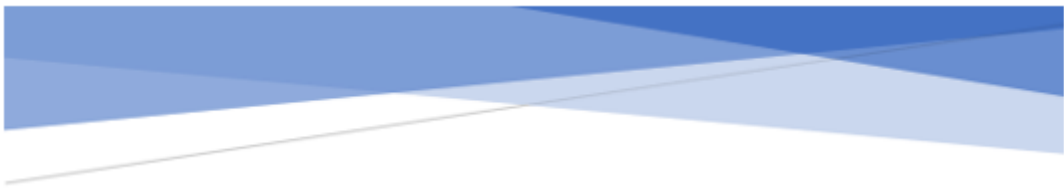




CODI DE VERIFICACIÓ	1W295N3L6C5I4P6C04AU		
PROCEDIMENT	V440 Protocols de seguretat informàtica		
EXPEDIENT NÚM.	AJT/84945/2025	DOCUMENT NÚM.	1288255/2025
ÀREA	Alcaldia-Presidència		
UNITAT	Informàtica i TIC		



## **POLÍTICA DE SEGURETAT DE LA INFORMACIÓ L'H** En relació a l'Esquema Nacional de Seguretat

Servei d'Infraestructures, seguretat i suport TIC  
**Edició:** Novembre de 2025



## SUMARI DE CONTINGUTS

1. Introducció (3)
2. Marc de regulació (3)
3. Missió i serveis prestats per l'Ajuntament de L'Hospitalet (4)
4. Principis bàsics: (4)
  - 4.1 La seguretat com un procés integral i millora contínua del procés de seguretat. (5)
  - 4.2 Mínim privilegi. (5)
  - 4.3 Vigilància contínua i reavaluació periòdica i integritat i actualització del sistema. (5)
  - 4.4 Gestió de personal i professionalitat. (6)
  - 4.5 Gestió de la seguretat basada en els riscos i anàlisi i gestió de riscos.(6)
  - 4.6 Incidents de seguretat, prevenció, detecció, resposta i conservació. (7)
  - 4.7 Línies de defensa. (7)
  - 4.8 Prevenció davant altres sistemes interconnectats. (8)
  - 4.9 Autorització i controls dels accessos i registres d'activitats i detecció de codi maliciós. (8)
  - 4.10 Protecció de les instal.lacions.(8)
  - 4.11 Adquisició de productes de seguretat i contractació de serveis de seguretat. (8)
  - 4.12 Protecció d' informació emmagatzemada i en trànsit i continuïtat de l'activitat.(9)
  - 4.13 Compliment dels requisits mínims. (9)
5. Objectius de la seguretat de la informació (10)
6. Abast (11)
7. Organització i gestió de la seguretat de la informació: (11)
  - 7.1 Definició de rols i responsabilitats associades a l'ENS: Responsables de la informació i dels serveis; Responsable de la seguretat de la informació; Responsable del sistema i Responsables del sistema delegats. (12)
  - 7.2 El Comitè de Seguretat de la informació de l'Ajuntament de L'Hospitalet: Composició; Funcions; Periodicitat de les reunions i adopció d'acords del Comitè; Grup de treball TIC. (14)
8. Gabinet de crisi (16)
9. Dades de caràcter personal (17)
10. Obligacions del personal (19)
11. Terceres parts (19)
12. Gestió i desenvolupament de la política de seguretat de la informació (20)



## 1 INTRODUCCIÓ

L'Ajuntament de l'Hospitalet depèn dels sistemes TIC (Tecnologies de la Informació i les Comunicacions) per assolir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant de danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat, traçabilitat i autenticitat de la informació tractada i dels serveis prestats.

Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com 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.

Les diferents unitats administratives de l'Ajuntament han de tenir present 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 les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en els plecs de licitació pels projectes que incloguin qualsevol tipus de tecnologia o aplicació.

I en definitiva, cal donar compliment a la legislació vigent en l'àmbit de la seguretat de les dades personals (RGPD) i de serveis per mitjans electrònics (ENS) i fomentar la millora, per tal que es garanteixin els principis que han de regir el tractament de dades: privacitat en el disseny, responsabilitat proactiva i gestió dels riscos associats.

La gestió de la informació ha d'incloure les mesures necessàries per garantir la protecció davant de les possibles incidències (accidentals o deliberades) que es puguin produir, de forma que es puguin minimitzar les afectacions sobre la disponibilitat, integritat o confidencialitat de la informació relacionada amb els serveis prestats i les dades personals.

Per tant, per a l'entitat, l'objectiu de la Seguretat de la Informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària per detectar qualsevol incident i reaccionant amb pretesa els incidents per recuperar els serveis com més aviat millor, amb l'aplicació de les mesures.

## 2 MARC DE REGULACIÓ

El marc normatiu que aplica a l'Ajuntament és aquell que està regit a través de totes aquelles normes que integrin la seguretat de la informació a l'àmbit del servei que presta l'organització, especialment l'Esquema Nacional de Seguretat (ENS), com la normativa aplicable en relació a l'Administració digital, protecció de dades i qualsevol norma que derivi o hi estigui tractada.



També es tindran en compte les instruccions tècniques de seguretat i les guies de seguretat del CCN, que seran aplicables per a millorar el compliment del que s'estableix en l'ENS.

Es mantindrà un annex amb la identificació de la normativa aplicable, el qual establirà l'actualització d'aquest annex, tant per un canvi normatiu com per una modificació del present document.

### **3 MISSIÓ I SERVEIS PRESTATS PER L'AJUNTAMENT DE L'HOSPITALET**

Mitjançant la present Política de Seguretat l'Ajuntament de l'Hospitalet de Llobregat expressa el seu compromís amb l'administració de la seguretat de la seva informació, d'acord amb els requeriments propis, així com amb les lleis i les normatives vigents.

L'Ajuntament, en l'exercici de les seves funcions i competències, impulsa serveis públics i tràmits electrònics orientats a satisfer les necessitats de la ciutadania i a promoure la participació activa en els afers públics. Aquesta aposta per la digitalització té com objectiu reforçar la transparència, l'eficiència i la confiança en la relació entre l'administració i la ciutadania.

Amb l'objectiu de disposar d'elements per a la defensa davant amenaces emergents a la seguretat de la informació i els processos, l'Ajuntament necessita disposar d'una estratègia que s'adapti als canvis constants que es produeixen a l'entorn per garantir la prestació continuada dels serveis.

Això implica que l'Ajuntament ha d'aplicar les mesures mínimes de seguretat exigides pel Reial Decret que regula l'ENS, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Totes les àrees funcionals de l'Ajuntament han d'integrar la seguretat de la informació com un element essencial en tot el cicle de vida dels sistemes, des del disseny fins a la seva retirada. Això implica incorporar els requisits de seguretat i les necessitats de finançament en la planificació, la contractació i l'execució de projectes relacionats amb les tecnologies de la informació, assegurant una gestió responsable i alineada amb les expectatives de la societat a la qual serveix.

### **4 PRINCIPIS BÀSICS**

L'ENS determina una sèrie de principis bàsics i requisits mínims de seguretat que cal respectar i desenvolupar de forma proporcional a les característiques de la informació i dels serveis a protegir i tenint en compte la categoria dels sistemes afectats.



#### **4.1 La seguretat com un procés integral i millora contínua del procés de seguretat**

La seguretat constitueix un procés integrat per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes. L'aplicació del ENS a l'Ajuntament de l'Hospitalet de Llobregat estarà presidida per aquest principi, que exclou qualsevol actuació puntual o tractament circumstancial.

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.

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

#### **4.2 Mínim privilegi**

Els sistemes es dissenyaran i configuraran atorgant els mínims privilegis necessaris pel correcte exercici de les seves funcions, el que implica incorporar els següents aspectes:

Els sistemes d'informació proporcionaran la funcionalitat mínima imprescindible perquè l'organització aconsegueixi els seus objectius competencials o contractuals.

Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'assegurarà que només són desenvolupades per les persones autoritzades, des d'emplaçaments o equips així mateix autoritzats.

S'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades a la finalitat que es persegueix. L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari.

#### **4.3 Vigilància contínua, reavaluació periòdica, integritat i actualització del sistema**

La vigilància contínua 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, i corregint-les aplicant les actualitzacions i modificacions necessàries.



Les mesures de seguretat es reavaluaran 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.

#### **4.4 Gestió de personal i professionalitat**

El personal, propi o aliè, relacionat amb els sistemes d'informació de l'Ajuntament de l'Hospitalet de Llobregat, haurà de ser format i informat dels seus deures, obligacions i responsabilitats en matèria de seguretat. El personal, en l'acompliment de les seves funcions, aplicarà les normes i procediments operatius de seguretat aprovats, i la seva actuació haurà de ser supervisada per a verificar que així sigui.

S'establirà un programa de conscienciació contínua per a tot el personal de l'Ajuntament, en particular per als de nova incorporació, incloent formació periòdica en matèria de seguretat de la informació i en l'ús segur dels sistemes d'informació. El significat i abast de l'ús segur dels sistemes d'informació es concretarà i plasmarà en unes normes de seguretat que seran aprovades pel Comitè de Seguretat de la Informació i que tot el personal haurà d'aplicar en l'acompliment de les seves funcions.

La seguretat dels sistemes d'informació estarà atesa i serà revisada i auditada, en totes les fases del seu cicle de vida per personal degudament qualificat, dedicat i instruït. L'Ajuntament exigirà, de manera objectiva i no discriminatòria, que les organitzacions que els prestin serveis de seguretat comptin amb professionals qualificats i amb uns nivells idonis de gestió i maduresa en els serveis prestats.

L'Ajuntament determinarà els requisits de formació i experiència necessària del personal per al desenvolupament del seu lloc de treball.

#### **4.5 Gestió de la seguretat basada en els riscos i anàlisi i gestió de riscos**

L'anàlisi i la gestió dels riscos és part essencial del procés de seguretat, havent de constituir 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.

L'Ajuntament realitzarà periòdicament l'anàlisi i tractament dels riscos de tots els sistemes afectats per aquesta Política de seguretat, emprant metodologies reconegudes internacionalment.



#### 4.6 Incidents de seguretat, prevenció, detecció, resposta i conservació

L'Ajuntament de l'Hospitalet de Llobregat disposarà de procediments de gestió d'incidents de seguretat que millorin la capacitat de resposta davant d'aquestes crisis i permetin afrontar-les de forma eficaç i eficient, amb l'objectiu de poder tornar a la normalitat amb les menors conseqüències per a l'organització i la ciutadania.

La seguretat del sistema ha de contemplar 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 gestiona o als serveis que presta.

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

Les mesures de detecció aniran dirigides a descobrir la presència d'un ciberincident. En el moment de detectar un incident de seguretat s'aplicaran criteris de classificació per decidir si la gravetat del mateix requereix o no la convocatòria del Comitè de Crisi.

Les mesures de resposta, que 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, així com a la comunicació que correspongui a les parts interessades, i al registre de les actuacions. Aquest registre s'utilitzarà per la millora contínua de la seguretat del sistema.

Sense detriment dels restants principis bàsics i requisits mínims establerts, 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.

#### 4.7 Línies de defensa

L'Ajuntament de l'Hospitalet implementarà una estratègia de protecció constituïda per múltiples capes de seguretat, constituïdes per mesures organitzatives, físiques i lògiques, de manera que, quan una de les capes sigui compromesa, permeti:

- a) 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.
- b) Minimitzar l'impacte final sobre aquest.



#### **4.8 Prevenció davant altres sistemes interconnectats**

Es protegirà el perímetre dels sistemes d'informació, especialment, si es connecten a xarxes públiques, 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.

#### **4.9 Autorització i control dels accessos i registres d'activitat i detecció de codi maliciós**

L'accés controlat als sistemes d'informació estarà limitat als usuaris, processos, dispositius o altres sistemes d'informació, degudament autoritzats, i exclusivament a les funcions permeses.

A fi de preservar la seguretat dels sistemes d'informació i de conformitat amb la normativa sobre protecció de dades personals i el respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació allà enunciats, es registraran 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. Així mateix es podran, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, de manera que sigui possible impedir accessos no autoritzats, atacs i danys a les 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.

#### **4.10 Protecció de les instal·lacions**

Els sistemes d'informació i la seva infraestructura de comunicacions associada hauran de romandre en àrees controlades i disposar dels mecanismes d'accés adequats i proporcionals en funció de l'anàlisi de riscos.

#### **4.11 Adquisició de productes de seguretat i contractació de serveis de seguretat**

En l'adquisició de productes de seguretat o contractació de serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació s'utilitzaran, de forma proporcionada a la categoria del sistema i el nivell de



seguretat determinats, aquells que tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició.

L'entitat de certificació preferent segons el ENS és l'Organisme de Certificació de l'Esquema Nacional d'Avaluació i Certificació de Seguretat de les Tecnologies de la Informació del Centre Criptològic Nacional.

En cas que aquest organisme no hagi realitzat encara certificacions d'una determinada categoria de productes o serveis de seguretat, o per causa major, es podran seleccionar productes amb altres certificacions de seguretat reconegudes internacionalment, principalment la de *Common Criteria*.

L'ús de productes o serveis de seguretat certificats només es podrà obviar en aquells casos en què les exigències de proporcionalitat en quant als riscos assumits no ho justifiquin, segons el criteri del Comitè de Seguretat.

#### **4.12 Protecció de la informació emmagatzemada i en trànsit. Continuitat de l'activitat**

En l'organització i implantació de la seguretat es 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, quan això sigui exigible.

Tota informació en suport no electrònic que hagi estat causa o conseqüència directa de la informació electrònica, 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.

#### **4.13 Compliment dels requisits mínims**

Per a donar compliment als requisits mínims establerts en el ENS, l'Ajuntament de L'Hospitalet de Llobregat adoptarà les mesures i reforços de seguretat corresponents indicats en l'annex II del ENS, tenint en compte:

- a) Els actius que constitueixen els sistemes d'informació implicats.
- b) La categoria del sistema.
- c) Les decisions que s'adoptin per a gestionar els riscos identificats.

Les mesures anteriors tindran la condició de mínims exigibles, sent ampliables a criteri del responsable de la seguretat, qui podrà incloure mesures addicionals, tenint en



compte l'estat de la tecnologia, la naturalesa de la informació tractada o els serveis prestats i els riscos als que estan exposats els sistemes d'informació afectats.

La relació de mesures de seguretat seleccionades es formalitzarà en un document denominat Declaració d'Aplicabilitat, signat pel responsable de la seguretat.

Les mesures de seguretat referenciades en l'annex II del ENS podran ser reemplaçades per altres compensatòries, sempre que es justifiqui documentalment que protegeixen, igual o millor, del risc sobre els actius i se satisfan els principis bàsics i els requisits mínims previstos en el ENS. Com a part integral de la Declaració d'Aplicabilitat s'indicarà, de manera detallada, la correspondència entre les mesures compensatòries implantades i les mesures de l'annex II del ENS que compensen.

## 5 OBJECTIUS DE LA SEGURETAT DE LA INFORMACIÓ

L'Ajuntament estableix com a objectius de la seguretat de la informació els següents:

- Garantir la qualitat i protecció de la informació.
- Aconseguir la plena conscienciació dels usuaris pel que fa a la seguretat de la informació.
- Gestió d'actius d'informació: els actius d'informació de l'entitat es trobaran inventariats i categoritzats i estaran associats a un responsable.
- Seguretat lligada a les persones: s'implantaran els mecanismes necessaris perquè qualsevol persona que hi accedeixi, o pugui accedir als actius d'informació, conegui les seves responsabilitats i d'aquesta manera es redueixi el risc derivat d'un ús indegut, aconseguint la plena conscienciació de els usuaris respecte a la seguretat de la informació.
- Seguretat física: els actius d'informació seran emplaçats en àrees segures, protegides per controls d'accés físics adequats al seu nivell de criticitat. Els sistemes i els actius d'informació que contenen aquestes àrees estaran suficientment protegits davant d'amenaques físiques o ambientals.
- Seguretat en la gestió de comunicacions i operacions: s'establiran els procediments necessaris per aconseguir una gestió adequada de la seguretat, operació i actualització de les TIC. La informació que es transmeti a través de xarxes de comunicacions haurà de ser adequadament protegida, tenint en compte el seu nivell de sensibilitat i de criticitat, mitjançant mecanismes que en garanteixin la seguretat.
- Control d'accés: es limitarà l'accés als actius d'informació per part dels usuaris, els processos i altres sistemes d'informació mitjançant la implantació dels mecanismes d'identificació, autenticació i autorització d'acord amb la criticitat de cada actiu. A més, queda registrada la utilització del sistema per assegurar la traçabilitat de l'accés i auditar-ne l'ús adequat, d'acord amb l'activitat de l'organització.
- Adquisició, desenvolupament i manteniment dels sistemes d'informació: es contemplaran els aspectes de seguretat de la informació en totes les fases del cicle de



vida dels documents, de les dades i dels sistemes d'informació, garantint la seva seguretat des del disseny i per defecte.

- Gestió dels incidents de seguretat: s'implantaran els mecanismes apropiats per a la correcta identificació, registre i resolució dels incidents de seguretat.
- Garantir la prestació continuada dels serveis: s'implantaran els mecanismes apropiats per assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels processos de negoci, d'acord amb les necessitats de nivell de servei dels usuaris.
- Protecció de dades: s'adoptaran les mesures tècniques i organitzatives que correspongui implantar per atendre els riscos generats pel tractament per complir la legislació de seguretat i privadesa.
- Compliment: s'adoptaran les mesures tècniques, organitzatives i procedimentals necessàries per al compliment de la normativa legal vigent en matèria de seguretat de la informació.
- Seguretat de la documentació: dissenyar i garantir les mesures de seguretat de la documentació municipal d'acord amb les polítiques de gestió documental aprovades.

## 6 ABAST

Aquesta política s'aplicarà als sistemes d'informació de l'Ajuntament de l'Hospitalet, 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'abast de l'Esquema Nacional de Seguretat (ENS).

Tots els empleats públics i càrrecs electes (membres) de l'Ajuntament de l'Hospitalet així com el personal de tercers relacionats amb aquest, que es trobin afectats per l'abast de l'ENS, tenen l'obligació de conèixer i complir aquesta Política i la normativa de seguretat, sent responsable del Comitè de Seguretat de la Informació disposar dels mitjans necessaris per què la informació arribi al personal afectat.

## 7 ORGANITZACIÓ I GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ

L'Ajuntament, tenint en compte els articles 11, 12 i 13 de l'ENS, estableix les accions següents per organitzar la Seguretat de la Informació:

1. Designarà rols de seguretat: Unificació del Responsable de la Informació i el Responsable dels Serveis; Responsable de la Seguretat de la Informació; Responsable del Sistema i Delegat de Protecció de Dades. També, es designaran Responsables del Sistema delegats.



2. Constituirà un òrgan consultiu i estratègic per a la presa de decisions en matèria de seguretat de la informació. Aquest òrgan s'anomena Comitè de Seguretat de la Informació.

### 7.1 Definició de Rols i Responsabilitats associades a l'ENS:

➤ **Responsable de la Informació i Responsable dels Serveis. Seran funcions dels Responsable de la Informació i del Responsable dels Serveis:**

- Establir els requisits de seguretat aplicables a la Informació (nivells de seguretat de la Informació) i als Serveis (nivells de seguretat dels serveis), dins del marc establert a l'Annex I del RD ENS, podent demanar una proposta al Responsable de Seguretat i tenint en compte l'opinió del Responsable del Sistema.
- Dictaminar respecte dels drets d'accés a la informació i als serveis.
- Acceptar els nivells de risc residual que afecten la informació i els serveis.
- Posar en comunicació del Responsable de Seguretat qualsevol variació respecte a la informació i els serveis dels quals és responsable, especialment la incorporació de nous serveis o informació al seu càrrec. El qual traslladarà aquests canvis, al Comitè de Seguretat de la Informació, en la propera reunió.
- Tenir la responsabilitat última de l'ús que es faci de determinats serveis i informació i, per tant, de la seva protecció.

➤ **Responsable de la Seguretat de la Informació. Seran funcions del Responsable de Seguretat de la Informació (d'ara endavant, Responsable de Seguretat):**

- Mantenir i verificar el nivell adequat de seguretat de la informació 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 i elaborar documentació del sistema.
- Aprovar la Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides d'acord amb l'Annex II de l'ENS.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable del Sistema i/o Comitè de Seguretat TIC.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comitè de Seguretat l'aprovació de canvis i altres requisits del sistema.
- Aprovar els procediments de seguretat que formen part del Mapa Normatiu (i no són competència del Comitè) i posar en coneixement el Comitè de les modificacions que s'hagin fet al llarg del període en curs.
- Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per aprovar-la per Direcció.
- Actuarà com a Secretari del Comitè de Seguretat de la Informació, realitzant les funcions següents:



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

➤ **Responsable del Sistema i Responsables del Sistema delegats. Seran funcions del Responsable del Sistema i els seus delegats en l'àmbit que els correspongui:**

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, elaborant 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.
- Aturar l'accés a informació o prestació de servei si es té el coneixement que aquests presenten deficiències greus de seguretat.
- Assegurar que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el Responsable de Seguretat i/o Comitè de Seguretat de la Informació.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat.
- Coordinar les funcions de l'administrador de la seguretat del sistema:
  - La gestió, configuració i actualització, si escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat.
  - La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la seva correspondència amb allò autoritzat.
  - Aprovar els canvis a la configuració vigent del Sistema d'Informació.
  - Assegurar que els controls de seguretat establerts són estrictament complerts.
  - Assegurar que són aplicats els procediments aprovats per manejar el sistema d'informació.
  - Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
  - Monitoritzar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i els mecanismes d'auditoria tècnica.
  - Informar el Responsable de Seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
  - Col·laborar en la investigació i resolució d'incidents de seguretat, des de la detecció fins a la resolució.

Les funcions dels Responsables del Sistema delegats seran aquelles que els hagin estat delegades pel Responsable del Sistema, i estaran relacionades amb l'operació, manteniment, instal·lació i verificació del correcte funcionament del Sistema d'Informació. Cada Responsable de Sistema delegat tindrà una relació directa amb el Responsable del Sistema, que és qui té la responsabilitat sobre la totalitat del Sistema.



#### **En quant a la designació dels rols descrits anteriorment:**

- Els rols de Responsable de la informació i Responsable dels Serveis són assumits pel Comitè de Seguretat de la informació.
- El rol de Responsable de la Seguretat de la Informació és assumit pel Cap de Servei d'Infraestructures, Seguretat i Suport TIC o lloc equivalent, en cas de canvi d'organigrama municipal.
- El rol de Responsable del Sistema és assumit pel Cap de Secció d'Infraestructura de Sistemes i Ciberseguretat o lloc equivalent, en cas de canvi d'organigrama municipal.

Els rols de Responsables del Sistema delegats, són assumits pels: Cap de Servei de Desenvolupament TIC; Cap de Secció de Comunicacions i Suport TIC; Cap de Secció de Govern de les Dades i el Cap de Servei de Sistemes d'Informació Territorial (o llocs equivalents, en el cas de canvi d'organigrama municipal).

#### **7.2 El Comitè de Seguretat de la Informació de l'Ajuntament de L'Hospitalet:**

És l'òrgan de direcció i seguiment en matèria de seguretat dels actius TIC de l'organització.

Amb la finalitat de facilitar la implantació i gestió del procés de seguretat a l'Ajuntament de L'Hospitalet de Llobregat, mitjançant l'aprovació de la present política s'aprova també la formació del Comitè de Seguretat de la Informació.

Aquest Comitè té la funció de coordinar totes les funcions de seguretat del Ajuntament de L'Hospitalet de Llobregat, vetllant pel compliment de la normativa d'aplicació legal, reguladora i sectorial, a la vegada que supervisa l'alineament de les activitats de seguretat amb els objectius de l'organització.

#### Composició del Comitè:

- **Presidència:**
  - El Gerent municipal o persona en qui delegui.
- **Vocals:**
  - Director/a de Serveis amb competències en l'àmbit TIC.
  - Responsable del Sistema.
  - Responsables del Sistema delegats.
  - Delegat/da de Protecció de Dades (DPD).
- **Secretaria, que recaurà en el Responsable de la Seguretat, amb les funcions següents:**
  - convocar las reunions del Comitè de Seguretat de la informació;
  - preparar els temes a tractar en les reunions del Comitè;
  - aportar informació puntual per la presa de decisions i elaborar acta de les reunions.



Els rols de Responsable de la informació i Responsable dels Serveis són assumits pel Comitè de Seguretat de la informació.

I com a convidats, interns o externs, que es considerin adients.

#### Funcions del Comitè:

- a) 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.
- b) Assessorar en matèria de Seguretat de la Informació.
- c) Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre les diferents unitats administratives, elevant aquells casos en que no tingui prou autoritat per decidir.
- d) 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, prioritant 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 les instruccions i normatives de Seguretat de la Informació.
  - 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 que permetin verificar el compliment de les obligacions de l'Administració en matèria de seguretat de la Informació.



- Gestionar la situació davant d'una crisi originada per un incident de ciberseguretat de gran impacte, creant un Gabinet de crisi, determinant la seva composició en funció de l'abast d'aquest impacte i delimitant les seves funcions.

Periodicitat de les reunions i adopció d'acords del Comitè:

- El Comitè de Seguretat de la Informació es reunirà, almenys, una vegada a l'any, sens perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, requereixi una freqüència més gran en les reunions.
- En qualsevol cas, les reunions es convocaran per la seva Presidència, a través de la Secretaria, a la seva iniciativa o per majoria dels seus membres.
- Les decisions s'han d'adoptar per consens dels membres del Comitè.

Grup de treball TIC:

Dins l'estructura de governança de la ciberseguretat de l'Ajuntament de L'Hospitalet de Llobregat es disposa d'un grup de treball TIC amb tasques relacionades amb les àrees de treball següents: adequació a l'ENS, normativa i gestió de riscos, anàlisi i millora contínua, seguretat en les interconnexions i connectivitat i altres funcions connexes o concordants.

Les tasques del Grup de Treball TIC seran, entre d'altres, les que puguin ser encomanades pel Comitè de Seguretat:

- Gestió i operativa de la seguretat del Projecte d'Adequació, Implantació i gestió de la Conformitat a l'ENS, anàlisi i gestió de riscos, explotació, normativa i manteniment.
- Redacció i presentació de propostes al Comitè de Seguretat TIC. Elaborarà els aspectes relacionats amb la ciberseguretat i els debatrà en primera instància, per tal de ser traslladats al Comitè.

La composició del grup de treball TIC vindrà determinada pel Comitè de Seguretat, proposant-se inicialment per la seva composició als següents càrrecs:

- Responsable de Seguretat.
- Responsable del Sistema.
- Administradors especialistes de seguretat.

## 8 GABINET DE CRISI

Davant d'un incident de ciberseguretat amb impacte de gran abast per l'Ajuntament, el Comitè de Seguretat podrà activar el Gabinet de Crisi, que permetrà una gestió unificada per enfrontar aquest incident.



En aquesta situació el Gabinet de Crisi de ciberseguretat tindrà com a comesa principal accelerar el procés de presa de decisions per resoldre incidències, definint les prioritats i establint l'estratègia a seguir.

Per aquest motiu es proposa que la seva composició compregui els següents càrrecs:

- Alcalde/ssa o a qui ell/a delegui
- Cap de Gabinet d'alcaldia o a qui ell/a delegui
- Tinència d'Alcaldia amb competències en l'àmbit TIC o a qui ell/a delegui
- Director/a de Serveis amb competències en l'àmbit TIC o a qui ell/a delegui
- Gerència o a qui ell/a delegui
- Director/a de serveis amb competències en l'àmbit de Recursos Humans o a qui ell/a delegui
- Director/a de serveis amb competències en l'àmbit de l'Assessoria Jurídica o a qui ell/a delegui
- Director/a de serveis amb competències en l'àmbit de Comunicació o a qui ell/ella delegui
- Responsable de Seguretat
- Responsable del Sistema i Responsables del Sistema delegats
- Delegat de Protecció de Dades
- Cap de Comunicació o a qui ell/a delegui
- I aquelles persones que es consideri adient.

Les funcions del Gabinet de Crisi són les següents:

- Avaluar la informació rebuda sobre l'incident i fer una valoració inicial del seu impacte.
- Realitzar previsions dels escenaris als que pot evolucionar l'incident per prendre mesures preventives.
- Determinar, validar i supervisar les estratègies i mesures implementades i/o proposades per l'equip de resposta a incidents.
- Determinar les prioritats per recuperar les activitats i serveis en el menor temps possible.
- Activar la mobilització de recursos extraordinaris quan sigui necessari.
- Assumir la responsabilitat de la comunicació i assegurar la interlocució amb totes les parts interessades i afectades internes o externes a l'organització.
- Definir l'estratègia de comunicació.

## 9 DADES DE CARÀCTER PERSONAL

L'Ajuntament de l'Hospitalet de Llobregat només recollirà dades de caràcter personal quan aquestes siguin adequades, pertinents i no excessives, i es trobin en relació amb l'àmbit i les finalitats per a les quals s'hagin obtingut. Així mateix, adoptarà les mesures tècniques i



organitzatives necessàries per garantir el compliment de la normativa de protecció de dades vigent en cada moment.

L'Ajuntament de l'Hospitalet de Llobregat ha implementat els mecanismes adequats per assegurar l'adequació a la normativa vigent en matèria de protecció de dades. En particular, l'Ajuntament ha adoptat les mesures oportunes per complir amb el 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 la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

En desenvolupament dels principis de la vigent normativa de protecció de dades, entre altres, la proactivitat, l'Ajuntament de l'Hospitalet de Llobregat té configurada la seva política de Protecció de Dades publicada a la seu electrònica municipal amb accés públic a l'adreça [Protecció de dades | Seu electrònica, https://seuelectronica.l-h.cat/2489353\\_1.aspx?id=1#politica](https://seuelectronica.l-h.cat/2489353_1.aspx?id=1#politica)

## 9.1 Drets dels interessats

El dret dels interessats són personals i seran exercits per l'afectat davant de l'Ajuntament de l'Hospitalet com a responsable de Tractament.

L'Ajuntament de l'Hospitalet de Llobregat ha definit procediments específics per l'exercici de drets de protecció de dades, on es descriu el procediment, normativa i terminis per gestionar cadascun dels drets que la legislació reconeix als interessats, disposant del seu accés dins l'apartat de protecció de dades de la seu electrònica.

- Dret d'accés (article 15 del RGPD)
- Dret de rectificació (article 16 del RGPD)
- Dret de supressió o "dret a l'oblit" (article 17 del RGPD)
- Dret a la limitació del tractament (article 18 del RGPD)
- Dret a la portabilitat de les dades (article 20 del RGPD)
- Dret d'oposició i a no ser objecte de decisions individuals automatitzades (articles 21-22 del RGPD)

## 9.2 Aplicació del principi de responsabilitat proactiva i demostrable

El Principi de responsabilitat proactiva i demostrable recull el compromís efectiu amb els drets i llibertats de les persones per part de la Corporació Municipal, de manera que es garanteixi que totes les accions que es duguin a terme respecte als tractaments de dades personals aniran sempre encaminades a complir de la manera més efectiva possible les obligacions establertes per la legislació.

Les accions que es portaran a terme seran les següents:



- Accions orientades a la protecció, accessibilitat i qualitat dels dades en el disseny, de manera que es garanteixi que davant d'un nou tractament de dades s'hagin tingut en compte els principis de la legislació de protecció de dades, transparència i dades obertes, així com els dissenys dels sistemes de gestió i processos interns.
- Avaluacions d'impacte sobre dades personals, tenint en compte l'impacte que els tractaments de dades puguin tenir a l'organització des de les dimensions tècniques, organitzatives i jurídiques.
- Anàlisi i gestió dels riscos associats als tractaments de dades personals.
- Creació d'un Registre d'Activitats de Tractament on la Corporació Municipal identificarà tots els tractaments de dades que duu a terme en el desenvolupament de la seva activitat.
- Aprovació per acord de la Junta de Govern Local, de sessió 17/05/2023, la instrucció d'aplicació a l'Ajuntament de l'Hospitalet de Llobregat del reglament (UE) 2016/679 de protecció dades personals i la llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals
- Nomenament del corresponent Delegat de Protecció de Dades.

## 10 OBLIGACIONS DEL PERSONAL

Tot el personal de l'Ajuntament, tant propi com aliè, que interactui amb el sistema d'informació haurà de complir aquesta política de seguretat de la informació i les diferents normatives que la sustenten.

## 11 TERCERES PARTS

Quan l'Ajuntament de l'Hospitalet de Llobregat presti serveis a altres organismes o manegi informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals per informe i coordinació dels respectius Comitès de Seguretat i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'Ajuntament de l'Hospitalet de Llobregat utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que pertoca a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, i poden desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta política.

Quan algun aspecte de la política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat i – si es tracten dades personals – del DPD, que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.



## 12 GESTIÓ I DESENVOLUPAMENT DE LA POLÍTICA DE SEGURITAT DE LA INFORMACIÓ

Aquesta política s'ha de desenvolupar per mitjà de normatives de seguretat que afrontin aspectes específics. Aquestes normatives de seguretat estaran a disposició de tots els membres de l'organització que necessitin conèixer-les, en particular per aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

Les normatives de seguretat estaran disponibles a través de xarxa corporativa, publicades a la Intranet o qualsevol altre sistema que permeti l'accés al personal de l'Ajuntament.