Política de Seguretat sota l'Esquema Nacional de Seguretat

Índex de continguts

Versió	Data modificació	Data aprovació	Autor	Raó / Comentaris	Aprovat
1.0	28/10/2025	28/10/2025	Responsable de Seguretat	Edició inicial	Direcció

1. Exposició de Motius

El **Consell Català de la Producció Agrària Ecològica (CCPAE)**, com autoritat de control de Catalunya, la seva funció és auditar i certificar els productes agroalimentaris ecològics de Catalunya. El CCPAE és una corporació de dret públic amb personalitat jurídica pròpia. Aquest òrgan està tutelat administrativament pel Departament d'Agricultura, Ramaderia, Pesca i Alimentació (DARPA) de la Generalitat de Catalunya. Desenvolupa la seva activitat amb l'objectiu de garantir la continuïtat, qualitat i seguretat dels serveis que presta.

Les plataformes, sistemes i xarxes que suporten aquests serveis s'han de dissenyar, implementar i operar amb la màxima diligència, adoptant mesures adequades des de les fases inicials de concepció i disseny per protegir-los davant danys accidentals o atacs deliberats que puguin afectar la **disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat** de la informació i els serveis prestats.

L'objectiu de la **Seguretat de la Informació** a CCPAE és assegurar la **resiliència organitzativa**, preservar la **reputació corporativa**, garantir la **qualitat de la informació** i del programari o sistemes desplegats, així com mantenir la prestació continuada dels serveis crítics. Això s'aconsegueix actuant preventivament, supervisant de forma constant l'activitat diària i reaccionant amb rapidesa i eficàcia davant qualsevol incident.

Per fer front a les amenaces, CCPAE adopta una estratègia dinàmica capaç d'adaptar-se als canvis tecnològics, regulatoris i operatius de l'entorn. Això implica que tots els departaments han d'aplicar les mesures de seguretat exigides per l'**Esquema Nacional de Seguretat (ENS)**, fer un seguiment continu de la qualitat de les infraestructures i serveis, analitzar i corregir les vulnerabilitats detectades, i preparar respostes efectives davant incidents de seguretat.

Els diferents equips de l'organització vetllaran perquè la **seguretat TIC** sigui un component integral en totes les fases del cicle de vida dels sistemes: des de la concepció, el desenvolupament o adquisició, fins a l'operació i eventual retirada de servei. Els requisits de seguretat i els recursos necessaris per al seu finançament s'hauran d'identificar i incloure en la planificació, en les sol·licituds d'oferta i en els plecs de licitació de projectes TIC.

Així mateix, hauran d'estar preparats per **prevenir, detectar, reaccionar i recuperar-se** d'incidents, conforme a l'establert a l'**article 7 i** l'**article 8 de l'ENS**.

Per tot això, **CCPAE** compta amb un **Sistema de Gestió de la Seguretat de la Informació** basat en l **'Esquema Nacional de Seguretat**, que segueix un **cicle de millora contínua**.

Per a tot això, CCPAE compta amb un Sistema de Gestió de la Seguretat de la informació basat en l'Esquema Nacional de Seguretat que segueix un cicle de millora contínua

2. Missió

Donar una confiança absoluta al consumidor que el producte ecològic que compra compleix amb la reglamentació europea, amb un ferm compromís amb la protecció de la informació.

3. Abast

La present Política aplica als:

- **Servei de control i certificació de productes agroalimentaris ecològics de Catalunya**.

4. Marc Normatiu

Com a base normativa per realitzar la present política de seguretat, s'ha analitzat la legislació vigent, que afecta el desenvolupament de les activitats de l'Administració Local i Privada pel que fa a Administració electrònica, i que implica la implantació de forma explícita de mesures de seguretat en els sistemes d'informació. El marc legal en matèria de Seguretat de la Informació ve establert per la legislació següent:

- Llei 39/2015, de l'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 209/2003, de 21 de febrer, pel qual es regulen els registres i les notificacions telemàtiques, així com la utilització de mitjans telemàtics per a la substitució de l'aportació de certificats pels ciutadans.
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

I. Procediment Administratiu

- Llei 39/2015, de l'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.

II. Protecció de dades de caràcter personal

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el qual respecta el tractament de dades personals i la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
- Llei 3/2018, de 5 de desembre, de Protecció de Dades de Caràcter Personal i Garantia dels Drets Digitals.

III. Administració Electrònica

- 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.
- Reial Decret-Llei 14/1999, de 17 de setembre, sobre signatura electrònica, com a norma bàsica en aquesta matèria.
- Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell (Identificació electrònica i serveis de confiança per a les transaccions electròniques en el mercat interior)
- La Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

IV. Signatura Electrònica

- Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE.
- COM (2001) 298 - final, de la Comissió Europea - Seguretat de les xarxes i de la informació: Proposta per a un enfocament polític europeu.
- Llei 6/2020, de l'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

V. Seguretat de les Xarxes i de la informació

- Guies de l'OCDE per a la seguretat dels sistemes d'informació i xarxes. Cap a una cultura de seguretat. Com a complement a la legislació vigent, existeix en l'actualitat la norma internacional UNE ISO/IEC 27002 "Codi de Bones Pràctiques per a la gestió de la Seguretat de la Informació" que s'ha configurat com un estàndard en l'hora d'auditar els aspectes relacionats amb la Seguretat de la Informació en les organitzacions.

5. Organització de Seguretat

I. Comitè: Funcions i Responsabilitats

El Comitè de Seguretat és l'Òrgan que coordina la Seguretat de la Informació a nivell de l'Organització.

Estarà constituït pel responsable de Seguretat de la Informació i per representants d'altres àrees afectades per l'ENS.

Funcions associades

- Responsabilitats derivades del tractament de dades de caràcter personal.
- Assumpció de la figura de responsable de Servei per a tots els serveis prestats en el marc de la Llei 11/2007.
- Assumpció de la figura de responsable de la Informació per a totes les informacions emprades pels serveis prestats en el marc de la Llei 11/2007.

- Atendre les inquietuds dels Òrgans superiors competents i dels diferents departaments.
- Informar regularment de l'estat de la Seguretat de la Informació els Òrgans superiors competents.
- Promoure la millora contínua del Sistema de Gestió de la Seguretat de la Informació.
- Elaborar l'estratègia d'evolució de l'Organització quant a la Seguretat de la Informació.
- Coordinar els esforços de les diferents àrees en matèria de Seguretat de la Informació, per assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
- Elaborar (i revisar regularment) la Política de Seguretat de la Informació perquè sigui aprovada pels Òrgans superiors competents.
- Aprovar la Normativa de Seguretat de la Informació.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de Seguretat de la Informació.
- Monitoritzar els principals riscos residuals assumits per l'Organització i recomanar possibles actuacions al respecte.
- Monitoritzar l'acompliment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions al respecte. En particular, vetllar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de Seguretat de la Informació.
- Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Aprovar plans de millora de la Seguretat de la Informació de l'Organització, amb les seves dotacions pressupostàries corresponents. En particular, vetllarà per la coordinació de diferents plans que puguin realitzar-se en diferents àrees.
- Vetllar perquè la Seguretat de la Informació es tingui en compte en tots els projectes TIC 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.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents àrees de l'Organització, elevant aquells casos en els quals no tingui prou autoritat per decidir.
- El Comitè de Seguretat de la Informació no és un comitè tècnic, però, en cas d'ocurrència d'incidents de Seguretat recaptarà regularment del personal tècnic, propi o extern, la informació pertinent per prendre decisions.
- El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els quals hagi de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, podent materialitzar-se de diferents formes i maneres:
    - Grups de treball especialitzats, interns, externs o mixtos
    - Assessoria externa
    - Assistència a cursos o altres tipus d'entorns formatius o d'intercanvi d'experiències
- El Responsable de la Seguretat de la Informació és el secretari del Comitè de Seguretat de la Informació i com a tal:
    - Convoca les reunions del Comitè de Seguretat de la Informació.

- Prepara els temes a tractar en les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elabora l'acta de les reunions.
- És responsable de l'execució directa o delegada de les decisions del Comitè.

Composició del Comitè de Seguretat de la Informació:

Posició / Rol	Nom
Presidència	
Responsable de la Informació	
Responsable del Servei	
Responsable de Seguretat	
Responsable del Sistema	
Responsable de Protecció de Dades	
Administrador de la Seguretat del Sistema	

Presidència del Comitè de Seguretat de la Informació

El Gerent del CCPAE presideix el Comitè de Seguretat de la Informació. El seu President és la màxima autoritat en matèria de seguretat de la informació dins de l'organització.

Funcions i responsabilitats

- Presideix les reunions del Comitè.
- Supervisa l'acompliment del Comitè i l'execució dels seus acords. El President del Comitè té vot de qualitat en cas de desacords en el si del Comitè.
- Promou la seguretat de la informació com a prioritat estratègica.
- Garanteix l'assignació de recursos necessaris per al compliment de l'ENS.

Secretari del Comitè de Seguretat de la Informació

Com succeeix habitualment en el cas de l'ENS, el Responsable de Seguretat actuarà com a Secretari del Comitè de Seguretat de la Informació, amb les següents **funcions derivades**:

- Convocar les reunions del Comitè de Seguretat de la Informació, atenent les instruccions del president del Comitè.
- Preparar els temes que cal tractar en les reunions del Comitè, la informació dels diferents responsables.
- Elaborar l'acta de les reunions.
- Remetre l'acta de les reunions als assistents, recaptant la seva signatura.
- Conservar les actes, d'acord amb els criteris de conservació documental de CCPAE.

Definició de Rols

La Política de Seguretat, segons requereix l'Annex II de l'Esquema Nacional de Seguretat en la seva secció 3.1, ha d'identificar uns clars responsables per vetllar pel seu compliment i ser coneguda per tots els membres de l'organització Administrativa.
S'estableixen els següents rols en l'organització relacionats amb la Seguretat de la Informació.

II. Responsable de la Informació

Correspon a l'Òrgan de Govern de màxim nivell, constituït pels òrgans superiors competents, que entén la missió de l'organització, determina els objectius que es proposa aconseguir i respon que s'aconsegueixin.

Les seves funcions han estat assumides pel Comitè de Seguretat de la Informació i les persones que el componen són identificades en una acta generada per la nostra organització.

Funcions associades

- Té la responsabilitat última de l'ús que es faci d'una certa informació i, per tant, de la seva protecció.
- El responsable de la Informació delega en el Comitè de Seguretat com a responsable de qualsevol error o negligència que porti a un incident de confidencialitat o d'integritat.
- Estableix els requisits de la informació en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de Seguretat de la Informació.
- El responsable de la Informació delega en El responsable de cadascun dels Actius com a responsable de Determinar els nivells de seguretat en cada dimensió dins del marc establert en l'Annex I de l'Esquema Nacional de Seguretat.
- Encara que l'aprovació formal dels nivells correspongui al responsable de la Informació, podrà demanar una proposta del responsable de la Seguretat i del responsable del Sistema.

Compatibilitat amb altres rols

Aquest rol podrà coincidir amb el del Responsable de Servei.

Aquest rol no coincidirà amb el de Responsable de Seguretat (excepte en organitzacions de reduïda dimensió que funcionin de forma autònoma) i amb el de Responsable del Tractament requerit pel RGPD. Aquest rol no podrà coincidir amb el de Responsable de Sistema ni amb el d'Administrador de la Seguretat del Sistema, ni tan sols quan es tracti d'organitzacions de reduïda dimensió que funcionin de forma autònoma.

III. Responsable del Servei

Quan sigui diferent del responsable de la Informació, pot correspondre al nivell d'un Òrgan de Govern de màxim nivell, igual que el responsable de la Informació, o bé al d'una Direcció General, que entén què fa cada departament, i com que els departaments es coordinen entre si per aconseguir els objectius marcats pels Òrgans superiors competents.

Les seves funcions han estat assignades al Comitè de Seguretat de la Informació que al seu torn delega en el responsable de cadascun dels actius com a responsable de determinar els nivells de seguretat en cada dimensió dins del marc establert en l'Annex I de l'Esquema Nacional de Seguretat.

La persona o òrgan que l'assumeixi haurà de ser identificada per a cada Servei que presti l'organització.

Funcions associades

- Estableix els requisits dels serveis en matèria de seguretat. En el marc del
- ENS, equival a la potestat de determinar els nivells de Seguretat de la Informació.
- Té la responsabilitat última de l'ús que es faci de determinats serveis i, per tant, de la seva protecció.
- El responsable del servei és El responsable últim de qualsevol error o negligència que porti a un incident de disponibilitat dels serveis.
- Determinarà els nivells de seguretat en cada dimensió del servei dins del marc
- establert a l'Annex I de l'Esquema Nacional de Seguretat.
- Encara que l'aprovació formal dels nivells correspongui al responsable del Servei, podrà demanar una proposta del responsable de la Seguretat i del responsable del Sistema.
- La prestació d'un servei sempre ha d'atendre els requisits de Seguretat de la Informació que maneja, de manera que poden heretar els requisits de seguretat d'aquest, afegint requisits de disponibilitat, així com altres com accessibilitat, interoperabilitat, etc.

Compatibilitat amb altres rols

Podrà coincidir en la mateixa persona o òrgan el rol de Responsable de la Informació i del Responsable del Servei, encara que generalment no coincidiran quan:

- El servei gestioni informació de diferents procedències, no necessàriament de la mateixa unitat departamental que la que presta el servei.
- La prestació del servei no depengui de la unitat a la qual pertany El responsable de la Informació.
- Aquest rol podrà coincidir amb el del responsable de Servei i amb el de responsable de
- Fitxer requerit pel RGPD.
- Aquest rol no podrà coincidir amb el de responsable de Seguretat, excepte en organitzacions de reduïda dimensió que funcionin de forma autònoma.
- Aquest rol no podrà coincidir amb el de Responsable de Sistema ni amb el d'Administrador de la Seguretat del Sistema, ni tan sols quan es tracti d'organitzacions de reduïda dimensió que funcionin de forma autònoma.

IV. Responsable de Seguretat de la Informació

Ha estat nomenada formalment com a tal una única persona en l'organització mitjançant acta.

Funcions associades

- Reportarà directament al Comitè de Seguretat de la Informació.
- Actuarà com a secretari del Comitè de Seguretat de la Informació.
- Convocarà el Comitè de Seguretat de la Informació, recopilant la informació pertinent.

- Pertany al Comitè de Seguretat Corporativa, per coordinar les necessitats de Seguretat de la Informació en el marc de la resta de necessitats de Seguretat Corporativa.
- Mantindrà la Seguretat de la Informació emprada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, segons el que estableix en la Política de Seguretat de l'Organització.
- Promoure la formació i conscienciació en matèria de Seguretat de la Informació dins del seu àmbit de responsabilitat.
- Recopilarà els requisits de seguretat dels responsables d'Informació i del Servei i determinarà la categoria del Sistema.
- Realitzarà l'Anàlisi de Riscos.
- Elaborarà una Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides conforme a l'Annex II de l'ENS i del resultat de l'Anàlisi de Riscos.
- Facilitarà als responsables d'Informació i als Responsables de Servei, informació sobre el nivell de risc residual esperat després d'implementar les opcions de tractament seleccionades en l'anàlisi de riscos i les mesures de seguretat requerides per l'ENS.
- Coordinarà l'elaboració de la Documentació de Seguretat del Sistema.
- Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per a la seva aprovació per la Direcció.
- Participarà en l'elaboració i aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de Seguretat de la Informació.
- Elaborarà i aprovarà els Procediments Operatius de Seguretat de la Informació.
- Facilitarà periòdicament al Comitè de Seguretat un resum d'actuacions en matèria de seguretat, d'incidents relatius a Seguretat de la Informació i de l'estat de la seguretat del sistema (en particular del nivell de risc residual al qual està exposat el sistema).
- Elaborarà, juntament amb els responsables de Sistemes, Plans de Millora de la Seguretat, per a la seva aprovació pel Comitè de Seguretat de la Informació.
- Elaborarà els Plans de Formació i Conscienciació del personal en Seguretat de la Informació, que hauran de ser aprovats pel Comitè de Seguretat de la Informació.
- Validarà els Plans de Continuïtat de Sistemes que elabori El responsable de Sistemes, que hauran de ser aprovats pel Comitè de Seguretat de la Informació i provats periòdicament pel responsable de Sistemes.
- Aprovarà les directrius proposades pels responsables de Sistemes per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis.

En cas d'ocurrències d'incidents de seguretat de la informació

Analitzarà i proposarà salvaguardes que previnguin incidents similars en un futur.

Compatibilitat amb altres rols

Aquest rol únicament podria arribar a coincidir amb la del Responsable de Servei i el Responsable d'Informació en organitzacions de reduïdes dimensions que tinguin una estructura autònoma de funcionament.

Aquest rol no coincidirà amb el de Responsable de Sistema ni amb el d'Administrador de Seguretat del Sistema.

Delegació de funcions

En situació que el nostre Sistema d'Informació adquirís una major complexitat, distribució, separació física dels seus elements o nombre d'usuaris es necessiti de personal addicional per dur a terme les funcions de responsable de la Seguretat, es podran designar els Responsables de Seguretat Delegats que es considerin necessaris. La designació correspon al responsable de la Seguretat. Per mitjà de la designació de delegats, es deleguen funcions. La responsabilitat final seguirà recaient sobre El responsable de la Seguretat.

Els responsables de Seguretat Delegats es faran càrrec, en el seu àmbit, de totes aquelles accions que delegui el/la responsable de la Seguretat, podent ser, per exemple, la seguretat de sistemes d'informació concrets o de sistemes d'informació horitzontals.

Cada responsable de Seguretat Delegat tindrà una dependència funcional directa del responsable de la Seguretat, que és a qui reporten.

La delegació de funcions passarà prèviament pel comitè.

V. Responsable del Sistema

Correspon al nivell d'una Direcció Operativa.

Es nomena formalment com a tal una única persona per a cada Sistema. El rol no serà desenvolupat per un òrgan col·legiat, encara que pugui delegar part de les seves funcions en altres persones

Funcions associades

- Desenvolupar, operar i mantenir el Sistema d'Informació durant tot el seu cicle de vida, de les seves especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i sistema de gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en el mateix.
- Cerciorar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- El responsable del Sistema pot acordar la suspensió de l'ús d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que poguessin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els responsables de la Informació afectada, del Servei afectat i amb El responsable de la Seguretat abans de ser executada.
- Aplicar els procediments operatius de seguretat elaborats i aprovats pel responsable de Seguretat.

- Monitoritzar l'estat de la seguretat del Sistema d'Informació i reportar-lo periòdicament, o davant d'incidents de seguretat rellevants, al responsable de Seguretat de la Informació.
- Elaborar els Plans de Continuïtat del Sistema que seran validats pel responsable de Seguretat de la Informació, i coordinats i aprovats pel Comitè de Seguretat de la Informació.
- Realitzar exercicis i proves periòdiques dels Plans de Continuïtat del Sistema per mantenir-los actualitzats i verificar que són efectius.
- Elaborarà les directrius per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos (especificació, arquitectura, desenvolupament, operació i canvis) i les facilitarà al responsable de Seguretat de la Informació per a la seva aprovació.
- Planificarà la implantació de les salvaguardes en el sistema.

En cas d'ocurrència d'incidents de seguretat de la informació

Supervisarà les accions de mitigació d'impacte i restauració de les operacions d'acord amb els plans aprovats.

Compatibilitat amb altres rols

Aquest rol no coincidirà amb el de Responsable d'Informació o amb el de Responsable del Servei.

No obstant això, aquest rol podria coincidir amb el d'Administrador de Seguretat del Sistema en organitzacions d'una dimensió reduïda o mitjana que tinguin una estructura autònoma de funcionament.

VI. Administrador de la Seguretat del Sistema

Correspon al nivell d'un empleat qualificat en seguretat informàtica de sistemes. Es nomena formalment com a tals l'equip d'IT.

El rol no es desenvoluparà per un òrgan col·legiat ni delegarà part de les seves funcions en altres persones.

Si s'escau, es nomenarien nous Administradors de la Seguretat del Sistema en cas que s'incrementi la mida de CCPAE.

Serà proposat pel responsable del Sistema, a qui reportarà en tot el relacionat amb Seguretat de la Informació.

Funcions associades

- La implementació, gestió i manteniment de les mesures de seguretat aplicables al Sistema d'Informació.
- Assegurar que els controls de seguretat establerts són complerts estrictament.
- Assegurar que la traçabilitat, pistes d'auditoria i altres registres de seguretat requerits es trobin habilitats i registrin amb la freqüència desitjada, d'acord amb la política de seguretat establerta per l'Organització.
- Aplicar als Sistemes, usuaris i altres actius i recursos relacionats amb aquest, tant interns com externs, els procediments operatius de Seguretat i els mecanismes i serveis de seguretat requerits.
- Assegurar que són aplicats els procediments aprovats per manejar el Sistema d'informació i els mecanismes i serveis de seguretat requerits.

- La gestió, configuració i actualització, si escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat del Sistema d'Informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa.
- Verificar el correcte funcionament dels Sistemes d'Informació després de la realització de canvis en les configuracions vigents, garantint que segueixin operatius els mecanismes i serveis de **seguretat** habilitats.
- Informar els responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Monitoritzar l'estat de la seguretat del sistema.

En cas d'ocurrència d'incidents de seguretat de la informació

- Dur a terme el registre, comptabilitat i gestió dels incidents de seguretat en els Sistemes sota la seva responsabilitat.
- Executar el Pla de Seguretat aprovat.
- Aïllar l'incident per evitar la propagació a elements aliens a la situació de risc.
- Prendre decisions a curt termini si la informació s'ha vist compromesa de tal manera que pogués tenir conseqüències greus (aquestes actuacions haurien d'estar documentades per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Assegurar la integritat dels elements crítics del Sistema si s'ha vist afectada la disponibilitat en els mateixos (aquestes actuacions quedaran documentades per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).
- Mantenir i recuperar la informació emmagatzemada pel Sistema i els seus serveis associats.
- Investigar l'incident: Determinar la manera, els mitjans, els motius i l'origen de l'incident.

Compatibilitat amb altres rols

Aquest rol no coincidirà amb el de Responsable d'Informació, amb el de responsable de Servei ni amb el de responsable de Seguretat Corporativa o de la Informació.

Delegació de funcions

En cas que el nostre sistema d'informació augmentés la seva complexitat, distribució, separació física dels seus elements o nombre d'usuaris requereixin de personal addicional per dur a terme les seves funcions, es podran designar Administradors de Seguretat del Sistema delegats.

Els Administradors de Seguretat del Sistema delegats seran responsables, en el seu àmbit, d'aquelles accions que delegui l'Administrador de Seguretat del Sistema relacionades amb la implantació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació.

L'Administrador de Seguretat del Sistema delegat serà designat a petició de l'Administrador de Seguretat del Sistema, del qual dependrà funcionalment.

La delegació de funcions passarà prèviament pel comitè.

La seva identitat apareixerà reflectida en la documentació de seguretat del sistema d'informació.

VII. Responsable en matèria de protecció de dades

A CCPAE confiem a oferir totes les garanties necessàries de seguretat de la informació. L'organització te nomenat un Delegat de Protecció de Dades.

Designació o no d'un delegat de protecció de dades

Segons el que estableix l'article 37 del RGPD, el responsable i l'encarregat del tractament han de designar un Delegat de Protecció de Dades sempre que:

- el tractament el dugui a terme una autoritat o organisme públic, excepte els tribunals que actuïn en exercici de la seva funció judicial;
- les activitats principals del responsable o de l'encarregat consisteixin en operacions de tractament que, a causa de la seva naturalesa, abast i/o finalitats, requereixin una observació habitual i sistemàtica d'interessats a gran escala, o
- les activitats principals del responsable o de l'encarregat consisteixin en el tractament a gran escala de categories especials de dades personals d'acord amb l'article 9 i de dades relatives a condemnes i infraccions penals a què es refereix l'article 10.

Funcions

Segons el que estableix l'article 39 del RGPD:

El delegat de Protecció de Dades tindrà com a mínim les següents funcions:

a) informar i assessorar el responsable o l'encarregat del tractament i els empleats que s'ocupin del tractament, de les obligacions que els incumbeixen en virtut d'aquest Reglament i altres disposicions de protecció de dades de la Unió o dels estats membres.
b) supervisar el compliment del que disposa el present Reglament, altres disposicions de protecció de dades de la Unió o dels Estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
c) oferir l'assessorament que se li demani sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar la seva aplicació de conformitat amb l'article 35 del reglament.
d) cooperar amb l'autoritat de control.
e) actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36 del reglament, i realitzar consultes, si s'escau, sobre qualsevol altre assumpte.

Així mateix, segons el RGPD, la posició del DPO/DPD comporta per a nosaltres:

- La participació de forma adequada i en temps oportú en totes les qüestions relatives a la protecció de dades personals.
- Rebre el suport del responsable o encarregat, que li hauran de facilitar els recursos necessaris per al compliment de les seves funcions.

- No rebre cap instrucció quant a l'exercici d'aquestes funcions i no ser destituït ni sancionat pel responsable o l'encarregat per causes relacionades amb aquest exercici de funcions.
- Retre comptes directament al més alt nivell jeràrquic del responsable o encarregat.
- Aquesta característica s'ha d'interpretar en el sentit que el DPD s'ha de poder relacionar amb nivells jeràrquics que tinguin la capacitat d'adoptar o promoure decisions basades en les recomanacions, propostes o avaluacions que realitzi el DPD.

6. Dades de caràcter personal

CCPAE tracta dades de caràcter personal.

Disposem d'un Registre d'Activitats del Tractament (RAT) on es recullen els fitxers afectats i els corresponents responsables. Tots els sistemes d'informació de CCPAE s'ajustaran als nivells de seguretat requerits per la normativa, a fi i efecte, de la naturalesa i finalitat de les dades de caràcter personal recollides.

7. Gestió de riscos

Justificació

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

L'anàlisi de riscos serà la base per determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establerts per l'Esquema Nacional de Seguretat, segons el previst a l'article 7 de l'ENS.

Criteris d'Avaluació de Riscos

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

Els criteris d'avaluació de riscos detallats s'especificaran en la metodologia d'avaluació de riscos que elaborarà l'organització, basant-se en estàndards i bones pràctiques reconegudes.

Hauran de tractar-se, com a mínim, tots els riscos que puguin impedir la prestació dels serveis o el compliment de la missió de l'organització de forma greu.

Es prioritzaran especialment els riscos que impliquin un cessament en la prestació dels serveis prestats.

Directrius de tractament

El Comitè de Seguretat de la Informació dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

Procés d'acceptació del Risc Residual

Els riscos residuals seran determinats pel responsable de Seguretat de la Informació. Els nivells de risc residual esperats sobre cada Informació després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II de l'ENS) hauran de ser acceptats prèviament pel responsable d'aquesta Informació.

Els nivells de risc residuals esperats sobre cada Servei després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes en l'Annex II de l'ENS) i hauran de ser acceptats prèviament pel responsable d'aquest Servei.

Els nivells de risc residuals seran presentats pel responsable de Seguretat de la Informació al Comitè de Seguretat de la Informació, perquè aquest procedeixi, si escau, a avaluar, aprovar o rectificar les opcions de tractament proposades.

Necessitat de realitzar o actualitzar avaluacions de riscos

L'anàlisi dels riscos i el seu tractament ha de ser una activitat repetida regularment, conforme el que estableix a l'article 7 de l'ENS. Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada l'any.
- Quan es produeixin canvis significatius en la informació manejada.
- Quan es produeixin canvis significatius en els serveis prestats.
- Quan es produeixin canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.
- Quan s'esdevingui un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

8. Gestió d'incidents de seguretat

Prevenció

Els departaments han d'evitar, o almenys prevenir en la mesura del possible, que la informació i els serveis prestats es vegin perjudicats per incidents de seguretat. L'ENS, a través del seu article 19 estableix que els sistemes s'han de dissenyar i configurar de manera que garanteixin la seguretat per defecte, en línia amb la política de mínim privilegi "*Need to Know*". De la mateixa manera, l'article 17 de l'esmentat ENS defineix que els sistemes s'instal·laran en àrees separades, dotades d'un procediment de control d'accés.

Per a la qual cosa els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per garantir el compliment de la política, els departaments han de:

- Establir àrees segures per als sistemes d'informació crítica o confidencial.
- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració realitzats de forma rutinària.

- Demanar la revisió periòdica per part de tercers per tal d'obtenir una avaluació independent.

Detecció

Atès que els sistemes es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració de les operacions fins a la seva detenció, s'han d'establir mecanismes de monitoratge continu per detectar anomalies en els nivells de prestació d'aquests servei, així com canvis o accessos no autoritzats a l'entorn digital i actuar en conseqüència segons el que estableix l'article 8 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 9 de l'ENS. S'establiran mecanismes de detecció, anàlisi i report que arribin als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

Els sistemes de detecció d'intrusos, tant a nivell de xarxa com de sistema, compleixen fonamentalment amb una tasca de supervisió i auditoria sobre els recursos de l'Organització, verificant que la política de seguretat no és violada i intentant identificar qualsevol tipus d'activitat maliciosa d'una forma primerenca i eficaç.

Resposta

CCPAE, a través dels seus diferents departaments:

- Estableix mecanismes per respondre eficaçment als incidents de seguretat.
- Designa un punt únic de contacte per a les comunicacions quant a incidents detectats dins de l'organització o bé a aquells que afectin altres organismes.
- Estableix protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en ambdós sentits, amb els Equips de Resposta a Emergències (CERT)

Recuperació

Per garantir el correcte restabliment dels serveis, CCPAE desenvolupa Plans de Continuïtat dels sistemes TIC com a part del seu Pla General de Continuïtat de Negoci i les corresponents activitats de recuperació.

9. Obligacions del personal

Tots els membres de l'Organització tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, és responsabilitat del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi als afectats.

El compliment de la present Política de Seguretat és obligatori per part de tot el personal intern o extern que intervingui en els processos de l'organització, constituint el seu incompliment, infracció greu a efectes laborals, conforme al conveni col·lectiu d'oficines i despatxos de la província de Barcelona.

10. Formació i conscienciació

L'objectiu de CCPAE és conscienciar de forma contínua als empleats sobre la importància de la ciberseguretat, per a això es realitza:

- Formació inicial a la incorporació dels empleats a l'organització.
- Enviament periòdic de píndoles de conscienciació en ciberseguretat.
- Enviament periòdic de píndoles informatives de ciberseguretat, responent a situacions de risc.
- Formació anual a tot el personal d'actualització en ciberseguretat.
- Formació específica segons el lloc de treball i necessitats concretes.

La Direcció es compromet a la formació i conscienciació del personal de CCPAE.

11. Terceres Parts

A CCPAE adquirim un especial compromís:

- Quan es prestin serveis o es gestioni informació d'altres organitzacions, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals de report i coordinació dels respectius Comitès de Seguretat de la Informació i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.
- Quan s'utilitzin serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que concerneixi aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la.
- S'establiran procediments específics de report i resolució d'incidències.
- Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que estableix 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.

12. Revisió i aprovació de la Política de Seguretat

La Política de Seguretat de la Informació serà revisada pel Comitè de Seguretat de la Informació a intervals planificats, que no podran excedir l'any de durada, o sempre que es produeixin canvis significatius, a fi d'assegurar que es mantingui la seva idoneïtat, adequació i eficàcia.

Els canvis sobre la nostra Política de Seguretat de la Informació seran aprovats per l'òrgan superior competent que correspongui, d'acord amb l'article 11, en el Capítol III Article 12 de l'ENS, en el nostre cas és aprovada per la direcció general mitjançant acta.

Qualsevol canvi sobre la mateixa haurà de ser difós a totes les parts afectades.

La Política de Seguretat està Notificada, Comunicada i disponible per a tot el personal de CCPAE.

13. Categoria de seguretat del sistema

La categoria de seguretat requerida és **MITJA**, dins del marc establert a l'article 40 i els criteris generals prescrits a l'Annex I del RD 311/2022 (ENS). Alguns dels criteris que determinen aquest nivell és que el procés està totalment definit. El catàleg de processos es manté actualitzat i garanteixen la consistència de les actuacions entre les diferents parts de l' organització.

Es disposa de normativa i procediments per a poder reaccionar davant qualsevol incident de seguretat, quina s'actualitza i manté de forma regular. Així mateix, hi ha una alta coordinació entre departaments i els projectes duts a terme.

El Comitè de Seguretat de la Informació preveu la possibilitat de modificar el nivell de seguretat requerit.

Els principis de la Política de Seguretat de la Informació són assumits i impulsats per la Direcció, qui proporciona els mitjans necessaris i dota els empleats dels recursos suficients per al seu compliment, plasmant-se i posant-los en coneixement públic mitjançant la present política.

14. Aprovació de la Política i entrada en vigor

Les modificacions de la present Política les realitzarà el Comitè de Seguretat de la Informació, que l'haurà de revisar anualment.

En cas de canvis substancials o dels principis o responsabilitats designades, el Comitè proposarà els canvis que hauran de ser aprovats, si s'escau, per la persona o òrgan amb les degudes competències.

La substitució de la Política serà instada pel Comitè de Seguretat de la Informació i ratificada per la persona o òrgan amb les degudes competències, de la qual cosa s'informarà adequadament els interessats pels mateixos canals usats per a la seva difusió.

Direcció
Data: 28/10/2025