**Exp. X2025000695**

# D E C R E T

## Aprovació de la Política de Seguretat de la Informació del Consorci del Parc Natural de la Serra de Collserola

## I. ANTECEDENTS DE FET

**1.** La informació constitueix un element essencial per a la prestació dels serveis per part del Consorci del Parc Natural de la Serra de Collserola. Aquesta informació és processada mitjançant les tecnologies de la informació i les comunicacions, que han esdevingut un element indispensable per a les administracions públiques al suportar el tractament d'aquesta informació, en especial, en els serveis de l'administració electrònica adreçats a la ciutadania i a les Administracions Públiques a les quals es prestin serveis.

**2.** Tot i les millores quant a operativitat i eficiència que suposa el tractament de la informació i els serveis per mitjans electrònics, aquestes impliquen l'assumpció de nous riscos i requereixen de la implantació d'un conjunt de mesures específiques per protegir la informació i els serveis prestats pel Consorci. En aquest sentit, la seguretat de la informació té com a objectiu protegir la informació i els serveis mitjançant l'anàlisi dels riscos als quals estan sotmesos i la proposta de les mesures necessàries per reduir-los fins a un nivell que resulti acceptable per a l'organització. Aquest nivell de risc acceptable ha de ser determinat per la direcció de l'entitat, així com l'ordenació de les actuacions necessàries i l'habilitació dels mitjans que siguin necessaris per dur-les a terme.

**3.** La finalitat de l'Esquema Nacional de Seguretat (ENS) és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeti a la ciutadania i a les administracions públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans.

**4.** Amb aquest objectiu, el Consorci ha elaborat la Política de Seguretat de la Informació, donant compliment a l'article 12 del Reial Decret 311/2022, de 3 de maig, pel qual es regula l'ENS, que obliga les Administracions Públiques a disposar d'una política de seguretat i estableix els requisits mínims que han de complir.

**5.** Resulta una actuació prioritària l'establiment d'una política de seguretat de la informació, amb la subsegüent distribució de funcions i responsabilitats en l'àmbit de la seguretat de la informació. Aquests són els dos instruments principals per al govern de la seguretat de la informació i constitueixen el marc de referència per a totes les actuacions posteriors.

**6.** La Política de Seguretat segueix les indicacions de la guia CCN-STIC-805 del Centre Criptològic Nacional (CCN), centre adscrit al Centre Nacional d'Intel·ligència (CNI). L'adaptació a l'ENS implica que el Consorci, mitjançant el seu personal i els tercers que faciliten serveis relacionats amb l'Administració Electrònica, ha de:

- Aplicar les mesures mínimes de seguretat exigides pel propi ENS
- Realitzar un seguiment continu dels nivells de prestació de serveis
- Seguir i analitzar les vulnerabilitats reportades
- Preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats

**7.** El Consorci té el deure d'assegurar que la seguretat de la informació és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i els costos associats han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en plecs de licitació per a projectes relacionats amb els sistemes d'informació. El Consorci ha d'estar preparat per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'Article 7 de l'ENS.

## II. FONAMENTS DE DRET

1. El Consorci del Parc Natural de la Serra de Collserola, de conformitat amb els articles 1 i 2 dels seus Estatuts, és un ens consorcial públic, de caràcter local i de naturalesa associativa i institucional que gaudeix de personalitat jurídica plena i, per tant, amb capacitat d'obrar i gestionar serveis i activitats d'interès local o general.

2. L'article 156.2 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, estableix que l'Esquema Nacional de Seguretat (ENS) té per objecte establir la política de seguretat en la utilització de mitjans electrònics i que està constituït pels principis bàsics i requisits mínims que garanteixin adequadament la seguretat de la informació tractada.

3. El Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat i que va entrar en vigor el 5 de maig de 2022.

4. La Presidència del Consorci és l'òrgan competent per a l'aprovació de la resolució que es proposa, d'acord amb l'article 13.h) dels Estatuts de l'entitat. No obstant això, la Vicepresidència Executiva del Consorci del Parc Natural de la Serra de Collserola està facultat per aprovar-la, en virtut de la delegació de competències al seu favor, dictada per resolució de la Presidència de data 13 de novembre de 2023 i publicada al Butlletí Oficial de la Província de Barcelona en data 18 de febrer de 2024.

## III. RESOLUCIÓ

Per tant, resolc:

1. Aprovar la Política de Seguretat de la Informació del Consorci del Parc Natural de la Serra de Collserola en els termes de l'annex que s'incorpora al present Decret.

2. Constituir, com a directrius vinculants per a totes les unitats organitzatives del Consorci, els criteris i instruccions contingudes en el document que s'aprova mitjançant la present resolució.
3. Informar el personal del Consorci de l'aprovació de la Política de Seguretat per tal de garantir-ne el compliment.
4. Mantenir la versió actualitzada de la Política de Seguretat de la Informació a la seu electrònica del Consorci: https://www.seu-e.cat/ca/web/parcnaturalcollserola

El vicepresident executiu

Xavier Paz Penche

En dono fe.

El secretari delegat

Antoni Puigarnau i Puigarnau

En data de signatura electrònica

Consorci del Parc Natural de la Serra de Collserola
Ctra. de l'Església, 92. 08017 BARCELONA Tel. 932 800 672

**ANNEX**

**Política de Seguretat del Consorci del Parc Natural de la Serra de Collserola**

Parc Natural de Collserola

Consorci del Parc Natural de la Serra de Collserola
Ctra. de l'Església, 92. 08017 BARCELONA Tel. 932 800 672

# POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DEL CONSORCI DEL PARC NATURAL DE LA SERRA DE COLLSEROLA

Data d'actualització: 10/3/2026

En aquest document trobareu:





NIF: P-0800066 - C

AMB Àrea Metropolitana de Barcelona · Diputació Barcelona · Generalitat de Catalunya

Barcelona, Cerdanyola del Vallès, el Papiol, Esplugues de Llobregat, Molins de Rei, Montcada i Reixac, Sant Cugat del Vallès, Sant Feliu de Llobregat, Sant Just Desvern i EMD de Valldoreix

# INTRODUCCIÓ

El Consorci del Parc Natural de la Serra de Collserola (d'ara endavant, el Consorci), en tant que Administració Pública al servei de la ciutadania, disposa d'una infraestructura de tecnologies d'informació i comunicacions (d'ara endavant, TIC) per a desenvolupar les seves competències i assolir els seus objectius.

La gestió de les TIC ha de ser portada a terme aplicant les mesures necessàries que li permetin 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.

La qualitat de la informació i la prestació continuada de serveis hauran de ser garantits actuant de forma preventiva, mitjançant una adequada supervisió periòdica i constant, tenint com a objectiu final la seguretat de la informació com a cultura general de l'entitat.

D'acord amb l'article 12 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (d'ara endavant, ENS), la **Política de Seguretat** s'ha de configurar sobre la base dels principis bàsics en l'àmbit de l'Administració electrònica i estableix que totes les entitats del sector públic han de disposar de la seva política de seguretat, que ha de ser aprovada formalment per l'òrgan competent i s'ha de desenvolupar aplicant els requisits mínims següents en proporció als riscos identificats en cada sistema:

a. Organització i implantació del procés de seguretat.
b. Anàlisi i gestió dels riscos.
c. Gestió de personal.
d. Professionalitat.
e. Autorització i control dels accessos.
f. Protecció de les instal·lacions.
g. Adquisició de productes de seguretat i contractació de serveis de seguretat.
h. Seguretat per defecte.
i. Integritat i actualització del sistema.
j. Protecció de la informació emmagatzemada i en trànsit.
k. Prevenció enfront d'altres sistemes d'informació interconnectats.
l. Registre de l'activitat i detecció de codi nociu.
m. Incidents de seguretat.
n. Continuïtat de l'activitat.
o. Millora contínua del procés de seguretat.

Per tot el que s'exposa anteriorment, en aquest document es defineix la **Política de Seguretat de la Informació del Consorci**, tenint en compte que l'article 12.1 i el propi Glossari de l'Annex IV del Reial Decret 311/2022, de 3 de maig, defineix la Política de seguretat (Política de seguretat de la informació) com el conjunt de directrius plasmades en un document escrit, que regeixen la forma com una organització gestiona i protegeix la informació que tracta i els serveis que presta.

## 1.1 Abast

Aquesta política s'aplica a tots els sistemes TIC (infraestructures, programari, comunicacions...) del Consorci i a tots els seus membres, sense excepcions.

També s'aplica als sistemes d'informació de les entitats del sector privat (inclosa l'obligació de comptar amb la política de seguretat) quan per relació contractual prestin serveis o proveeixin solucions al sector públic per a l'exercici de les seves competències i potestats administratives.

### 1.2 Missió

Mitjançant la present *Política de Seguretat* el Consorci 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 normatives vigents.

### 1.3 Aprovació i entrada en vigor

Aquesta política de seguretat de la informació és efectiva des de la data d'aprovació mitjançant Decret de Vicepresidència executiva i fins que sigui reemplaçada per una nova política.

## MARC LEGISLATIU

L'ús de les TIC per part del Consorci es troba regulat per les següents normes jurídiques:

**ESTATAL**

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Reial decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat.
- Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.
- 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 (RGPD).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD)
- Reial decret 1671/2009, de 6 de novembre, pel que es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Instruccions del Centre Criptogràfic Nacional, CCN-STIC.

**AUTONÒMIC**

- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, d'ús dels mitjans electrònics al sector públic de Catalunya.

# PRINCIPIS DE COMPLIMENT DE LA POLÍTICA DE SEGURETAT

Les TIC utilitzades pel Consorci han de disposar d'elements que en garanteixin una protecció adient contra amenaces que, degut a la seva constant evolució, tenen un gran potencial per a produir afectacions en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis.

Amb l'objectiu de disposar d'elements per a la defensa d'aquestes amenaces, el Consorci necessita disposar d'una estratègia que s'adapti als canvis constants que es produeixen a l'entorn per garantir la prestació contínua dels serveis. Això implica que el Consorci ha d'aplicar les mesures mínimes de seguretat exigides pel Reial decret 311/2022, de 3 de maig, que regula l'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.

El Consorci ha de garantir que la seguretat TIC esdevingui un element integral del sistema, des del seu disseny inicial fins a la retirada del servei, passant per les decisions de desenvolupament o adquisició de programari i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació de l'àrea, en la sol·licitud de propostes de serveis, i en l'elaboració dels plecs per a la licitació de projectes relacionats amb les TIC.

## 3.1 Dades de caràcter personal

El Consorci, en el desenvolupament de les seves competències, tracta dades de caràcter personal de la ciutadania. La documentació que regula el tractament de dades de caràcter personal al Consorci es troba al registre d'activitats de tractament.

Els sistemes d'informació del Consorci han d'aplicar les mesures de seguretat adients en funció dels nivells de seguretat requerits per la normativa en funció de les dades de caràcter personal identificades al registre d'activitats de tractament.

## 3.2 Gestió de riscos

Tots els sistemes subjectes a aquesta política hauran de ser objecte d'una anàlisi de riscos, on s'avaluïn les amenaces i els riscos a què estan exposats. Aquesta anàlisi es portarà a terme anualment.

A més de l'anàlisi anual, també caldrà portar a terme l'anàlisi quan es produeixin les circumstàncies següents:

- Quan es produeixin canvis en la informació tractada.
- Quan es produeixin canvis en els serveis prestats.
- Quan es detecti una incidència de seguretat greu.
- Quan es detectin vulnerabilitats greus.

Per a l'harmonització de les anàlisi de riscos, el Consorci establirà una valoració de referència per als diferents tipus d'informació tractats i els diferents serveis prestats.

El Consorci garantirà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.



NIF: P-0800066 - C

AMB Àrea Metropolitana de Barcelona · Diputació Barcelona · Generalitat de Catalunya

Barcelona, Cerdanyola del Vallès, el Papiol, Esplugues de Llobregat, Molins de Rei, Montcada i Reixac, Sant Cugat del Vallès, Sant Feliu de Llobregat, Sant Just Desvern i EMD de Valldoreix

### 3.3 Prevenció i reacció davant incidències

El personal del Consorci ha de disposar dels mecanismes per a la prevenció, detecció, resposta i conservació per minimitzar les vulnerabilitats, evitar que les amenaces es materialitzin i, en cas contrari, reaccionar davant de possibles incidents, d'acord amb els articles 8 i 25 de l'ENS, i l'article 33 de l'RGPD si afecta dades personals.

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 aquest no es materialitzin o que, en el cas de fer-ho, no afectin greument a la informació que gestiona o als serveis que presta.

Les mesures de prevenció, que poden 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 incident de seguretat.

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

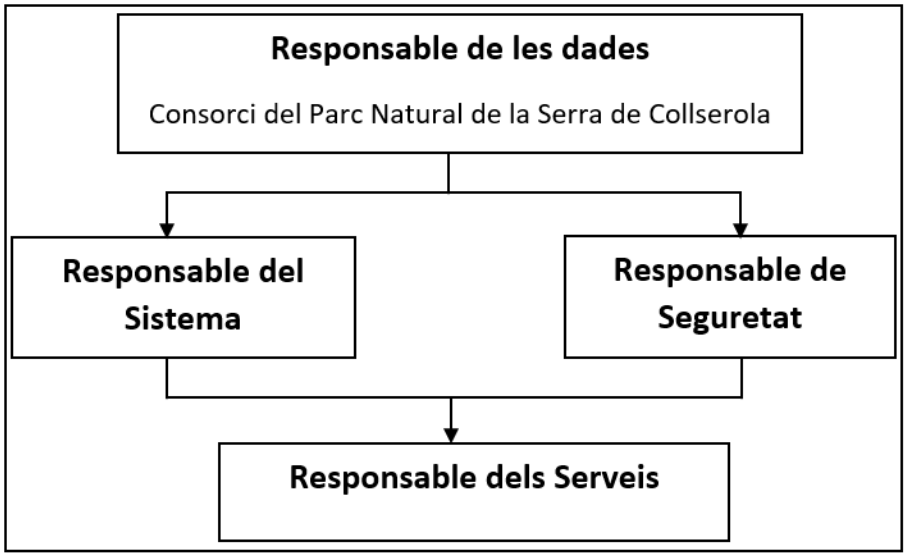
El sistema d'informació garantirà la conservació de les dades i la informació en suport electrònic, garantint que la seva aplicació no suposa una reducció en l'aplicació dels principis bàsics i requisits mínims establerts.

De la mateixa manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital, mitjançant una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

## ORGANITZACIÓ DE LA SEGURETAT

### 4.1 Responsabilitats i funcions

L'organització de la seguretat de la informació del Consorci es concreta en la següent estructura.



### 4.1.1 Responsable de la Informació

| | |
|---|---|
| Responsable | El Consorci |
| Funcions | 1. Nomenar el Responsable de Seguretat ENS.<br>2. Nomenar el Responsable del Sistema.<br>3. Donar el suport i dotar dels recursos necessaris al Responsable de Seguretat i al Responsable del Sistema per a poder portar a terme les seves funcions. |

### 4.1.2 Responsable de Seguretat

| | |
|---|---|
| Responsable | Comissió de Seguretat |
| Components de la Comissió | Segons es determini al document de nomenaments |
| Funcions | 1. Establir, impulsar i garantir l'aplicació i el compliment de les polítiques i procediments de seguretat aprovats pel Consorci.<br>2. Validar i tramitar l'aprovació de la documentació relacionada amb la seguretat de la informació (Política de Seguretat, Reglaments Interns,...).<br>3. Promoure les auditories i controls regulars que permetin verificar el compliment de les obligacions del Consorci en seguretat de la informació.<br>4. Promoure la formació i conscienciació de la seguretat de la informació al personal del Consorci.<br>5. Garantir, amb el suport del Responsable del Sistema, la implantació i control de les mesures de seguretat de manera que aquestes s'integrin adequadament a l'operativa d'Administració Electrònica.<br>6. Garantir la correcta regulació legal dels proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS.<br>7. Vetllar per tal que es dugui a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema.<br>8. Fer el seguiment dels incidents de seguretat que hagin ocorregut relatius a la seguretat de la informació, amb el suport del Responsable del Sistema. |

### 4.1.3 Responsable del Sistema

| | |
|---|---|
| Responsable | Segons es determini al document de nomenaments |
| Funcions delegades | 1. Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar el seu correcte funcionament i operativitat.<br>2. Gestió, configuració i actualització, del maquinari i programari sota el seu àmbit de gestió en què es basen els mecanismes i serveis de seguretat del sistema. |

| | |
|---|---|
| | 3. Implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema que es trobi sota el seu àmbit de gestió.<br>4. Interlocució amb els proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS.<br>5. Assegurar que la traçabilitat, auditoria i altres registres de seguretat es duen a terme sovint, d'acord amb la política de seguretat establerta.<br>6. Establir procediments de seguiment i reacció davant incidències.<br>7. Donar d'alta nous rols d'accés als programes i aplicacions corporatives que es trobin sota el seu àmbit de gestió. |

### 4.1.4 Responsable dels Serveis

| | |
|---|---|
| Responsable | Segons es determini al document de nomenaments |
| Funcions delegades | 1. Definir els serveis necessaris per portar a terme les competències del Consorci.<br>2. Vetllar pel compliment de les polítiques i normes de seguretat determinades pel Consorci en el tractament dels fitxers de l'àmbit de responsabilitat. |

### 4.2 Procediments de designació

Els nomenaments dels membres de la Comissió de Seguretat, que assumeix les funcions de Responsable de Seguretat, i del Responsable del Sistema seran recollits al Decret de Nomenaments.

Si un servei es desenvolupa fora de l'àmbit competencial de la Comissió de Seguretat, l'àrea responsable del servei que es presti electrònicament haurà de designar el Responsable del Sistema, prèvia autorització i validació expressa de la Comissió de Seguretat.

## OBLIGACIONS DEL PERSONAL

Tots els membres del Consorci tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, i és responsabilitat del Responsable de Seguretat disposar dels mitjans necessaris per tal que la informació arribi als afectats.

Tots els membres del Consorci atendran a una sessió de conscienciació en matèria de seguretat TIC quan el Responsable de Seguretat ho estimi necessari. Igualment s'establirà un programa de conscienciació contínua per atendre tots els membres del Consorci.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessitin per realitzar-la. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

# TERCERES PARTS

Quan el Consorci presti serveis a altres organismes o gestioni 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 Responsables de Seguretat i s'establiran procediments d'actuació per a la reacció davant d'incidents de seguretat.

Quan el Consorci 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 pertoqui 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 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.

# GESTIÓ I DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta política s'ha de desenvolupar per mitjà de normativa de seguretat que afronti aspectes específics. La normativa de seguretat estarà a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per aquelles persones que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible a la unitat de servidor definida per als documents a compartir entre el personal del Consorci.

## 7.1 Revisió de la política de seguretat de la informació

Serà missió del Responsable de Seguretat la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa.



NIF: P-0800066 - C