

Política de Ciberseguretat del Consorci de Serveis Universitaris de Catalunya (CSUC)

31 de gener de 2024

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

Sumari

1.	Prèambul.....	3
2.	Àmbit material i personal d'aplicació.....	4
3.	Normativa bàsica d'aplicació	5
4.	Principis bàsics	7
5.	Objectius	8
6.	Organització de la Seguretat de la Informació	9
7.	Funcions dels òrgans i persones amb els rols associats a l'Esquema Nacional de Seguretat.....	10
7.1.	Responsable de la Informació i dels Serveis	10
7.2.	Responsable de Seguretat	10
7.3.	Responsable del Sistema	11
7.4.	Comitè de Seguretat de la Informació	12
7.5.	Centre d'Operacions i Ciberseguretat (CSUC-CSIRT)	13
8.	Gestió de riscos i notificació d'incidents.....	13
9.	Disposició Addicional: Desenvolupament de la Política de Seguretat de la Informació	14
10.	Entrada en vigor	15

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

1. Prèambul

El CSUC requereix dels sistemes de Tecnologies de la Informació i les Telecomunicacions per aconseguir els seus objectius. Aquests sistemes han de ser gestionats amb diligència, prenent les mesures adequades per protegir-los davant de danys accidentals o deliberats que puguin afectar la seguretat de la informació tractada o els serveis prestats, i sempre estant protegits contra amenaces o incidents amb potencial per incidir en la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació tractada i els serveis prestats.

Per fer front a aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que les àrees, els departaments i les unitats han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), així com realitzar un seguiment continu dels nivells de prestació dels serveis, monitoritzar i analitzar les vulnerabilitats notificades, i preparar una resposta efectiva als ciberincidents per garantir la continuïtat dels serveis prestats.

La seguretat TIC és una part integral de cada etapa del cycle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'exploració. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en els plecs de licitació per a projectes TIC del CSUC

Pel CSUC, l'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant de manera preventiva, supervisant l'activitat diària per detectar qualsevol incident i reaccionant amb celeritat davant els incidents per recuperar els serveis el més aviat possible, segons l'establert a l'article 8 de l'ENS, mitjançant l'aplicació de les mesures que es relacionen a continuació en l'àmbit de la prevenció, la detecció, la resposta i la recuperació.

En l'àmbit preventiu, per tal que la informació i/o els serveis no es vegin perjudicats per incidents de seguretat, el CSUC implementa les mesures de seguretat establertes per l'ENS, així com qualsevol altre control addicional que hagi identificat com a necessari mitjançant una avaluació de amenaces i riscos. Aquests controls, els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per garantir el compliment de la política de Ciberseguretat, el CSUC:

- Autoritza els sistemes abans d'entrar en operació.
- Avalua regularment la seguretat, incloent l'anàlisi dels canvis de configuració realitzats de forma rutinària.
- Sol·licita una revisió periòdica per part de tercers amb l'objectiu d'obtenir una avaluació independent.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

Des de la perspectiva de la detecció, el CSUC 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 disposa l'article 10 de l'ENS (vigilància contínua i reavaluació periòdica). Quan es produeix una desviació significativa dels paràmetres preestablerts com a normals (d'acord amb l'article 9 de l'ENS, Existència de línies de defensa), s'establiran els mecanismes de detecció, anàlisi i informació necessaris perquè arribin als responsables regularment.

Pel supòsit en que es produeixin incidents, el CSUC establirà les següents mesures:

- Mecanismes per respondre de manera eficaç als incidents de seguretat.
- Designar un punt de contacte electrònic i telefònic per a les comunicacions referents als incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou les comunicacions en ambdós sentits amb els Equips de Resposta a Emergències davant emergències informàtiques (CERT).

Finalment, i per garantir la disponibilitat dels serveis, el CSUC disposa dels mitjans i tècniques necessàries per garantir la recuperació dels serveis més crítics.

2. Àmbit material i personal d'aplicació

1. Aquesta Política s'aplicarà als sistemes d'informació del Consorci de Serveis Universitaris de Catalunya, relacionats amb l'exercici de les seves competències, i a tots els usuaris amb accés autoritzat als mateixos, siguin o no empleats públics i amb independència de la naturalesa de la seva relació jurídica amb el consorci. Tots ells tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la normativa de seguretat derivada, sent responsable del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi al personal afectat.
2. El CSUC haurà d'organitzar la formació necessària per tal que tot el personal del CSUC inclòs en l'àmbit de l'ENS, assisteixi a una o diverses sessions de conscienciació en matèria de seguretat i protecció de dades, com a mínim un cop a l'any. Es desenvoluparà un programa de conscienciació contínua per a tot el personal, especialment per al de nova incorporació.
3. El Consorci de Serveis Universitaris de Catalunya només recollirà i tractarà dades personals quan siguin adequades, pertinents i no excessives, i aquestes estiguin relacionades amb l'àmbit i les finalitats per a les quals s'hagin obtingut. De la mateixa manera, adoptarà les mesures de caràcter tècnic i organitzatiu necessàries per al compliment de la normativa de Protecció de Dades.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

4. Les persones amb responsabilitat en l'ús, operació o administració de sistemes d'informació rebran formació per al maneig segur dels sistemes en la mesura que la necessitin per realitzar la seva feina. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.
5. Quan el Consorci de Serveis Universitaris de Catalunya presti serveis a altres organismes o gestioni informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació. S'estableixen canals per al report i la coordinació dels respectius Comitès de Seguretat de la Informació i es definiran procediments d'actuació per a reaccionar davant d'incidents de seguretat.

Quan el Consorci de Serveis Universitaris de Catalunya utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Ciberseguretat i de la normativa de seguretat relativa a aquests serveis o informació. Aquest tercer estarà subjecte a les obligacions establertes en aquesta normativa i podrà desenvolupar els seus propis procediments operatius per complir-los. Es definiran procediments específics de report i resolució d'incidències. Es garantirà que el personal dels tercers estigui adequadament conscient en matèria de seguretat, almenys al mateix nivell establert en aquesta Política de Seguretat.

Quan alguna aspecte d'aquesta Política de Seguretat de la Informació no pugui ser satisfet per un tercer segons el que es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisarà 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 continuar endavant.

3. Normativa bàsica d'aplicació

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

- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

Seguretat de la Informació

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i per la qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.
- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

- Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança en la matèria. Reial decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de firma electrònica.
- Reial decret-llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions.
- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text Refós de la Llei de Propietat Intel·lectual.
- Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat.
- Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Informe de l'Estat de la Seguretat.
- Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Auditoria de la Seguretat dels Sistemes d'Informació.
- Resolució de 13 d'abril de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat de Notificació d'Incidents de Seguretat.
- Llei 40/2015, de 1 d'octubre, de Règim Jurídic del Sector Públic.
- 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 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

Gestió Administracions Públiques

- Llei 9/2014, de 9 de maig, General de Telecomunicacions.
- Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local, modificada per la llei 11/1999, de 21 d'abril.
- Llei 57/2003, de 16 de desembre, de mesures per a la modernització del govern local.
- Llei 56/2007, de 28 de desembre, de Mesures d'Impuls de la societat de la Informació.
- Llei 19/2013, de 9 de desembre, de Transparència, Accés a la Informació Pública i Bon Govern.
- Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, per la qual es transposen a l'ordenament jurídic espanyol les Directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.
- Reial decret legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q58562531

Signatura realitzada en data 05/02/2024 10:07:56+01:00

Bones pràctiques de Seguretat de la Informació:

- ISO 27001:2022 – Sistema de Gestió de la Seguretat de la Informació.
- ISO 27002:2022 - Tecnologia de la Informació. Tècniques de seguretat. Codi de pràctiques per als controls de seguretat de la informació.
- ISO 27701:2019 – Gestió d'Informació de la Privacitat.
- ISO 20000-1:2018 - Tecnologies de la informació. Gestió de Serveis. Part 1 – Requisits del Sistema de Gestió de Serveis.
- ISO 30301: 2019 - Sistemes de gestió per als documents. Requisits.

També formen part del marc normatiu les altres normes aplicables a l'Administració Electrònica del Consorci de Serveis Universitaris de Catalunya, derivades de les anteriors i publicades en la seu electrònica compresa dins de l'àmbit d'aplicació de la present Política.

4. Principis bàsics

Els principis bàsics són directrius fonamentals de seguretat que s'han de tenir sempre presents en qualsevol activitat relacionada amb l'ús dels actius d'informació i que es concreten a través dels objectius després establerts. En destaquen els següents:

- **Abast estratègic:** La seguretat de la informació ha de comptar amb el compromís i suport de tots els nivells directius del CSUC, de manera que pugui estar coordinada i integrada amb la resta d'iniciatives estratègiques de l'organització per conformar un tot coherent i eficaç.
- **Responsabilitat determinada:** En els sistemes TIC s'identificaran les funcions de el **Responsable de la Informació**, que determina els requisits de seguretat de la informació tractada; el **Responsable del Servei**, que determina els requisits de seguretat dels serveis prestats; el **Responsable del Sistema**, que té la responsabilitat sobre la prestació dels serveis, i el **Responsable de la Seguretat**, que determina les decisions per satisfer els requisits de seguretat. La persona responsable de la seguretat serà diferent a la responsable del sistema sense que pugui haver dependència jeràrquica entre ambdues persones
- **Seguretat integral:** La seguretat s'entendrà com un procés integral format per tots els elements tècnics, humans, materials i organitzatius relacionats amb els sistemes TIC, procurant evitar qualsevol actuació puntual o tractament conjuntural. La seguretat de la informació s'ha de considerar com una part de l'operativa habitual, estant present i aplicant-se des del disseny inicial dels sistemes TIC.
- **Gestió de Riscos:** L'anàlisi i gestió de riscos serà part essencial del procés de seguretat. La gestió de riscos permetrà mantenir un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells es realitzarà mitjançant l'aplicació de mesures de seguretat que establiran un equilibri entre la naturalesa de les dades i els tractaments, l'impacte i la probabilitat dels riscos als quals estiguin exposats, i l'eficàcia i

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

el cost de les mesures de seguretat. En avaluar el risc en relació amb la seguretat de les dades, cal tenir en compte els riscos derivats del tractament de dades personals.

- Proporcionalitat: L'establiment de mesures de protecció, detecció i recuperació ha de ser proporcional als riscos potencials i a la criticitat i valor de la informació i dels serveis afectats.
- Millora contínua: Les mesures de seguretat s'avaluaran i actualitzaran periòdicament per adequar la seva eficàcia a la constant evolució dels riscos i sistemes de protecció. La seguretat de la informació serà atesa, revisada i auditada per personal qualificat.
- Seguretat per defecte: Els sistemes han de dissenyar-se i configurar-se de manera que garanteixin un grau suficient de seguretat per defecte.

5. Objectius

El Consorci de Serveis Universitaris de Catalunya posa a disposició de la comunitat universitària i de recerca la realització de tràmits en línia i noves vies de participació que faciliten el desenvolupament i el bon funcionament de les seves funcions i tasques.

En potenciar l'ús de les noves tecnologies al CSUC, es persegueix fomentar la relació electrònica de tota la comunitat universitària i de recerca.

Els objectius de la seguretat de la informació tant des de la perspectiva de la qualitat i protecció de la informació com de les persones usuàries es concreten a través de:

- Aconseguir una plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Gestió dels actius d'informació: Els actius d'informació del consorci estaran inventariats i categoritzats, i estaran associats a una persona responsable.
- Seguretat lligada a les persones: S'implantaran els mecanismes necessaris perquè qualsevol persona que accedeixi o pugui accedir als actius d'informació conegui les seves responsabilitats i, d'aquesta manera, es redueixi el risc derivat d'un ús indegut, aconseguint la plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Seguretat física: Els actius d'informació estaran ubicats en àrees segures, protegides per controls d'accés físics adequats al seu nivell de criticitat. Els sistemes i els actius d'informació que continguin aquestes àrees estaran protegits davant amenaces físiques o ambientals.
- Seguretat en la gestió de comunicacions i operacions: S'establiran els procediments necessaris per aconseguir una gestió adequada de la seguretat, operació i actualització de les TIC. La informació que es transmeti a través de xarxes de comunicacions ha de ser adequadament protegida, tenint en compte el seu nivell de sensibilitat i criticitat, mitjançant mecanismes que garanteixin la seva seguretat.
- Control d'accés: Es limitarà l'accés als actius d'informació per part d'usuaris, processos i altres sistemes d'informació mitjançant la implementació de mecanismes d'identificació, autenticació i autorització adequats a la criticitat de cada actiu. A més,

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

s'enregistraran les utilitzacions del sistema amb l'objectiu d'assegurar la traçabilitat de l'accés i auditar el seu ús adequat, segons l'activitat de l'organització.

- Adquisició, desenvolupament i manteniment dels sistemes d'informació: Es tindran en compte els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, garantint la seva seguretat per defecte.
- Gestió dels incidents de seguretat: S'implementaran els mecanismes adequats per a la correcta identificació, registre i resolució dels incidents de seguretat.
- Garantir la prestació continuada dels serveis: S'implementaran els mecanismes adequats per assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels seus processos de negoci, d'acord amb les necessitats de nivell de servei dels usuaris.
- Protecció de dades: S'adoptaran les mesures tècniques i organitzatives corresponents per abordar els riscos generats pel tractament i complir amb la legislació de seguretat i privacitat.
- Compliment: S'adoptaran les mesures tècniques, organitzatives i procedimentals necessàries per a complir amb la normativa legal vigent en matèria de seguretat de la informació.

6. Organització de la Seguretat de la Informació

El Consorci de Serveis Universitaris de Catalunya, tenint en compte el que s'estableix en el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), i les directrius establertes a la Guia CCN-STIC-801 "Responsabilitats i Funcions en l'ENS", emprendre les següents accions:

- Designarà rols de seguretat: Responsables dels Serveis, Responsables de la Informació, Responsable de la Seguretat, Responsable del Sistema i Delegat de Protecció de Dades
- Constituirà un òrgan consultiu i estratègic per a la proposta d'accions en matèria de Seguretat de la Informació. Aquest òrgan es constituirà com un òrgan col·legiat i es denominarà **Comitè de Seguretat de la Informació**. Serà presidit per la persona titular de la direcció general del CSUC o la persona delegada per ella, i en seran vocals permanents els responsables de serveis, els d'informació, el de sistemes i el de seguretat així com el Delegat de protecció de dades del CSUC

El Responsable de la Seguretat, que serà el secretari del Comitè de Seguretat, correspondrà a un càrrec de nivell executiu, designat formalment per la direcció general. El Responsable de la Seguretat no podrà ser un òrgan de govern unipersonal del consorci i no haurà de tenir cap responsabilitat sobre la prestació dels serveis TIC, ni haurà d'estar sota la dependència jeràrquica del Responsable del Sistema (i viceversa).

El Comitè podrà convocar a assessors externs i altres i especialistes externs dels sectors públic, privat i/o acadèmic, i altres representants del consorci la presència dels quals, per raó de la seva experiència o vinculació amb els assumptes tractats, sigui necessària o aconsellable. En qualsevol cas, aquestes persones tindran dret a veu sense vot.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

El Secretari/a del Comitè realitzarà les convocatòries i redactarà les actes de les reunions del Comitè de Seguretat.

7. Funcions dels òrgans i persones amb els rols associats a l'Esquema Nacional de Seguretat

7.1. Responsable de la Informació i dels Serveis

Seràn funcions dels Responsables de la Informació i dels Serveis:

- Establir i elevar per a la seva aprovació al Comitè de Seguretat de la Informació els requisits de seguretat aplicables a la Informació (nivells de seguretat de la Informació) i als Serveis (nivells de seguretat dels serveis), dins del marc establert a l'Annex I del RD ENS, sol·licitant en el seu cas propostes i informes respectivament al Responsable de Seguretat i al Responsable del Sistema.
- Dictaminar respecte als drets d'accés a la informació i els serveis.
- Acceptar els nivells de risc residual que afecten a la informació i els serveis.
- Posar en coneixement del Responsable de Seguretat qualsevol variació respecte a la Informació i els Serveis dels quals és responsable, especialment la incorporació de nous Serveis o Informació a la seva càrrec. Aquest comunicarà aquests canvis al Comitè de Seguretat de la Informació en la propera reunió.

7.2. Responsable de Seguretat

Seràn funcions del Responsable de Seguretat:

- Coordinar el manteniment i la supervisió del nivell adequat de seguretat de la Informació gestionada i dels Serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la Declaració d'Aplicabilitat, de promoure la identificació de mesures de seguretat, de determinar les configuracions necessàries i d'elaborar la documentació del sistema.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable del Sistema i/o Comitè de Seguretat TIC.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i, si s'escau, en els plans de continuïtat, procedint a la seva validació.
- Promoure la realització de l'anàlisi de riscos, en el que identifiquin les mancances i debilitats, per posar-les en coneixement del Comitè de Seguretat de la Informació
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comitè de Seguretat la proposta de canvis i altres requisits del sistema.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

- Promoure l'elaboració dels procediments de seguretat que formen part del Mapa Normatiu (i no són competència del Comitè) i posar en coneixement del Comitè les modificacions que s'hagin realitzat al llarg del període en curs.

7.3. Responsable del Sistema

Seràn funcions del Responsable del Sistema:

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, elaborant els procediments operatius necessaris.
- Definir la topologia i la gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en el mateix.
- Aturar l'accés a la informació o prestació de serveis si té coneixement que aquests presenten deficiències greus de seguretat.
- Assegurar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable de Seguretat i/o Comitè de Seguretat de la Informació.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i, si s'escau, en els plans de continuïtat.
- Dur a terme, si escau, les funcions de l'administrador de la seguretat del sistema:
 - La gestió, configuració i actualització, si escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
 - La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent la monitorització de l'activitat desenvolupada en el sistema i la seva correspondència amb el que està autoritzat.
 - Aprovar els canvis en la configuració vigent del Sistema d'Informació.
 - Assegurar que els controls de seguretat establerts siguin complerts estrictament.
 - Assegurar que s'apliquin els procediments aprovats per gestionar el Sistema d'Informació.
 - Supervisar les instal·lacions del maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no estigui compromesa i que en tot moment es compleixin les autoritzacions pertinents.
 - Monitoritzar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.
 - Informar al Responsable de Seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
 - Col·laborar en la investigació i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

Quan la complexitat del sistema ho justifiqui, el Responsable del Sistema podrà designar els responsables de sistema delegats que consideri necessaris, que en tindran dependència funcional directa i seran responsables en el seu àmbit de totes aquelles accions que se'ls hi delegui.

7.4. Comitè de Seguretat de la Informació

- a. Estar permanentment informat de la normativa que regula la Certificació de Conformitat amb l'ENS, incloent les seves normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques. Aquesta informació serà facilitada pel responsable d'Operacions i Ciberseguretat.
- b. Estar permanentment informat de la relació d'Entitats de Certificació acreditades i organitzacions, públiques i privades, certificades.
- c. Estar permanentment informat de la relació d'esquemes de certificació de la seguretat amb els quals l'Administració Pública té establerts acords o reconeixement mutu de certificats.
- d. Proposar directrius i recomanacions, que seran recollides en les corresponents actes de les reunions del Comitè.
- e. Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació per assegurar-se que siguin consistents, alineats amb l'estratègia decidida en la matèria i evitar duplicacions.
- f. Atendre les inquietuds en matèria de Seguretat de la Informació de l'Administració i de les diferents àrees, informant periòdicament de l'estat de la seguretat de la informació a la direcció del CSUC.
- g. Resoldre els conflictes de responsabilitat que puguin sorgir entre els diferents responsables i/o entre diferents departaments, elevant aquells casos en els quals no tingui prou autoritat per decidir.
- h. Assessorar en matèria de seguretat de la informació sempre que se li requereixi.
- i. Promoure la disponibilitat de recursos per satisfer les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.
- j. Seleccionar les mesures de seguretat a aplicar, es quals hauran de ser proporcionals als riscos i estar justificades.
- k. Revisar la Política de Seguretat de la Informació abans de l'aprovació per part de l'òrgan competent.
- l. Proposar la Normativa d'Equipament Informàtic del Consorci de Serveis Universitaris de Catalunya per a l'aprovació per la direcció general del CSUC.
- m. Aprovar el Mapa de Normativa intern amb la llista de Normativa i Procediments de seguretat per a la implantació de l'ENS.

Periodicitat de les reunions i presa d'acords:

1. Durant el desenvolupament del projecte d'adequació a l'ENS, per avaluar el desenvolupament del mateix i possibilitar-ne el seguiment adequat, el Comitè de Seguretat TIC es reunirà, com a mínim, una vegada al trimestre.
2. Un cop assolida la Certificació de Conformitat amb l'ENS dels serveis prestats pel CSUC, el Comitè de Seguretat TIC es reunirà, com a mínim, dues vegades a l'any amb caràcter semestral, sense perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, requereixi una major freqüència en les reunions.
3. En tot cas, les reunions seran convocades per la seva Presidència, a través del Secretari, per iniciativa pròpia o per majoria dels seus vocals permanents.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I
Signatura realitzada en data 05/02/2024 10:07:56+01:00

4. Les decisions s'adoptaran per consens dels vocals i, en cas d'empat, amb el vot de qualitat de la presidència.

7.5. Centre d'Operacions i Ciberseguretat (CSUC-CSIRT)

El CSUC disposa d'un Centre d'Operacions de Ciberseguretat, anomenat CSUC-CSIRT, que presta serveis de ciberseguretat, desenvolupant la capacitat de vigilància i detecció d'amenaques en l'operació diària dels sistemes TIC, alhora que millora la capacitat de resposta del sistema davant de qualsevol atac.

El CSUC-CSIRT realitzarà les següents funcions:

- Supervisar i monitoritzar la seguretat dels sistemes i dels dispositius de defensa, ja sigui mitjançant les interfícies previstes o instal·lant les corresponents sondes.
- Anàlisi i correlació d'esdeveniments de seguretat i registres d'activitat dels sistemes.
- Operacions de seguretat sobre els dispositius de defensa.
- Podrà constituir un Equip de Resposta a Incidents de Seguretat: Fer un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte a aquests.
- Servei d'Alerta Precoç (SAT) d'alertes de seguretat a les xarxes corporatives i a les connexions a Internet dels sistemes.
- Gestió de vulnerabilitats (anàlisi i determinació de les accions de correcció/actualització) d'aplicacions i serveis.
- Anàlisi forense digital i de seguretat.
- Servei de cibervigilància que possibiliti la prospectiva sobre la ciberamença.

La persona responsable de l'administració de la seguretat de l'àmbit TIC es coordinarà amb tots els responsables per a la definició i aplicació de les mesures de seguretat en els sistemes i infraestructures sota la seva responsabilitat, i de l'altra banda, col·laborar en les tasques de operativa diària.

8. Gestió de riscos i notificació d'incidents

Tots els sistemes afectats per aquesta Política de Seguretat de la Informació estan subjectes a una anàlisi de riscos amb l'objectiu d'avaluar les amenaces i els riscos als quals estan exposats. Aquest anàlisi es realitzarà:

- Com a mínim una vegada a l'any.
- Quan hi hagi canvis significatius en la informació i/o els serveis gestionats.
- Quan es produeixi un incident greu de seguretat o es detectin vulnerabilitats greus.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

El procés de gestió de riscos continuarà les següents fases:

- Categorització dels sistemes.
- Anàlisi de riscos.

Les fases d'aquest procés es realitzaran segons el que s'estableix als Annexos I i II del Reial Decret 311/2022, de 8 de gener, i seguint les normes, instruccions, Guies CCN-STIC i recomanacions per a la seva aplicació elaborades pel Centre Criptològic Nacional.

En particular, per dur a terme l'anàlisi de riscos, com a norma general s'utilitzarà una metodologia reconeguda d'anàlisi i gestió de riscos.

9. Disposició Addicional: Desenvolupament de la Política de Seguretat de la Informació

La present Política de Seguretat de la Informació serà complementada per mitjà de diversa normativa i recomanacions de seguretat (normatives i procediments de seguretat, procediments tècnics de seguretat, informes, registres i evidències electròniques). Correspon al Comitè de Seguretat de la Informació la seva revisió anual i/o manteniment, proposant, en cas que sigui necessari, millores a la mateixa.

El cos normatiu sobre seguretat de la informació es desenvoluparà en tres nivells per àmbit d'aplicació, nivell de detall tècnic i obligatorietat de compliment, de manera que cada norma d'un determinat nivell de desenvolupament es fonamenti en les normes de nivell superior. Aquests nivells de desenvolupament normatiu són els següents:

- a) Primer nivell normatiu: constituït per la present Política de Seguretat de la Informació, la Normativa Interna de l'Ús dels Mitjans Electrònics i les directrius generals de seguretat aplicables al CSUC.
- b) Segon nivell normatiu: constituït per les normes de seguretat derivades de les anteriors.
- c) Tercer nivell normatiu: constituït per procediments, guies i instruccions tècniques. Són documents que, complint amb el que s'exposa a la Política de Seguretat de la Informació, determinen les accions o tasques a realitzar en el desenvolupament d'un procés.

Correspon a la direcció general del Consorci de Serveis Universitaris de Catalunya l'aprovació de la Política de Seguretat de la Informació i la Normativa Interna de l'Ús dels Mitjans Electrònics el CSUC, essent el Comitè de Seguretat de la Informació l'òrgan responsable de l'aprovació dels altres documents, sent també responsable de la seva difusió perquè les parts afectades en tinguin coneixement.

De la mateixa manera, aquesta Política de Seguretat de la Informació complementa la Política de privadesa del Consorci de Serveis Universitaris de Catalunya en matèria de protecció de dades.

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00

La normativa de seguretat i, especialment, la Política de Seguretat de la Informació i la Normativa Interna de l'Ús dels Mitjans Electrònics, estarà a disposició de tots els membres del CSUC, especialment per aquells que utilitzin, operin o administren els sistemes d'informació i comunicacions. Estarà disponible per a la consulta a la Intranet. Aquesta documentació serà custodiada per l'àrea de Serveis TIC.

10. Entrada en vigor

L'entrada en vigor d'aquesta norma es produirà a partir del dia següent a la seva publicació en els mitjans telemàtics del CSUC, prèvia aprovació i signatura per part de la direcció general del Consorci.

Signatura

Original signat per:

OLGA LANAU RAMI
CONSORCI DE SERVEIS UNIVERSITARIS DE
CATALUNYA - CIF Q5856253I

Signatura realitzada en data 05/02/2024 10:07:56+01:00