els mecanismes necessaris per a garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals.

Registre d'activitat i detecció de codi nociu

L'Ajuntament amb el propòsit de satisfer l'objecte d'aquest reial decret, amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a 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 resultin d'aplicació, registrarà les activitats dels usuaris, retenint la informació estrictament necessària per a monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar a cada moment a la persona que actua.

A fi de preservar la seguretat dels sistemes d'informació, garantint la rigorosa observança dels principis d'actuació de les Administracions públiques, i de conformitat amb el que es disposa en el Reglament General de Protecció de Dades i el respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació allí enunciats, l'Ajuntament podrà, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, i únicament per als fins de seguretat de la informació, de manera que sigui possible impedir l'accés no autoritzat a les xarxes i sistemes d'informació, detenir els atacs de denegació de servei, evitar la distribució malintencionada de codi nociu així com altres danys a les avantdites xarxes i sistemes d'informació.

Per a corregir o, en el seu cas, exigir responsabilitats, cada usuari que accedeixi al sistema d'informació haurà d'estar identificat de manera única, de manera que se sàpiga, en tot moment, qui rep drets d'accés, de quin tipus són aquests, i qui ha realitzat una determinada activitat.

Infraestructures i serveis comuns

L'Ajuntament tindrà en compte que la utilització d'infraestructures i serveis comuns de les administracions públiques, inclosos els compartits o transversals, facilitarà el compliment del que es disposa en aquest reial decret.

Perfils de compliment específics i acreditació d'entitats d'implementació de configuracions segures.

L'Ajuntament tindrà en compte l'aplicació d'aquells perfils de compliment específics per a Entitats Locals que siguin aplicable.

MODEL DE GOVERNANÇA

Per a garantir el compliment de l'Esquema Nacional de Seguretat i establir l'organització de la seguretat de la informació adaptada a les necessitats i particularitat d'aquest Ajuntament, es proposa una designació de rols per blocs de responsabilitat: Govern, Supervisió i Operació.

D'acord amb aquesta estructura, s'han assignat les següents responsabilitats i funcions de seguretat:

Bloc de Govern:

- **Responsable de Govern**, les funcions del qual exercita l'Alcaldia-Presidència de l'Ajuntament, que integra els següents rols i funcions ENS:
    - Comitè de Seguretat de la Informació.
    - Responsable de la Informació.
    - Responsable del Servei.

- L'Alcaldia-Presidència pot delegar aquests rols i/o funcions en un Regidor o Regidors.

Bloc Executiu/Supervisió:

- **Responsable de Supervisió**, les funcions de la qual exercita la Secretaria-Intervenció de l'Ajuntament, i que integra el següent rol ENS:
    - Responsable de la Seguretat.

- **Delegat Protecció de Dades (DPD)** fent costat al Responsable de Supervisió, amb funcions d'assessorament i supervisió en matèria de protecció de dades.

Bloc d'Operació:

- **Responsable d'Operació**, les competències de la qual exercita un empleat municipal, personal extern o bé el Tècnic del Consell Comarcal i que integra el següent rol ENS:

    - Responsable del Sistema.

PROCEDIMENTS DE DESIGNACIÓ I FUNCIONS DE SEGURETAT

La designació dels Responsables identificats en aquesta Política serà mitjançant Decret d'Alcaldia, quin contindrà el detall de les funcions de seguretat i responsabilitats assignades a cada rol.

Els rols de seguretat seran revisats cada quatre anys, en el cas que existeixi una vacant la mateixa haurà de ser coberta en el termini d'un mes, seguint el mateix procediment.

RESPONSABILITATS ASSOCIADES A L'ESQUEMA NACIONAL DE SEGURETAT

A continuació, es detallen i s'estableixen les funcions i responsabilitats de cadascun 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 del marc establert en l'annex I del Reial decret de l'Esquema Nacional de Seguretat.
- Acceptar els nivells de risc residual que afectin el Servei i a 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 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.
- Participar en l'elaboració i 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 a la Direcció 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 té 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.
- Cerciorar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Prestar al Responsable de Seguretat de la Informació assessorament per a la determinació de la Categoria del Sistema.
- Col·laborar, si així se li requereix, en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat.
- Dur a terme les funcions de l'administrador de la seguretat del sistema:
    - La gestió, configuració i actualització, en el seu cas, del maquinari i programari en els quals 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 l'autoritzat.
    - Aprovar els canvis en la configuració vigent del Sistema d'Informació.
    - Assegurar que els controls de seguretat establerts són complerts estrictament.
    - Assegurar que són aplicats els procediments aprovats per a manejar el Sistema d'Informació.
    - Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
    - Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

FUNCIONS DEL COMITÉ DE SEGURETAT DE LA INFORMACIÓ

Les funcions pròpies d'un Comitè de Seguretat de la Informació són les 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 a això s'encarregarà de:

    - Coordinar els esforços de les diferents àrees en matèria de Seguretat de la Informació, per a 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 seva dotació pressupostària corresponent, prioritzant 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 seva 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 possibles actuacions respecte d'ells.
    - Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'ells.
    - Elaborar i revisar regularment la Política de Seguretat de la Informació per a la seva aprovació per l'òrgan competent.
    - Elaborar la normativa de Seguretat de la Informació per a la seva aprovació en coordinació amb la Direcció General.
    - Verificar els procediments de seguretat de la informació i altra documentació per a la seva aprovació.
    - Elaborar programes de formació destinats a formar i sensibilitzar al 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.

RESOLUCIÓ DE CONFLICTES

Si hi hagués conflicte entre els Responsables, serà resolt pel Comitè de Seguretat de la Informació.

DADES DE CARÀCTER PERSONAL

L'Ajuntament, en el tractament de les dades personals, compleix amb els principis i obligacions de la normativa vigent, entre una altra el Reglament 679/2016, 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-) i la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia de drets digitals, respectant, en tot cas, el dret fonamental a la protecció de dades personals, la intimitat i la resta dels drets fonamentals reconeguts tant en la legislació i tractats internacionals com en la Constitució vigent.

El Delegat/da de protecció de dades de la corporació local va ser adjudicat mitjançant contracte de serveis per acord de la Junta de Govern Local de data 15 d'abril de 2019 i 12 d'agost de 2024.

DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El compliment dels objectius marcats en aquesta Política de Seguretat es duu a terme mitjançant el desenvolupament de documentació que componen les normes i procediments de seguretat associats al compliment de l'Esquema Nacional de Seguretat. Per a la seva organització s'ha definit una Norma per a la Gestió de la Documentació, que estableix les directrius per a l'organització, gestió i accés.

La revisió anual de la present Política correspon al Responsable de Govern, proposant en cas que sigui necessari millores d'aquesta, per a la seva aprovació per part del mateix òrgan que la va aprovar inicialment.

TERCERES PARTS

Quan el presti serveis a altres organismes, o manegi informació d'altres organismes, se'ls farà partícip d'aquesta Política de Seguretat de la Informació.

L'Ajuntament 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 de les actuacions que l'Ajuntament dugui a terme en matèria de Seguretat en relació amb altres organismes.

Quan l'Ajuntament 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 concerneixi a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en l'esmentada normativa, podent

desenvolupar els seus propis procediments operatius per a 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 l'establert en aquesta Política de Seguretat.

D'igual manera, tenint en compte l'obligació de complir amb el que es disposa en les Instruccions Tècniques de Seguretat recollida en la Disposició addicional segona (Desenvolupament de l'Esquema Nacional de Seguretat) del Reial decret Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, i en consideració a la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat, on s'estableix que els operadors del sector privat que prestin serveis o proveeixin solucions a les entitats públiques, als quals resulti exigible el compliment de l'Esquema Nacional de Seguretat, 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 requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la manera de tractar-los. Aquest informe haurà de ser aprovat pels responsables d'informació i els serveis, amb caràcter previ a l'inici de la relació amb la tercera part.

APROVACIÓ I ENTRADA EN VIGOR

Aquesta “Política de Seguretat de la Informació”, d'ara endavant Política, serà efectiva des del dia següent a la seva aprovació pel Ple.