Acord de Consell de Govern de la Universitat Rovira i Virgili, de data 23 d'octubre de 2018, pel qual s'aprova la Política de seguretat de la URV.

1 APROVACIÓ I ENTRADA EN VIGOR

Aquesta Política de Seguretat és efectiva des de la data d'aprovació pel Consell de Govern.

2 INTRODUCCIÓ

El propòsit de la present Política de Seguretat de la Informació de la Universitat Rovira i Virgili és establir les bases de la fiabilitat amb que els sistemes d'informació prestaran els seus serveis i custodien la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control i sense que la informació pugui arribar al coneixement de persones no autoritzades. En aquest document es recull el conjunt de mesures necessàries, tant tècniques com organitzatives, encaminades a aconseguir un nivell de protecció adequat per tal d'assegurar el compliment legal, garantir la disponibilitat i la confidencialitat de la informació.

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

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, cal una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica l'organització ha d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

És innegable que Internet i les TIC en general tenen un paper important en la producció científica i, per tant, en el desenvolupament i difusió de les innovacions. Aquesta importància es manifesta en una doble vessant; d'una banda, com a elements que faciliten l'accés a bases de dades, revistes, estadístiques i publicacions, canalitzant la transferència d'innovacions des de l'àmbit científic al seu desenvolupament comercial; i de l'altra, com a eines que possibiliten la comunicació i difusió del coneixement. Per aquest motiu la universitat, com a organització que competeix en el mercat, ha de valer-se de les TIC, no només en una vessant educativa o investigadora, sinó també estructural, com a organització que desenvolupa i modernitza els seus processos per mitjà de les noves tecnologies. Així, la universitat es planteja la seva contribució a la societat de la informació al voltant de tres grans àmbits d'aplicació de les TIC al món universitari:

- en aspectes d'organització i govern de la universitat
- com a mitjà per millorar la qualitat i difusió de la investigació
- en la incorporació de les TIC al procés educatiu

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

Com ha quedat de manifest, a causa de l'enorme rellevància de les TIC en tots els àmbits d'acció de la Universitat, una adequada política de seguretat dels sistemes d'informació en els quals aquesta es recolza és fonamental per mantenir la confiança de la comunitat universitària i de tots els ciutadans a la nostra universitat. El

principal fonament de l'aplicació de l'ENS a la Universitat és institucionalitzar els seus principis, per a això tot l'equip de direcció de la Universitat i el seu Consell de Govern posen tot el seu esforç per tal que la seguretat i el bon ús dels seus sistemes d'informació siguin uns dels principals valors de la Universitat.

L'organització ha de comprovar que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema d'informació, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

L'organització ha d'estar preparada per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l' ENS.

A més a més, cal tenir en compte que des de l'aprovació de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques i la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, l'ENS no és només d'aplicació als sistemes TIC sinó a tots els sistemes d'informació.

Així mateix, el Reglament (EU) 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 (en endavant, RGPD) estableix que el responsable del tractament i l'encarregat de tractament han d'aplicar les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc. Així, de la mateixa manera que ho requereix l'ENS, caldrà realitzar una avaluació dels riscos per a cadascun dels tractaments de la Universitat. Per aquest motiu, es fa necessari descriure les figures responsables obligatòries en el RGPD des d'una visió conjunta amb l'estructura organitzativa de l'ENS, considerant d'aquesta manera la seguretat des d'un punt de vista global.

2.1 Prevenció

L'organització ha d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. En aquest sentit, s'han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

2.2 Detecció

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, s'ha de monitoritzar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que estableix l'article 9 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i informe que arribin als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

2.3 Resposta

L'organització està obligada a:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar punt de contacte per a les comunicacions pel que fa a incidents detectats en altres serveis universitaris o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en ambdós sentits, amb els Equips de Resposta a Emergències (CERT).

2.4 Recuperació

Per garantir la disponibilitat dels serveis crítics, s'han de desenvolupar plans de continuïtat dels sistemes d'informació com a part del pla general de continuïtat del servei.

3 ABAST

Aquesta política de seguretat de la Universitat Rovira i Virgili s'aplica a tota la comunitat universitària, als seus actius d'informació i a tots els sistemes d'informació sense excepcions.

4 MARC NORMATIU

La Universitat es regeix per la Llei 36/1991, de 30 de desembre, de creació de la Universitat Rovira i Virgili, la Llei orgànica 6/2001, de 21 de desembre, d'universitats (modificada per la Llei orgànica 4/2007, de 12 d'abril), la Llei 1/2003, de 19 de febrer, d'universitats de Catalunya, l'Estatut de la Universitat Rovira i Virgili (aprovat per l'Acord GOV/23/2012, de 27 de març) i la resta de normativa d'aplicació.

La normativa relativa als sistemes d'informació que és d'aplicació es troba recollida en l'apartat de normatives de la pàgina web de la Universitat.

5 ORGANITZACIÓ DE LA SEGURETAT A LA URV

5.1 Estructura de la seguretat a la URV:

La gestió de la seguretat de la informació a la Universitat Rovira i Virgili està organitzada d'acord amb l'estructura següent:

- Comitè de Seguretat de la Informació
- Responsable de Seguretat
- Responsable del CERT (Computer Emergency Response Team)
- Responsable del sistema
- Administrador de seguretat

El rector o rectora nomenarà les figures previstes en aquesta política de seguretat.

Els responsables podran delegar les funcions assignades en altres òrgans, d'acord amb la legislació vigent.

5.1.1 Comitè de Seguretat de la Informació (CSI)

1. El Comitè de Seguretat de la Informació (en endavant, CSI) coordina la seguretat de la informació a nivell de l'organització.

2. El CSI està format per:

- Rector o rectora
- Secretari o secretària general
- Vicerectors/es i/o persones designades pel rector/a amb competències en noves tecnologies, instal·lacions i edificis, organització.
- Vicerector o vicerectora amb competències en economia.

3. La presidència del CSI correspon al rector o rectora o al vicerector o vicerectora en qui delegui, i actua com a secretari o secretària la persona designada pel rector o rectora en matèria de noves tecnologies.

4. Podran assistir amb veu i sense vot a les sessions del CSI els delegats de protecció de dades (DPD), el director o directora del SRITIC i qualsevol persona que el CSI consideri convenient.

5. El Comitè de Seguretat de la Informació té les funcions següents:

- Promou la millora contínua del sistema de gestió de la seguretat de la informació.
- Elabora l'estratègia d'evolució de la URV pel que fa a la seguretat de la informació.
- Revisa anualment la política de seguretat de la informació que ha de ser aprovada pel Consell de Govern.
- Proposa al Consell de Govern la normativa de seguretat de la informació de la URV.
- Proposa al rector o la rectora el nomenament de les figures següents: responsable de seguretat, responsable del CERT, responsable del sistema i administrador de seguretat del sistema.
- Supervisa les tasques de desenvolupament de l'Esquema Nacional de Seguretat.
- Determina els nivells de seguretat requerits pels diferents serveis.
- Avalua l'acompliment dels processos de gestió d'incidents de seguretat i recomana possibles actuacions respecte a aquests.
- Defineix i crea els grups de treball i/o totes les estructures que cregui necessàries pel correcte desplegament en l'organització dels principis de seguretat identificats en la present política.
- Totes aquelles altres funcions establertes en l'ENS o en les guies de seguretat que siguin d'aplicació.

5.1.2 Responsable de Seguretat:

El Responsable de Seguretat de la URV tindrà les següents funcions:

- Mantenir el nivell adequat de seguretat de la informació gestionada i dels serveis prestats pels sistemes.
- Realitzar o promoure les auditories periòdiques que permetin verificar l'acompliment de les obligacions de l'organisme en matèria de seguretat, per verificar-ne l'acompliment.
- Promoure la formació i conscienciació en matèria de seguretat TIC.
- Proposar al CSI les categories dels sistemes d'informació.
- Verificar que les mesures de seguretat establertes son adequades per les necessitats de l'entitat (la protecció de la informació gestionada i els serveis prestats).
- Revisar, analitzar, completar i aprovar tota la documentació relacionada amb la seguretat del sistema d'informació.
- Monitoritzar l'estat de seguretat del sistema d'informació proporcionat per les eines de gestió d'incidents de seguretat i mecanismes d'auditoria implementats en el sistema d'informació.
- Donar suport i supervisar la investigació dels incidents de seguretat des de la seva notificació fins a la seva resolució.
- Elaborar l'informe periòdic de seguretat pel Comitè de Seguretat de la Informació, incloent els incidents TIC més rellevants del període.
- Aprovació dels procediments de seguretat fets pel Responsable del sistema.

- Elaboració de la normativa de seguretat.
- Totes aquelles altres funcions establertes en l'ENS o en les guies de seguretat que siguin d'aplicació.

5.1.3 Responsable del CERT (Computer Emergency Response Team):

El Responsable del CERT de la URV tindrà les següents funcions:

- Informar al Responsable de Seguretat i a l'OCAS (Òrgan de coordinació i assessorament en matèria de seguretat) dels incidents de seguretat dels sistemes de la informació.
- Fer el seguiment dels incidents de seguretat dels sistemes de la informació, la investigació i resolució d'incidents de seguretat, des de la seva detecció fins la resolució.
- Totes aquelles altres funcions establertes en l'ENS o en les guies de seguretat que siguin d'aplicació.

5.1.4 Responsable del sistema:

El Responsable del sistema de la URV tindrà les funcions següents:

- Gestionar el sistema d'informació durant tot el seu cicle de vida, des de l'especificació, instal·lació fins el seguiment del seu funcionament.
- Definir els criteris d'ús i els serveis disponibles al sistema d'informació.
- Definir les polítiques d'accés d'usuaris al sistema d'informació.
- Aprovar els canvis que afectin a la seguretat del mode de funcionament del sistema d'informació.
- Determinar la configuració autoritzada de hardware i software a utilitzar en el sistema d'informació i aprovar les modificacions importants de dita configuració.
- Participar en l'anàlisi i gestió de riscos del sistema d'informació.
- Elaborar i aprovar la documentació de seguretat del sistema d'informació.
- Participar en la categorització del sistema d'informació segons el procediment en l'Annex I de l'ENS.
- Implantar i controlar les mesures específiques de seguretat del sistema d'informació.
- Establir els plans de contingència i emergència, duent a terme exercicis freqüents per que el personal estigui familiaritzat amb aquests.
- Suspensió de la gestió de certa informació o de la prestació d'un servei si es detecten deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts.
- Totes aquelles altres funcions establertes en l'ENS o en les guies de seguretat que siguin d'aplicació.

5.1.5 Administrador de Seguretat del sistema:

L'Administrador de seguretat del sistema de la URV tindrà les funcions següents:

- La implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació.
- La gestió, configuració i actualització, si escau, del hardware i software en els que es basen els mecanismes i serveis de seguretat del sistema d'informació.

- La gestió de les autoritzacions concedides als usuaris del sistema d'informació, en particular els privilegis concedits, incloent la monitorització de que l'activitat desenvolupada en el sistema s'ajusta a allò autoritzat.
- L'aplicació dels procediments operatius de seguretat.
- Aprovar els canvis en la configuració vigent del sistema d'informació.
- Assegurar que els controls de seguretat establerts s'acompleixen estrictament.
- Assegurar que s'apliquen els procediments aprovats per gestionar el sistema d'informació.
- Supervisar les instal·lacions de hardware i software, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- Monitoritzar l'estat de seguretat del sistema d'informació proporcionat per les eines de gestió d'events de seguretat i mecanismes d'auditoria tècnica implementats en el sistema d'informació.
- Informar als Responsables de la Seguretat i del sistema 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 la resolució.
- Totes aquelles altres funcions establertes en l'ENS o en les guies de seguretat que siguin d'aplicació.

5.2 Mecanismes de coordinació i assessorament

Es crearà l'Òrgan de Coordinació i Assessorament en Seguretat (OCAS), integrat pels delegats de protecció de dades, que desenvoluparan les funcions pròpies del DPD a la Universitat i també s'encarregaran de l'impuls i la coordinació de la seguretat de la informació a la URV, i particularment de la implantació de l'ENS.

5.3 Grups de treball especialitzats

Els Grups de treball de la URV seran definits i creats pel CSI per donar suport en el desenvolupament de llurs funcions, així com proposar les mesures que considerin adequades en matèria de seguretat de la informació.

5.4 Resolució de conflictes

En cas de conflicte entre els diferents responsables, aquest es resoldrà pel superior jeràrquic dels mateixos. En defecte de l'anterior, prevaldrà la decisió del Comitè de Seguretat de la Informació de la URV.

6 DADES DE CARÀCTER PERSONAL

La URV realitza tractaments de dades en els que es fa ús de dades de caràcter personal. El RGPD requereix que les organitzacions creïn codis de conducta on es recullin normes dirigides al compliment del RGPD i la legislació nacional que reguli la protecció de les dades personals. Pel que fa a les mesures de seguretat de les dades a les administracions són d'aplicació els procediments i mesures regulades en la legislació i normativa vigent.

7 GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats. Aquesta anàlisi es repetirà:

- Quan canviï la informació manejada
- Quan canviïn els serveis prestats
- Quan passi un incident greu de seguretat
- Quan es reportin vulnerabilitats greus

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat de la Informació establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats. El Comitè dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent actuacions de caràcter horitzontal.

8 GESTIÓ D'INCIDENTS DE SEGURETAT

La Universitat ha de disposar d'un servei de resposta davant d'incidents de seguretat que estigui dotat dels mitjans necessaris per implantar i gestionar totes i cadascuna de les mesures de seguretat requerides en cada sistema d'informació per donar resposta als incidents de seguretat que es produeixin.

Aquest servei podrà efectuar les auditories de seguretat que consideri oportunes i necessàries sobre qualsevol equip connectat a la xarxa de la Universitat, podent procedir a la seva desconnexió o aïllament en aquells casos que suposin un risc potencial o real per a la resta dels sistemes d'informació o usuaris de la URV.

Tanmateix, qualsevol usuari ha de traslladar incidents, suggeriments i/o debilitats que puguin tenir relació amb la seguretat de la informació i les directrius contingudes en la present política.

9 DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta Política de Seguretat serà desenvolupada per normatives, instruccions o procediments de seguretat que estaran a disposició de tots els membres de la comunitats universitària que necessitin conèixer-la a través de la pàgina web de la Universitat o la intranet, segons escaigui.

10 OBLIGACIONS DEL PERSONAL

Tots els membres de la URV tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la normativa i instruccions de seguretat i de protecció de dades de caràcter personal, i és responsabilitat del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi als afectats.

L'objectiu és aconseguir la plena consciència respecte a que la seguretat de la informació i la protecció de dades afecta tots els membres de la URV i a totes les activitats, així com l'articulació dels mitjans necessaris perquè totes les persones que intervenen en el procés i els seus responsables jeràrquics tinguin sensibilitat cap als riscos que es corren.

Es formarà adequadament a tota la comunitat universitària en matèria de seguretat i protecció de dades i s'establirà un programa de conscienciació contínua per atendre tots els membres de la URV, en particular els de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessitin per realitzar-la. La formació serà obligatòria abans d'assumir una responsabilitat,

tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

11 TERCERES PARTS

Quan la URV presti serveis a altres organismes o manegi informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals per a informe i coordinació dels respectius comitès de seguretat i s'establiran procediments d'actuació per a la reacció davant d' incidents de seguretat.

Quan la URV utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la normativa i instruccions de seguretat que pertoqui a aquests serveis o informació.

Aquesta tercera part queda subjecta a les obligacions que estableix la normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política.

Quan algun aspecte de la política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

12 ANNEX. GLOSSARI DE TERMES

Anàlisi de riscos

Utilització sistemàtica de la informació disponible per identificar perills i estimar els riscos.

Dades de caràcter personal

Qualsevol informació sobre una persona física identificada o identificable.

Delegat/da de protecció de dades

Persona/es designada/es pel rector/a per exercir les funcions establertes en l'article 39 del Reglament europeu de protecció de dades.

Gestió d'incidents

Pla d'acció per a atendre les incidències que es donen. A més de resoldre-les, ha d'incorporar mesures d'acompliment que permeten conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.

Gestió de riscos

Activitats coordinades per dirigir i controlar una organització respecte els riscos.

Incident de seguretat

Succés inesperat o no desitjat amb conseqüències que van en detriment de la seguretat del sistema d'informació, el servei o la informació en si mateixa.

Servei

Funció o prestació exercida per alguna entitat oficial destinada a cuidar interessos o a satisfer necessitats dels ciutadans.

Sistema d'informació

Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre.