Consorci
Administració Oberta
de Catalunya

Política de seguretat

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

Realitzat per: Comitè operatiu de Seguretat

Versió: 3.0

Data: 29/11/2022

Índex

1 Control del document

1.1 Informació General

Títol	Política de Seguretat
Versió	3.0
Elaborat per	Comitè Operatiu
Revisat per	Comitè Executiu que ho eleva a la comissió Executiva per a la seva aprovació
Aprovat per	Comissió Executiva el dia 21 de desembre de 2022
Nom del Fitxer	PDS_ Política de Seguretat 3.0.docx

1.2 Llista de Distribució

	Organització
Personal del Consorci AOC	Intranet

1.3 Històric de canvis

Data	Aprovació	Raó de la modificació
30/04/2015	Comissió Executiva	Versió 1.0
29/04/2017	Comissió Executiva	Versió 1.1. Revisió i actualització.
18/03/2020	Comissió Executiva	Versió 2.0 Revisió i actualització.
06/05/2022	Comissió Executiva	Versió 2.1 Canvi en quan s'han de fer nous anàlisi de riscos
29/11/2022	Comissió Executiva	Versió 3.0 Actualització del marc normatiu de referència, canvis en la periodicitat de les reunions

Data	Aprovació	Raó de la modificació
		ordinàries dels comitès Operatiu i Executiu i canvis en la repetició d'anàlisis de riscos en cas de vulnerabilitats

2 Introducció

La Informació és un dels actius més importants per a una organització i per tant, s'ha de protegir adequadament independentment de la forma que prengui o els mitjans pels quals es transmeti, emmagatzemi o processi.

El Consorci Administració Oberta de Catalunya (d'ara en endavant Consorci AOC), conscient de la importància i del valor de la informació que tracta i com a prestador de serveis fonamentals per a l'operativitat dels diferents i diversos ens als quals dóna suport, garanteix la disponibilitat, integritat, traçabilitat, confidencialitat i autenticitat de la informació tractada i del serveis prestats, actuant preventivament, supervisant l'activitat diària i reaccionant ràpidament als incidents, per recuperar els serveis lo abans possible d'acord l'establert en l'article 8 de l'Esquema Nacional de Seguretat (en endavant, ENS) , amb l'aplicació de les mesures que es relacionen a continuació i al marc normatiu de ciberseguretat de l'Agència de Ciberseguretat de Catalunya:

Prevenció

Per tal que la informació i/o els serveis no es vegin perjudicats per incidents de seguretat, el Consorci AOC implementa les mesures de seguretat de l'ENS i del Marc de Ciberseguretat de l'Agència de Ciberseguretat de Catalunya, així com controls addicionals identificats mitjançant l'avaluació d'amenaces i riscos. Aquests controls, els rols, i responsabilitats de seguretat de tot el personal, estan clarament definits i documentats.

Per garantir l'acompliment de la política el Consorci:

- Autoritzar tots els sistemes abans d'estar operatius.
- Avaluar regularment la seguretat, incloent avaluacions de canvis de configuracions.
- Sol·licitar la revisió periòdica per part de tercers. Avaluació independent.

Detecció

El Consorci AOC, estableix controls d'operació dels seus sistemes d'informació amb l'objectiu de detectar anomalies en la prestació dels serveis i actuar en conseqüència segons el que es disposa en l'article 10 del ENS (vigilància contínua i reavaluació periòdica). Quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals (conforme a l'indicat en l'article 9 del ENS, Existència de línies de defensa), s'establiran els mecanismes de detecció, anàlisi i reporti necessaris perquè arribin als responsables regularment.

Resposta

S'han de:

- Establir mecanismes de resposta eficaç per incidents de seguretat.

- Designar un punt de contacte per les comunicacions respecte a incidents detectats internament o reportats per altres organismes.
- Establir protocols per a intercanvis d'informació amb l'incident. Això inclou les comunicacions en ambdós sentits, amb els Equips de Resposta a Emergències (CERT).

Recuperació

Per a garantir la disponibilitat dels serveis crítics. El Responsable de Seguretat de la informació ha de desenvolupar plans de continuïtat dels sistemes TIC com a part del pla general de continuïtat del negoci i activitats de recuperació.

3 Missió del Consorci AOC

La missió de l'AOC és impulsar la transformació digital de les administracions catalanes, de conformitat amb els objectius i funcions establerts als seus estatuts.

4 Marc Normatiu de Referència

El marc normatiu en que es desenvolupen les activitats del Consorci AOC, i en particular, la prestació dels seus serveis electrònics està integrat per les següents normes:

- Estatuts del Consorci Administració Oberta de Catalunya.
- Normativa europea, estatal i catalana reguladora de:
  - del règim jurídic i del procediment administratiu comú.
  - de la protecció de dades de caràcter personal.
  - de la seguretat de la informació
- Normativa sectorial específica referenciada en cadascuna de les condicions reguladores de la prestació de serveis oferts pel Consorci.
- Qualsevol altre normativa aprovada pel Consorci AOC.

Aquesta Política de Seguretat i qualsevol altra normativa específica de seguretat elaborada pel Consorci AOC, s'haurà de mantenir actualitzada i adaptada a la normativa aplicable en matèria de seguretat, si s'escau, i al Marc Normatiu de Seguretat impulsat pel l'Agència de Ciberseguretat de Catalunya vigent a la Generalitat de Catalunya en cada moment.

5 Política de seguretat

5.1 Objectiu

L'objectiu de la present Política de Seguretat és establir el conjunt de directrius que regeixen la forma com el Consorci AOC gestiona i protegeix la informació que tracta i els serveis que presta.

5.2 Àmbit de l'Aplicació

Aquesta Política s'aplicarà als sistemes d'informació del Consorci AOC, relacionats amb l'exercici de les seves competències i a tots els usuaris amb accés autoritzat a aquests, siguin o no treballadors del Consorci AOC i amb independència de la naturalesa de la seva relació jurídica amb el Consorci AOC.

Tots els usuaris tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la seva Normativa de Seguretat derivada, sent responsabilitat del Comitè Executiu de Seguretat del Consorci AOC disposar els mitjans necessaris perquè la informació arribi al personal. Cada responsable de contracte és responsable de traslladar la informació a les empreses proveïdores per al seu compliment i trasllat al personal adscrit amb accés las sistemes d'informació del Consorci.

5.3 Organització de la Seguretat

Es crea l'estructura organitzativa de seguretat del Consorci és:

5.3.1 Comissió Executiva del Consorci AOC

La Comissió Executiva és l'òrgan col·legiat de direcció executiva del Consorci AOC i està formada per sis membres, dels quals quatre ho són en representació de l'Administració de la Generalitat i dos en representació del Consorci Localret.

El director gerent del Consorci AOC assisteix a les reunions, amb veu però sense vot.

Correspon a la Comissió Executiva en matèria de seguretat:

- Aprovar la Política de Seguretat i les normes en matèria de Seguretat de la Informació i dotar al Consorci dels mitjans personals i materials necessaris per a la seva efectiva implantació i execució.

5.3.2 Comitè Executiu de Seguretat de la Informació del Consorci AOC

El Comitè Executiu de Seguretat coordinarà i centralitzarà tots els esforços sobre les decisions de seguretat, polítiques, normes, anàlisis de riscos, plans de

continuïtat de serveis, recuperació de desastres, etc., assegurant en tot moment l'alineació amb l'estratègia de seguretat definida.

Aquest Comitè estarà format per:

- Director Gerent del Consorci AOC, que és alhora responsable del tractament de les dades de caràcter personal i que actuarà com a President
- Subdirector/s del Consorci AOC.
- Caps d'Àrea del Consorci AOC.
- Responsable de Seguretat de la Informació.

El Secretari del Comitè Executiu de Seguretat serà el Responsable de Seguretat de la Informació.

El Comitè Executiu estarà integrat per les persones que en cada moment ostentin el càrrec o càrrecs que el composen i la seva durada coincidirà amb el càrrec que ocupa.

El Comitè Executiu de Seguretat reportarà a la Comissió Executiva del Consorci AOC.

Les funcions del Comitè Executiu seran:

- Presentar a l'aprovació de la Comissió Executiva la Política de Seguretat i les normes en matèria de Seguretat de la Informació.
- Identificar objectius i estratègies relacionades amb la seguretat.
- Donar suport al Comitè Operatiu i als seus membres, dotar-lo dels recursos necessaris i establir les seves directrius de treball.
- Revisar la implantació de la política de seguretat.
- Aprovar els plans d'implementació i assignar els recursos necessaris.
- Vigilar que les mesures de la política planificades són implantades tal com s'havia previst i donen els resultats esperats.
- Aprovar el pla de formació i conscienciació dels usuaris i liderar la comunicació necessària.
- Aprovar els procediments de seguretat així com les seves posteriors modificacions.
- Assumir les funcions de responsable del servei en matèria de Seguretat de la informació. Te la potestat de determinar els nivells de seguretat dels serveis.
- Assumir les funcions de responsable d'informació. Te la responsabilitat última de l'ús que es faci d'una certa informació i, per tant, de la seva protecció. I també de qualsevol error o negligència que porti a un incident de confidencialitat o d'integritat. Estableix el requisits de la informació en matèria de seguretat.

- Assignar dins del Consorci AOC aquells rols i funcions en matèria de Seguretat de la Informació que no estiguin definits a la present Política de Seguretat.
- Aprovar el Pla d'acció en matèria de Seguretat de la Informació del Consorci AOC. Supervisar i fer el seguiment de la seva implantació.
- Supervisar i aprovar els Plans de Continuïtat de Negoci.
- Vetllar pel compliment de la legislació que en matèria de seguretat sigui d'aplicació.
- Supervisar els incidents de seguretat.
- Fer seguiment del Quadre de Comandament de la Seguretat de la Informació del Consorci AOC.
- En casos de desastres naturals, incidents greus del servei o altres esdeveniments que afectin al funcionament i/o l'Organització del Consorci AOC de forma severa, el Comitè Executiu actuarà com a Comitè de Crisis i nomenarà als membres que actuaran en el seguiment de la crisis.
- A proposta dels Caps de Servei, aprovar la categorització dels sistemes dins el marc del que preveuen els annexos de l'Esquema Nacional de Seguretat.
- Acceptar els nivells de riscs residuals que afecten a la informació i als serveis.
- L'aprovació, a proposta del Responsable de Seguretat, de les mesures tècniques i organitzatives i operacionals apropiades per garantir un nivell de seguretat adequat al risc pels sistemes d'informació i per als drets i llibertats de les persones, tenint en compte l'estat de la tècnica, els costos d'aplicació, i la naturalesa, l'abast, el context i les finalitats del tractament, d'acord amb el que exigeix el Reglament General de Protecció de Dades (en Endavant RGPD), la LLei Orgànica de Protecció de Dades de Caràcter (en endavant, LLOPDiGDD) i l'ENS.

Les reunions ordinàries seran cada 12 mesos i es realitzarà l'avaluació i revisió de la situació del Consorci AOC respecte a la Seguretat de la Informació i s'estudiaran les propostes de seguretat a abordar.

A les reunions del Comitè Executiu de Seguretat es convocarà al Delegat de protecció de dades quan s'adoptin decisions amb afectació a dades de caràcter personal i altres persones (membres del Comitè Operatiu de Seguretat, experts en matèria de Seguretat, juristes...) prèvia invitació del President.

5.3.3 Responsable de Seguretat de la Informació del Consorci AOC

El responsable de Seguretat de la Informació es responsabilitzarà de:

- Mantenir la Seguretat de la Informació gestionada i dels serveis prestats pels sistemes d'informació, així com de fer complir la Política de Seguretat del Consorci AOC.
- Supervisar la implantació de les polítiques, normes, guies i procediments de seguretat establerts en el Consorci AOC i de promoure la formació i conscienciació en matèria de Seguretat de la Informació.
- Coordinar les accions orientades a garantir la Seguretat de la Informació en qualsevol de les seves formes (digital, òptica, paper, ...) i en tot el seu cicle de vida (creació, manteniment, distribució, emmagatzematge i destrucció), per protegir la informació en termes de confidencialitat i privacitat, integritat, disponibilitat, autenticitat i traçabilitat.
- Proporcionar recolzament en matèria de seguretat a totes les àrees del Consorci AOC, realitzar el seguiment de l'estat dels incidents de seguretat ocorreguts, assegurar el compliment de les polítiques, normes, guies i procediments de seguretat, etc.

  Són funcions del responsable de Seguretat de la Informació les següents:

  - Assessorar al **Comitè Executiu de Seguretat**.
  - Definir les funcions i responsabilitats associades a la seguretat dels sistemes d'informació.
  - Gestionar i solucionar els incidents de seguretat de la informació, conjuntament amb el Comitè Executiu de Seguretat.
  - Definir i desenvolupar la normativa de seguretat i formació en aspectes relatius a la Seguretat de la Informació.
  - Encomanar la realització dels Anàlisi de Riscos pels sistemes d'informació i pel drets i llibertats dels titulars de les dades de caràcter personal, així com identificar mancances i debilitats i posar-les en coneixement de Comitè Executiu
  - Promoure plans de contingència i formació en aspectes relatius a la Seguretat de la Informació.
  - Dirigir i coordinar les tasques realitzades del **Comitè Operatiu de Seguretat.**
  - Supervisar i controlar internament el compliment de la Política de Seguretat del Consorci AOC, les diferents normatives i procediments de seguretat establerts dins de l'Organització.
  - Presentar a l'aprovació del Comitè Executiu les polítiques, normes i responsabilitats en matèria de Seguretat de la Informació.

- Elaborar el pla de formació i conscienciació dels usuaris.
- Donar compte al Comitè Executiu de les incidències de seguretat.
- Crear grups específics de treball, de caràcter temporal, que desenvolupin funcions específiques delegades i dirigides pel Responsable de Seguretat de la Informació.
- Elaborar el Quadre de Comandament de Seguretat de la Informació del Consorci AOC i informar al Comitè Executiu.
- Vetllar pel compliment normatiu, coordinant actuacions amb les unitats responsables que corresponguin.
- Aprovar la declaració d'aplicabilitat
- Analitzar els informes d'autoavaluació i/o els informes d'auditoria i elevar-ne les conclusions al responsable del sistema perquè adopti les mesures correctores oportunes
- Elevar al Comitè Executiu la proposta d'aprovació de les mesures tècniques, organitzatives i operacionals apropiades per garantir un nivell de seguretat adequat al risc pels sistemes d'informació i per als drets i llibertats de les persones.
- Participar en les Avaluacions d'Impacte de Protecció de Dades de caràcter personal.

5.3.4 Comitè Operatiu de Seguretat de la Informació del Consorci AOC

El Comitè Operatiu de Seguretat, és un òrgan de suport i assessorament al Responsable de Seguretat de la Informació.

Aquest Comitè estarà format per:

- Responsable de Seguretat de la Informació, que actuarà com a president.
- Responsable del Sistema del Consorci AOC.
- Responsable d'assessorament jurídic intern
- El Delegat de Protecció de Dades.

El Responsable de Seguretat, proposarà a Direcció Gerència el nomenament d'altres membres permanents.

El Responsable de Seguretat podrà invocar la presència puntual a les seves reunions de personal del Consorci o d'experts externs per raó de la seva experiència o vinculació amb els assumptes tractats.

Les funcions del Comitè Operatiu seran:

- Donar suport al Responsable de la Seguretat de la Informació en:
  - La definició del model de seguretat del Consorci AOC
  - Seguiment del compliment de la política de Seguretat del Consorci AOC.

- L'elaboració de la normativa interna de Seguretat, les polítiques i procediments de seguretat.
- Seguiment del compliment de les normatives internes de seguretat de la informació.
- Assistir al Cap del Servei en la categorització dels sistemes d'informació, i al Responsable de Seguretat en els anàlisi de riscos i les avaluacions d'impacte de protecció de dades de caràcter personal.
- L'elaboració del pla de formació i conscienciació dels usuaris.
- El desenvolupament i manteniment del Pla de Continuïtat de Negoci en els serveis que ho requereixen.
- L'elaboració del Quadre de Comandament de Seguretat de la Informació del Consorci AOC.
- Seguiment del compliment normatiu, coordinant actuacions amb les unitats responsables que corresponguin.

Les reunions ordinàries seran cada 3 mesos i es realitzarà seguiment i revisió de la situació del Consorci AOC respecte a la seguretat de la informació.

5.3.5 Responsable de Sistema del Consorci AOC

El responsable de sistema es responsabilitzarà de desenvolupar, operar i mantenir el Sistema d'informació, durant tot el seu cicle de vida, les seves especificacions, instal·lació i verificació del seu correcte funcionament.

Aquest càrrec pot ser assumit per un Cap d'unitat, Cap de Projecte i/o Responsable de Servei.

Són funcions del responsable de sistema:

Definir la topologia i sistema de gestió d'informació, establint els criteris d'us i els serveis disponibles.

Assegurar que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.

Tenir coneixement de la normativa general o sectorial aplicable a la informació de la qual és responsable, inclosa la normativa vigent en matèria de protecció de dades de caràcter personal.

Definir els requeriments de seguretat pel tractament de la informació, ja sigui de forma automatitzada o manual en tot el seu cicle de vida (creació, modificació, conservació i destrucció, si s'escau).

Fer seguiment de l'estat de la seguretat dels sistemes d'informació i gestionar la mitigació de riscos dins del seu grau d'autonomia de decisió.

Donar impuls i implicar-se en l'elaboració dels plans de continuïtat del negoci, i definir procediments alternatius en cas d'indisponiblitat del sistema o manca d'integritat de la informació.

Adoptar les mesures correctores oportunes d'acord amb l'establert pel Responsable de Seguretat.

En el cas de sistemes de categoria alta acordar, si s'escau, la retirada d'operació d'alguna informació, d'algun servei o del sistema en la seva totalitat fins a la seva adequada subsanació o mitigació de les deficiències detectades.

5.3.6 Altres responsabilitats en Seguretat de la Informació distribuïdes al Consorci AOC.

5.3.6.1 Revisió de la informació i dels serveis i la seva categorització.

El responsable de cada servei i/o de la informació tractada és l'encarregat de determinar la seva categorització de seguretat en funció de la valoració de l'impacte que tindria un incident que afectés a la seguretat dels sistemes d'informació o els drets i llibertats de les persones titular de les dades de caràcter personal objecte de tractament.

Aquesta categorització es durà a terme d'acord amb l'establert a l'ENS i al Marc de Ciberseguretat de Catalunya.

5.3.6.2 Usuaris dels Sistemes d'Informació

Tots els usuaris tant externs com interns, es responsabilitzaran de conèixer i complir amb les directrius de seguretat definides a la Política de Seguretat del Consorci AOC per prevenir situacions que puguin derivar en perjudicis, com poden ser: pèrdues o usos indeguts de la informació, deteriorament o indisponiblitat dels sistemes, interrupció dels serveis prestats, etc.

El personal del Consorci AOC o que realitzi tasques pel Consorci AOC (proveïdors, estudiants en pràctiques, etc.), es responsabilitzarà de complir amb les indicacions establertes en la Política de Seguretat del Consorci AOC i en particular de:

- Conèixer i aplicar les directrius i regulacions en matèria de Seguretat de la Informació i de protecció de dades de caràcter personal vigents al Consorci AOC, fent un ús adequat de la informació i dels sistemes que la suporten.
- No divulgar informació del Consorci AOC a persones no autoritzades.
- Utilitzar els Sistemes d'Informació propietat del Consorci AOC per a les finalitats designades, no permetent ni facilitant l'ús dels mateixos a persones no autoritzades.

- Reportar immediatament al Responsable de seguretat seguint els procediments establerts pel Consorci AOC, qualsevol esdeveniment que pugui comprometre la seguretat de la seva informació o els Sistemes d'Informació que la suporten i al Delegat de protecció de dades si afecta a dades de caràcter personal.
- El personal ha de participar en les accions formatives i plans relacionats amb la Seguretat de la Informació impartides pel Consorci AOC. Les empreses proveïdores de serveis han de formar al seu personal i posar a disposició del Consorci l'acreditació de la formació impartida, cas que se li sol·liciti.
- Fer bon ús dels equips i de la informació a la que tingui accés i protegir-la d'accessos no autoritzats.
- No compartir les credencials d'accés als sistemes d'informació.
- Guardar el deure de secret respecte de la informació tractada.

5.3.7 Procediment de Nomenaments.

El Director Gerent del Consorci AOC designarà al Responsable de Seguretat de la Informació, al Responsable del Sistema i, a proposta del responsable de seguretat, els nous membres permanents a incorporar al Comitè Operatiu.

5.3.8 Model de Relació

La Comissió Executiva es relaciona amb el Comitè Executiu de Seguretat per mitjà del Director gerent del Consorci AOC que és qui elevarà les propostes acordades en seu del Comitè Executiu.

Dins del Consorci AOC, el Comitè Executiu de Seguretat defineix l'estratègia en matèria de Seguretat, corresponent la seva execució al Comitè Operatiu de Seguretat que serà l'encarregat de dur-la a terme.

El Responsable de Seguretat de la Informació com a membre d'ambdós comitès (Executiu i Operatiu) serà l'encarregat de reportar en cada reunió la informació respectiva.

5.4 Directrius de Seguretat de la Informació

- Salvaguarda d'interessos, entès com que qualsevol acció o mesura implementada en matèria de seguretat de la informació, ha de salvaguardar els interessos dels ciutadans, del Consorci AOC i dels seus empleats, i ha de permetre el compliment de les seves obligacions.
- Proporcionalitat i gestió del risc, entès com que cal aplicar mesures de protecció de la informació per garantir la seva disponibilitat, confidencialitat, privacitat i

integritat segons el principi de proporcionalitat, de manera que les mesures adoptades per protegir la informació siguin fruit d'un anàlisi del risc existent i de l'impacte pel Consorci AOC en cas que aquest risc es materialitzés. Tenint en compte a més el risc pels drets i llibertats dels ciutadans derivats del tractament de dades de caràcter personal.

- Assumpció de riscos, entès com que l'assumpció de riscos en matèria de Seguretat de la Informació per part del Comitè Executiu. Aquest nivell de risc ha de tenir competència sobre l'àmbit afectat en cas de materialització del risc.
- Continuïtat del negoci, entès com que cal desenvolupar plans de continuïtat del negoci d'acord amb el resultat d'una anàlisi del risc per assegurar la continuïtat dels processos crítics.
- Propietat i classificació de la informació, entès com que tota informació ha de tenir una persona propietària responsable de classificar-la en funció del seu valor i els requeriments legals existents, controlar el seu cicle de vida i autoritzar-ne l'accés.
- Accés d'acord amb el principi de necessitat, entès com que només es facilitarà accés a la informació a aquelles persones que en tinguin una necessitat legítima pel desenvolupament de les seves funcions.
- Responsabilitat i qualitat, entès com que la informació proporcionada a través de mitjans electrònics ha d'estar protegida adientment per garantir la seva veracitat i autenticitat.
- Compliment normatiu, entès com que cal donar compliment a la legislació i marc normatiu de referència vigent en matèria de Seguretat de la Informació i de protecció de dades de caràcter personal.
- Relació amb tercers, entès com que cal adoptar les mesures necessàries per garantir la Seguretat de la Informació en la relació amb terceres parts. En concret, els contractes inclouran clàusules que obliguin a l'empresa contractista i si s'escau subcontractada a aplicar les mesures de Seguretat de la Informació que corresponguin en aplicació d'aquesta política, a complir o desenvolupar els procediments de Seguretat de la Informació necessaris i a complir altres polítiques del Consorci AOC que puguin ser d'aplicació a l'empresa, el servei o al personal extern que presta el servei. El contracte haurà de recollir la possibilitat de realitzar auditories per part del Consorci AOC sense previ avís, i de penalitzar al prestador de serveis en cas d'incompliment. El contracte inclourà, si s'escau, també les mesures necessàries per preservar els drets i llibertats dels titulars de les dades de caràcter personal objecte de tractament en el marc del contracte.
- Divulgació, entès com que es duran a terme accions de formació i conscienciació de tots els usuaris en matèria de seguretat de la informació, i de comunicació de responsabilitats, obligacions i pautes de comportament ètic, així com dels procediments establerts per la notificació d'incidències.

- Ús legítim, entès com que cal assegurar-se que tots els actius d'informació, ja siguin llogats, cedits, compartits o propietat del Consorci AOC, siguin per l'ús exclusiu en les activitats i objectius previstos i legítims del Consorci AOC, i que no es permeti cap ús privat o per a qualsevol altre objectiu.
- Disponibilitat de recursos, entès com que s'establirà l'estructura de gestió i s'assignaran els recursos necessaris per garantir i controlar la correcta implantació de la seguretat de la informació.
- Segregació de funcions, entès com que l'assignació de funcions i responsabilitats es farà respectant sempre que sigui possible el principi de segregació de funcions (les operacions d'alt risc no haurien de poder ser realitzades de principi a fi per una sola persona).
- Seguiment continuat, entès com que es farà un seguiment continuat del sistema de gestió de la Seguretat de la Informació i dels indicadors que se'n derivin, i es realitzaran auditories regulars dels sistemes per garantir l'aplicació dels controls i mesures de Seguretat de la Informació establerts, i detectar possibles vulnerabilitats o mancances.

Aquestes directrius es complementen amb les previstes en la Política de Protecció de dades de caràcter personal.

5.5 Gestió i avaluació del risc

El Consorci AOC durà a terme una avaluació continua dels riscos. Aquest procés permetrà conèixer la situació de la seguretat i valorar les amenaces i els riscos als quals estan sotmesos els sistemes d'informació i els drets i llibertats de les persones de qui es tracten dades de caràcter personal.

Per a la realització de l'anàlisi de riscos, el Consorci AOC identificarà les amenaces a les quals estan sotmesos els actius i les possibles afectacions pel que fa a les dades de caràcter personal que s'hi tracten, determinant la possibilitat que aquestes amenaces es materialitzin explotant alguna vulnerabilitat. En funció d'aquest risc i el valor de l'actiu i de si es tracten o no dades de caràcter personal i les característiques del tractament, es determinarà l'impacte o perjudici que ocorri una determinada situació en cas de materialitzar-se una amenaça.

Amb els resultats de l'anàlisi de riscos, el Consorci AOC planificarà la gestió i el tractament dels riscos identificats, seleccionant les salvaguardes necessàries per reduir els riscos a uns nivells acceptables i d'aquesta forma, reduir l'impacte.

L'anàlisi de gestió de riscos es realitzarà:

- Regularment d'acord amb l'establert a l'ENS.
- Quan canviï la informació gestionada o el tractament dut a terme

- Quan canviïn els serveis prestats.
- Quan succeeixi un incident i/o violació de seguretat.
- Quan es reportin vulnerabilitats que no es puguin resoldre en el temps acordat.

5.6 Desenvolupament i complementarietat de la Política de Seguretat de la Informació

La política de Seguretat es desenvoluparà mitjançant normes, procediments, guies, i documents de suport de seguretat per cada especificitat, sent d'aplicació supletòria el Marc Normatiu de la Seguretat de la Informació de la Generalitat de Catalunya impulsat pel l'Agència de Ciberseguretat de Catalunya.

La política de Seguretat es complementa amb la Política de Protecció de Dades de Caràcter Personal i els procediments que la desenvolupen.

5.7 Revisió o control de compliment

El responsable de Seguretat de la Informació realitzarà revisions o controls periòdics de verificació de l'aplicació i compliment de la Política de Seguretat, així com del marc normatiu que la desenvolupa.

Des del Comitè Operatiu de Seguretat es realitzaran controls de compliment de la Política de Seguretat, així com, s'identificarà i es mantindrà actualitzada la relació de requisits legals, organitzatius i tècnics que li siguin aplicables en matèria de seguretat de la informació.

5.8 Divulgació i comunicació

Una vegada aprovada la present Política de Seguretat, així com la normativa que la complementi, es posarà a disposició de tots els subjectes afectats per la mateixa segons l'àmbit d'aplicació. Així mateix, els esmentats documents estaran disponibles a la intranet del Consorci AOC.

Per a la difusió i coneixement de la Política de Seguretat i la normativa complementària, es realitzaran sessions de formació per a tot el personal del Consorci AOC, on s'informarà de l'obligatorietat de compliment amb les esmentades normatives. L'assistència a les sessions de formació és de caràcter obligatori.

Quan el Consorci contracti serveis a tercers o cedeixi informació a tercers, se'ls farà partícips de la normativa de seguretat i de protecció de dades que afecti a dits serveis o informació. Normativa que podrà ser desenvolupada per dits tercers aprovant procediments propis per donar-hi compliment.

S'informarà als diferents proveïdors, en el moment de la contractació, de l'existència de la Política de Seguretat a la que resten subjectes.

5.9 Aprovació i actualització

La present Política de Seguretat ha estat aprovada per la Comissió Executiva i és d'obligat compliment per a tota la organització.

5.10 Revisions i vigència

La present Política de Seguretat serà revisada, com a mínim, anualment o de manera extraordinària, sempre que es produeixin canvis substancials del seu contingut. El Comitè Executiu és el responsable de dur a terme dites revisions.

Si com a conseqüència de les esmentades revisions es fa necessari modificar el contingut de la Política de Seguretat, el Comitè Operatiu elaborarà la proposta de modificació. El projecte aprovat pel Comitè Executiu es sotmetrà l'aprovació definitiva per part de la Comissió Executiva per a la seva aprovació. Un cop aprovada la darrera versió, passarà a ser la Política de Seguretat de la Informació vigent, quedant la versió anterior derogada.

Es fixa un termini de sis mesos des de la publicació de la present Política de Seguretat, per a determinar la normativa de desenvolupament i emprendre les accions necessàries per assolir, el compliment de les prescripcions que s'hi estableixen.

5.11 Penalitzacions

L' incompliment de la Política de Seguretat de la Informació comportarà l'aplicació del règim disciplinari que pertoqui.