Consorci
Administració Oberta
de Catalunya

Política de seguretat

Pla Director de Seguretat

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

Realitzat per:
Versió: 1.0
Data: 28/05/2015
Arxiu: PDS.Política de seguretat.docx

Índex

1 Control del document

1.1 Informació General

Títol	Política de Seguretat
Versió	
Creat per	
Revisat per	
A aprovar per	
Nom del Fitxer	.Política de seguretat 1.0.docx

1.2 Llista de Distribució

	Organització

1.3 Històric de canvis

Data	Autor	Raó de la modificació

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 de l'Administració Oberta de Catalunya (d'ara en endavant Consorci AOC), conscient de la importància i del valor de la seva informació i com a prestador de serveis fonamentals per a l'operativitat dels diferents i diversos ens als quals dóna suport, garanteix la integritat i disponibilitat dels sistemes que proporcionen els serveis, així com la confidencialitat, integritat i disponibilitat de la informació emmagatzemada, transmesa o processada pels Sistemes d'Informació i comunicacions del qual és responsable.

2.1 Objectius

La Política de Seguretat estableix una sèrie d'objectius orientats a protegir la informació i els sistemes que la suporten davant de possibles amenaces, reduir els danys provocats per incidents i assegurar la continuïtat dels seus serveis, preservant els components bàsics de la seva seguretat:

- **Confidencialitat**: Garanteix que a la informació i als sistemes només accedeixen les persones degudament autoritzades.
- **Integritat**: Garanteix l'exactitud de la informació i els sistemes contra alteració, perduda o destrucció, ja sigui de forma accidental o fraudulenta.
- **Disponibilitat**: Garanteix que la informació i els sistemes puguin ser utilitzats en la forma i el temps requerits.
- **Responsabilitat** o "no refutació", entesa com la garantia de que és possible demostrar quin personal usuari tracta la informació.
- **Traçabilitat,** entesa com la garantia de que és possible reproduir l'històric o seqüència d'accions sobre un determinat procés i determinar qui ha estat l'autor de cada acció.
- **Compliment normatiu,** entès com l'adequada protecció de la informació de caràcter personal o qualsevol altre informació d'acord tant a la legislació vigent en matèria de seguretat com al Marc Normatiu de Seguretat de la Informació del CESICAT a l'àmbit de la Generalitat de Catalunya, amb caràcter supletori en manca d'un de propi
- **Criticitat** per la presa de decisions, entesa com l'adequada protecció de la informació rellevant per a la presa de decisions del negoci.

Tots els paràmetres anteriorment descrits, són essencials per al compliment de la legislació vigent en matèria de seguretat de la informació i per a la prestació d'un servei de qualitat.

L'objectiu de la seguretat de la Informació es garantir la qualitat de la informació i prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant ràpidament als incidents.

Els sistemes TIC han d'estar protegits davant d'amenaces de ràpida evolució amb potencial per incidir a la confidencialitat, integritat, disponibilitat, us previst i valor de la informació i dels serveis. Per tal de defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis i condicions de l'entorn per a garantir la prestació continua dels serveis.

Les diferents àrees han d'aplicar les mesures mínimes de seguretat previstes en la present Política de Seguretat.

Les diferents àrees del Consorci AOC han d'assumir que la seguretat TIC i el seu finançament són una part integral del cicle de vida del sistema, des de la concepció fins a la retirada del servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació.

Les diferents àrees del Consorci AOC han d'estar preparades per a prevenir, detectar, reaccionar i recuperar-se d'incidents. La notificació d'incidents es realitzarà al CESICAT a través del CESICAT-CERT

Prevenció

Les àrees han d'evitar, o com a mínim prevenir en la mida del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat, per això s'han d'implementar mesures mínimes de seguretat, així com controls addicionals identificats mitjançant l'avaluació d'amenaces i riscos. Els controls, els rols, i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per garantir l'acompliment de la política han de:

- 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

Donat que els serveis es poden degradar ràpidament a causa d'incidents, s'ha de monitoritzar l'operació de forma contínua per a la detecció d'anomalies i actuar en conseqüència

La monitorització es particularment rellevant quan s'estableixen línies de defensa. Establint mecanismes de detecció, anàlisis i reporting.

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 en altres àrees o 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. Les àrees han de desenvolupar plans de continuïtat dels sistemes TIC com a part del pla general de continuïtat del negoci i activitats de recuperació.

2.2 Àmbit de l'Aplicació

2.2.1 Objectiu

Aquesta Política de Seguretat afecta a la seguretat de la informació que s'ocupa de la informació en totes les seves formes (oral, escrita, impresa, electrònica, òptica, electromagnètica, etc.) en qualsevol moment del seu cicle de vida (creació o captura, manteniment, distribució i ús, i emmagatzematge, arxivament i destrucció).

2.2.2 Subjectiu

Aquesta Política de Seguretat, afecta als Sistemes d'Informació gestionats o supervisats pel Consorci AOC, s'aplica amb caràcter obligatori a:

- Personal del Consorci
- Proveïdors o col·laboradors que prestin els seus serveis tant a les instal·lacions del Consorci com des de les seves pròpies instal·lacions que accedeixin a la informació i/o als sistemes del Consorci AOC.
- Tota persona que accedeixi a la informació i/o als sistemes del Consorci AOC.

2.3 Marc Normatiu de Referència

El marc normatiu en que es desenvolupen les activitats del Consorci de l'Administració Oberta de Catalunya, i, en particular, la prestació dels seus serveis electrònics està integrat per les següents normes:

- Llei 29/2010, del 3 d'agost, de l'ús mitjans electrònics al sector públic de Catalunya
- Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics
- Llei 59/2003, de 19 de desembre, de firma electrònica
- Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal
- Estatuts del Consorci de l'Administració Oberta de Catalunya
- Reial Decret 3/2010, de 8 de gener, pel que es regula L'Esquema Nacional de Seguretat a l'àmbit de l'Administració electrònica.
- l'Estàndard Internacional ISO/IEC 27002:2005
- El Marc Normatiu de Seguretat de la Informació del CESICAT a l'àmbit de la Generalitat de Catalunya que determina les línies estratègiques, polítiques, estàndards i guies de seguretat pròpies de la Generalitat de Catalunya, amb caràcter supletori a manca d'un propi.

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

3 Política de seguretat

Polítiques, principis, estàndards i requeriments de conformitat de la seguretat:

3.1 Organització de la Seguretat

Es crea una estructura organitzativa de seguretat amb la finalitat de coordinar i aprovar tots els aspectes relacionats amb la Seguretat de la Informació, gestionats o supervisats pel Consorci AOC així com tot el personal implicat o que faci ús dels mateixos.

L'estructura Organitzativa de seguretat del Consorci AOC és la següent:

3.1.1 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 el Consorci Localret.

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

Correspon a la Comissió Executiva en matèria de seguretat:

- Vetllar que la Seguretat de la Informació estigui alineada amb els objectius i plans d'acció de la seguretat.
- Realitzar un seguiment a alt nivell de les polítiques i plans d'acció de la seguretat.
- Realitzar un seguiment a alt nivell dels fets i incidents més rellevants en l'àmbit de la Seguretat de la Informació.
- Aprovar la Política de Seguretat, el Pla Director de Seguretat i les normes en matèria de Seguretat de la Informació.
- Realitzar un seguiment de nivell de compliment de la Seguretat de la Informació i d'adequació a la legislació vigent.

3.1.2 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 actuarà com a President.
- Subdirector del Consorci AOC
- Cap d'Àrea d'Operacions
- Cap d'Àrea d'Organització
- Cap d'Àrea de Client
- Responsable de Seguretat de la Informació.

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

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, el Pla Director de Seguretat i les normes en matèria de Seguretat de la Informació,
- Identificar objectius i estratègies relacionades amb la seguretat
- Donarà suport al Comitè Operatiu, als seus membres, el dotarà dels recursos necessaris i establirà les seves directrius de treball
- Revisar la implantació de la política de seguretat.
- Iniciar, dirigir i controlar els processos 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.
- Validar el mapa de riscos i les accions de mitigació proposades pel Responsable de Seguretat de la informació.
- 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 el desenvolupament i manteniment del Pla de Continuïtat de Negoci.
- Vetllar pel compliment de la legislació que en matèria de seguretat sigui d'aplicació
- Revisar les incidències més destacades.
- Fer seguiment del Quadre de Comandament de la Seguretat de la Informació el Consorci AOC.

Les reunions ordinàries seran cada 3 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 podran assistir altres persones (membres del Comitè Operatiu de Seguretat, experts en matèria de Seguretat, juristes...) prèvia invitació del President.

3.1.3 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 a la direcció en matèria de seguretat com a membre del **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.
  - Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.
  - Identificar els riscs relatius a la seguretat de la informació
  - Promoure plans de contingència i formació en aspectes relatius a ala seguretat de la informació
  - Dirigir i coordinar les tasques realitzades del **Comitè Operatiu de Seguretat**
  - Supervisar i controlar internament el compliment de la Política, 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.
  - Elaborar el Pla director de Seguretat de la Informació del Consorci AOC i presentar-ho al Comitè Executiu per a la seva aprovació. Implementar-ho.
  - Desenvolupar i mantenir del Pla de Continuïtat de Negoci.
  - Elevar al Comitè Executiu les incidències més destacades
  - 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 Aquest càrrec serà assumit per un Cap d'Àrea

3.1.4 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

- Tècnics de Seguretat de la informació, jurídica, TIC i auditories,

Els membres que han de formar part del Comitè seran proposats pel Responsable de Seguretat de la informació i ha de ser personal de l'Organització amb coneixements jurídics, en seguretat de la informació ; seguretat TIC i auditoria

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 la normativa interna de Seguretat, les polítiques i procediments de seguretat
  - Seguiment del compliment de les normatives internes de seguretat de la informació.
  - Control de la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.
  - La realització de l'anàlisi de risc de seguretat de la informació a l'entorn del Consorci AOC.
  - L'elaboració el mapa de riscos i proposar les accions de mitigació.
  - L'elaboració el pla de formació i conscienciació dels usuaris.
  - L'elaboració del Pla director de Seguretat
  - El desenvolupament i manteniment del Pla de Continuïtat de Negoci.
  - 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
- Col·laborar amb les Àrees i/o Serveis en la inclusió de pautes a seguir per mantenir el nivell de seguretat de la informació adequat. Promoure l'anàlisi de risc dels processos més crítics i informació més sensible i proposar accions de millora i mitigació del risc
- Col·laborar amb les Àrees i/o Serveis en la definició de requeriments de seguretat pels sistemes d'informació. Identificar i reportar les vulnerabilitats dels sistemes d'informació sorgides a l'entorn tecnològic del Consorci AOC

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

A les reunions del Comitè Operatiu de Seguretat podran assistir, a requeriment del Comitè i en funció dels temes a tractar, altres persones (membres d'altres Àrees, responsables de RRHH, assessors, experts en matèria de Seguretat, ...) .

3.1.5 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.

El responsable de sistema forma part del **Comitè Operatiu de Seguretat**.

Aquest càrrec pot ser assumit per 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 de 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 en són responsables, inclosa normativa vigent en matèria de protecció de dades de caràcter personal.

Definir els requeriments de seguretat per al 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 que tracten la informació de la qual en són responsables, 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.

3.1.6 Responsabilitats en Seguretat de la Informació distribuïdes al Consorci AOC.

3.1.6.1 Propietaris de la Informació

Són les persones responsables de la seguretat de certa informació i els responsables de classificar-la en funció de la seva confidencialitat, integritat, disponibilitat, autenticitat, traçabilitat i impacte mediàtic, designant les mesures de seguretat i així com de vetllar pel compliment per part dels proveïdors i/o col·laboradors de les mesures de Seguretat de la Informació.

Han de col·laborar en la realització de revisions i auditories de seguretat de la informació.

Aquests rols seran assumits per Caps d'Àrea, Caps d'Unitat, Caps de Projecte i Responsables de Servei.

Es coordinaran amb el Comitè Operatiu de Seguretat.

3.1.6.2 Custodis

Es responsabilitzaran de salvaguardar la informació que els sigui confiada pels propietaris, implementant les mesures de seguretat per protegir la informació. Han de realitzar còpies de seguretat i implementar, operar i mantenir les mesures de seguretat establertes.

Aquests rols seran assumits per la persona encarregada de la custòdia de la informació

Es coordinaran amb el Comitè Operatiu de Seguretat.

3.1.6.3 Personal en general

Tots els usuaris tant externs com a 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, deterioració o indisponibilitat dels sistemes, interrupció dels serveis prestats, etc.

El personal pel Consorci AOC o que realitzin tasques pel Consorci AOC (proveïdors, subcontractats, personal 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 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 i 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.
- Participar en les accions formatives i plans relacionats amb la seguretat de la informació impartides pel Consorci AOC.
- Fer bon ús dels equips i de la informació a la que tingui accés i protegir-la d'accessos no autoritzats.
- Fer un bon ús de les credencials d'accés a la informació :usuari i contrasenya / targeta amb certificat digital i PIN.
- Guardar el deure de secet respecte a la informació.

3.1.7 Procediment de Nomenaments.

El Director Gerent del Consorci AOC designarà al Responsable de Seguretat de la Informació, així com a la resta de càrrecs associats al desenvolupament d'aquesta Política.

El Responsable de Seguretat de la Informació proposarà al Comitè Executiu les persones per assumir les funcions i els diferents rols associats al Comitè Operatiu i Grups de Treballs. El comitè Executiu nomenarà als membres del Comitè Operatiu de Seguretat del Consorci AOC.

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..

3.1.8 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.

3.2 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 i els 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'una anàlisi del risc existent i de l'impacte pel Consorci en cas que aquest risc es materialitzés.
- Assumpció de riscos, entès com que l'assumpció de riscos en matèria de seguretat de la informació ha de ser aprovada per un nivell directiu adequat, que serà més alt conforme major sigui l'impacte màxim del risc. Aquest nivell directiu 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.
- 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 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 sense previ avís, i de penalitzar al prestador de serveis en cas d'incompliment.
- 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, siguin per l'ús exclusiu en les activitats i objectius previstos i legítims del Consorci, 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.

3.3 Seguretat lligada al personal

El Consorci AOC establirà les mesures tècniques i organitzatives necessàries per evitar els riscos derivats d'accions humanes com poden ser: frau, sabotatge, robatoris, errors, etc.

3.3.1 Segregació de tasques

El Consorci AOC és conscient de la importància de la segregació de tasques en activitats considerades com a crítiques i prendrà les mesures que estimi convenients per evitar que una única persona disposi de plena capacitat per assumir totes les tasques en aquest tipus d'activitat.

3.3.2 Formació i conscienciació

Segons les necessitats identificades, el Consorci AOC realitzarà obligatòriament les activitats de formació i conscienciació, podent ser específiques per a cada àrea, grup o persona destinatària.

Per a tot el personal que utilitzi, operi o administri els sistemes d' informació i comunicacions del Consorci AOC, és obligatori l'assistència a les accions formatives que es realitzin en matèria de seguretat de la informació.

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

3.3.3 Ús acceptable dels Sistemes d'Informació

El Consorci AOC a través dels mitjans que cregui oportuns, posarà a la disposició de tot el personal usuari dels serveis prestats pel Consorci AOC, les pautes convenients per realitzar un bon ús de la informació i dels sistemes que la suporten, amb la finalitat d'evitar riscos derivats del seu ús incorrecte o inadequat.

3.4 Gestió i avaluació del risc

El Consorci AOC veu la necessitat de realitzar de forma periòdica un procés d'anàlisi i gestió de riscos que serveixi com a pedra angular de les actuacions de seguretat a realitzar. Aquest procés permetrà conèixer la situació de la seguretat i valorar les amenaces i els riscos als quals estan sotmesos els actius d'informació.

Per a la realització de l'anàlisi de riscos, el Consorci AOC identificarà les amenaces a les quals estan sotmesos els actius, determinant la possibilitat que aquestes amenaces es materialitzin explotant alguna vulnerabilitat. En funció d'aquest risc i el valor de l'actiu, 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 un cop a l'any
- Quan canviï la informació gestionada
- Quan canviïn els serveis prestats
- Quan succeeixi un incident greu de seguretat
- Quan es reportin vulnerabilitats greus.

3.5 Desenvolupament 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 CESICAT

3.6 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, identificarà i mantindrà actualitzada la relació de requisits legals, organitzatius i tècnics que li siguin aplicable en matèria de seguretat de la informació.

3.7 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

En els contractes, llicències i acords subscrits amb tercers pel Consorci AOC s'inclourà el deure de compliment de la legislació vigent en matèria de Seguretat, així com la legislació aplicable en matèria de propietat intel·lectual, protecció de dades i qualsevol altra normativa aplicable.

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

3.8 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.

3.9 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 Executiu elaborarà el projecte de la nova versió i l'elevarà a 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.

3.10 Penalitzacions

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