RESOLUCIÓ de 1 d'octubre de 2018, del Rectorat de la Universitat Jaume I, per la qual s'aprova la política de seguretat de la informació de la Universitat Jaume I i s'estableix la seua organització

La informació és un dels actius principals de la Universitat Jaume I i resulta fonamental per a la realització dels seus fins. D'altra banda, les tecnologies de la informació i les comunicacions, en l'ús i implantació de les quals la Universitat ha sigut sempre capdavantera, faciliten el tractament de la informació i milloren la gestió que es fa d'aquesta en tots els àmbits de la institució. Tot i això, les considerables millores que les tecnologies de la informació i les comunicacions suposen per a la comunitat universitària no estan exemptes de riscos i, en conseqüència, cal establir mesures específiques per a protegir tant els actius d'informació com els sistemes en els quals es tracten, i garantir la prestació dels serveis universitaris.

La preocupació de la Universitat Jaume I per la seguretat de la informació es va formalitzar per primera vegada amb la Resolució d'1 de desembre de 2009, del Rectorat de la Universitat Jaume I, relativa a la política de seguretat de la informació de la Universitat Jaume I i a la delegació de firma de resolucions i d'actes administratius relacionats amb el Sistema de gestió de la seguretat de la informació institucional. El contingut d'aquella va ser modificat posteriorment per Resolució de 15 de febrer de 2012 del Rectorat de la Universitat Jaume I. En ambdues resolucions s'establia la política de seguretat institucional i es donava publicitat a les normes que la desenvolupaven a través de la pàgina principal del portal de la Universitat. Igualment, s'aprovava el Sistema de gestió de la seguretat de la informació institucional i s'instava totes les persones que formen part de la comunitat universitària a conèixer, complir i fer complir, tant la política de seguretat, com els procediments i normes que la portaven a terme. Addicionalment, s'acordava, per a aconseguir una major eficiència en la gestió, delegar en el vicerector o vicerectora amb competències sobre tecnologies de la informació la firma de les resolucions i actes administratius relacionats amb l'aprovació de normes i procediments vinculats al Sistema de gestió de la seguretat de la informació de la Universitat. Finalment, per resolució de 30 de gener de 2014, del Rectorat de la Universitat Jaume I, per la qual s'aprovava la política de seguretat de la informació de la Universitat Jaume I i s'establia la seua organització, es complia allò que disposa el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema nacional de seguretat en l'àmbit de l'administració electrònica i que, en l'article 11 imposa als òrgans superiors de totes les administracions públiques l'obligació de dotar-se formalment d'una política de seguretat, aprovada pel titular de l'òrgan. La mateixa disposició estableix que tenen la consideració d'òrgans superiors i, en conseqüència, la responsabilitat abans assenyalada, els responsables directes de l'acció de govern en un sector d'activitat específic.

La seguretat de la informació té com a objectiu reduir, fins a un nivell que resulte acceptable, els riscos a què estan sotmesos la informació, els sistemes i els serveis que donen suport a l'activitat universitària. Aquest nivell acceptable no pot ser fixat arbitràriament, sinó que ha de respondre a una valoració conjunta de la gravetat de les amenaces, els recursos disponibles, el respecte als drets individuals i el compliment normatiu. Només els òrgans de direcció de la Universitat tenen les competències necessàries per a establir aquest nivell, ordenar les actuacions necessàries en matèria de seguretat de la informació i habilitar els mitjans necessaris per a portar-les a terme. En aquest sentit, resulta imprescindible establir una política de seguretat de la informació i una organització d'aquesta que garantisca la correcta distribució de tasques i responsabilitats, i l'aprovació de les disposicions necessàries que regulen la presa de decisions i els mecanismes de coordinació amb altres estructures de la Universitat, de

gestió de la innovació, de desenvolupament d'aplicacions i de serveis prestats per al compliment del que preveu aquesta política, i que conformaran el document marc de govern de bones pràctiques en la gestió del procés tecnològic a la Universitat.

L'actualització de l'Esquema nacional de seguretat amb el RD 951/2015, de 23 d'octubre i l'aprovació del Reglament general de protecció de dades (RGPD 2016/679 de 27 d'abril), que està vigent des de maig de 2016 però l'aplicació del qual s'ha diferit fins al maig de 2018, tracten d'harmonitzar la seguretat de la informació i la protecció dels drets i les llibertats fonamentals de les persones físiques en relació amb les activitats de tractament de dades de caràcter personal entre els estats membres de la Unió Europea.

És per tot això que cal actualitzar la política de seguretat, les mesures tècniques, organitzatives, de control i de govern dels procediments del Sistema de gestió de la seguretat de la informació, a les noves disposicions normatives, que han de ser aprovades pel titular de l'òrgan.

Els Estatuts de la Universitat Jaume I, aprovats pel Decret 116/2010, de 27 d'agost, del Consell de la Generalitat Valenciana, i modificats pel Decret 67/2013, de 7 de juny, estableixen que la Universitat és una institució de dret i interès públic amb personalitat jurídica pròpia i atribueixen al rector les competències i les facultats de direcció i representació d'aquesta.

Per tot l'exposat, en l'exercici de les atribucions per a les quals em faculta la llei,

RESOLC

Aprovar les normes que regulen la política de seguretat de la informació de la Universitat Jaume I i estableixen la seua organització, que es detallen en els articles següents:

Capítol I

Objecte i àmbit d'aplicació

Article 1. Objecte

Aquesta resolució té per objecte definir i regular la política de seguretat que cal aplicar en el tractament de la informació que s'origina com a conseqüència de l'activitat en la Universitat i el seu sector públic instrumental i establir les diferents funcions i responsabilitats en matèria de seguretat de la informació i de govern.

Article 2. Àmbit d'aplicació

Aquesta política de seguretat cal aplicar-la a tota la informació que es genere com a conseqüència de les activitats de la Universitat, així com al tractament del qual puga ser objecte, independentment que aquest siga manual o automatitzat, i que incloga o no dades de caràcter personal.

Article 3. Principi general d'actuació

1. La seguretat de la informació depèn de totes les persones que participen en el seu tractament i compromet la totalitat de la comunitat universitària. La Universitat ha d'establir els mecanismes necessaris perquè tot el personal propi que accedisca o tracte informació corporativa es comprometa a fer-ne un ús correcte, a accedir únicament a la indispensable per al desenvolupament de les seues funcions, a respectar aquesta política i les mesures de seguretat establertes i a notificar, per mitjà del procediment formal que

es determine, qualsevol incident o punt feble que detecte en el tractament de la informació.

2. L'alumnat, igual que la resta de membres de la comunitat universitària, es compromet, en el moment de fer efectiva la matrícula, a fer un ús correcte de la informació que es posa al seu abast i dels sistemes que la tracten, així com a respectar aquesta política i les mesures de seguretat establertes. Igualment, ha de ser informat dels mitjans adients per a la notificació de qualsevol incident relacionat amb el tractament d'informació o de les seues dades personals.

3. Als efectes previstos en aquesta resolució, les definicions, termes i expressions han de ser interpretats d'acord amb el sentit indicat en el glossari de termes que s'inclou com a annex.

Article 4. Conscienciació i formació del personal

1. El personal que participe en el tractament d'informació o tinga accés als locals on es custodie la informació o es realitze el tractament d'aquesta, ha de tenir especial cura a observar i fer observar les mesures de seguretat establertes. Aquestes obligacions són independents del tipus de relació jurídica que es mantinga amb la Universitat.

2. En les relacions amb terceres parts, proveïdors externs o contractistes, les unitats responsables han de vetlar perquè s'incloguen en els contractes o convenis les clàusules adients perquè, en el cas que siga necessari o possible l'accés a informació de la Universitat per part del personal d'aquelles, es faça respectant el que es preveu en la política de seguretat de la informació de la Universitat. En tot cas, quan el personal afectat per alguna de les condicions indicades estiga contractat per una empresa de serveis o forme part d'alguna entitat col·laboradora, el compliment de les disposicions d'aquesta política s'ha d'incloure en els contractes o convenis que regulen la relació entre la Universitat i l'empresa o entitat.

3. Es desenvoluparan activitats formatives específiques orientades a la conscienciació i formació dels empleats i empleades, així com a la difusió entre aquests d'aquesta política i del seu desenvolupament normatiu.

Article 5. Compliment

1. El compliment del que es preveu en aquesta política de seguretat té caràcter obligatori per a tots els membres de la comunitat universitària i per a les terceres persones que tinguen accés als sistemes d'informació universitaris o en facen ús.

2. L'incompliment de la política de seguretat pot tenir conseqüències disciplinàries, d'acord amb el règim sancionador aplicable en cada cas, sense perjudici d'altres responsabilitats en què es puga incórrer.

3. La Universitat Jaume I ha de publicar, donar a conèixer i facilitar el compliment d'aquesta política i dels documents que la despleguen recollits en el Sistema de gestió de la seguretat de la informació. Així mateix, ha d'habilitar canals de participació que permeten, tant als membres de la comunitat universitària, com a terceres persones afectades per aquesta, participar en la seua revisió i millora, així com aportar informació que servisca per a verificar-ne l'aplicació i efectivitat.

Capítol II

Principis de la seguretat de la informació

Article 6. La seguretat de la informació en la Universitat Jaume I

1. La seguretat de la informació és el resultat d'un procés que depèn del conjunt de factors humans, tècnics, materials i organitzatius que intervenen en el tractament d'aquesta.

2. Tots els membres de la comunitat universitària estan obligats a col·laborar en la prevenció, detecció i control dels riscos derivats d'actuacions negligents, ignorància de les normes, fallades tècniques o errades de coordinació, organització i direcció.

3. El Sistema de gestió de la seguretat de la informació és l'instrument del qual es dota la Universitat per a garantir la integritat, la confidencialitat, la disponibilitat i l'autenticitat de la informació que tracta, així com per a garantir el compliment normatiu, el govern i la traçabilitat de les accions que es porten a terme sobre aquesta.

4. El Sistema de gestió de la seguretat de la informació ha d'estar sotmès a monitoratge, control i millora continus per tal de mantenir-ne l'eficàcia davant la constant evolució de les amenaces, dels sistemes tècnics de protecció i dels sistemes que la tracten.

5. El Sistema de gestió de la seguretat de la informació disposarà dels mecanismes adients per a identificar i mantenir actualitzat el conjunt normatiu que conforma el marc legal vigent, especialment el relacionat amb l'Esquema nacional de seguretat i la protecció de dades, per a garantir el seu compliment.

Article 7. Gestió de riscos

1. L'article 6 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema nacional de seguretat estableix que l'anàlisi i la gestió dels riscos són parts essencials del procés de seguretat i han de mantenir-se permanentment actualitzades.

2. La gestió de riscos ha de permetre el manteniment d'un entorn controlat, que minimitze els riscos fins a nivells acceptables i que involucre els òrgans de direcció de la Universitat en l'acceptació d'un determinat risc residual.

3. L'anàlisi i gestió dels riscos s'han de fer d'acord amb eines i metodologies comunament acceptades per altres administracions públiques de l'entorn.

4. L'anàlisi i la gestió de riscos han d'estar presents en totes les fases del cicle de vida de les aplicacions i dels serveis i sistemes que donen suport al tractament de la informació. La selecció i l'aplicació dels controls de seguretat, així com l'avaluació de la seua eficiència, s'han de tenir en compte durant el disseny, construcció, contractació, adquisició, explotació i terminació o cancel·lació de les aplicacions, sistemes i serveis mencionats.

5. El model de govern de les TI de l'UJI descriurà entre altres totes les fases del cicle de vida de les aplicacions i dels serveis i sistemes que donen suport al tractament de la informació, inclourà l'anàlisi i la gestió de riscos de qualsevol iniciativa, tant en la fase d'aprovació com en la d'acceptació de les aplicacions i dels serveis i sistemes que donen suport al tractament de la informació. I mantindrà un registre actualitzat del conjunt d'iniciatives en forma de cartera de projectes TI, així com de les disposicions administratives necessàries que garantisquen el cicle de vida dels actius i els seus tractaments, i que serà accessible a tota la comunitat d'usuaris interns i externs.

6. Les diferents unitats administratives i departaments de la Universitat han de valorar especialment, en els processos de contractació, les empreses, productes i serveis que puguen acreditar un determinat nivell de seguretat.

7. Els responsables de la seguretat de la informació han d'elaborar un informe anual sobre l'estat de la seguretat, els riscos previsibles i els plans d'actuació recomanats.

Article 8. Classificació de la informació

Els actius d'informació que tracta la Universitat han d'estar inventariats i classificats. El nivell de protecció i les mesures de seguretat que s'han d'aplicar a la informació es basaran en la seua classificació.

Article 9. Planificació i coordinació

1. Periòdicament, la Universitat ha de definir un conjunt d'objectius de seguretat que han d'incloure una descripció de la línia o línies d'actuació previstes, els projectes en què es concreten, els objectius que s'han d'assolir i els indicadors de compliment i progrés corresponents. Aquests objectius, que han de prendre en consideració els resultats de les auditories i de l'anàlisi de riscos, s'han de revisar anualment.

2. La comissió competent haurà d'emetre informe del resultat de les auditories i de l'anàlisi de riscos.

3. L'esquema organitzatiu de la seguretat de la informació inclou els òrgans de coordinació i decisió necessaris per a l'aplicació i control de les mesures de seguretat.

Article 10. Accés a la informació

1. Les persones que tracten informació de la Universitat que no tinga el caràcter de pública han d'estar degudament acreditades i identificades per unes credencials electròniques personals i intransferibles.

2. Els privilegis d'accés a la informació s'han de limitar als que siguen estrictament imprescindibles per al desenvolupament de les funcions de cadascú.

3. Els accessos a la informació que impliquen modificacions d'aquesta o que suposen l'accés a dades a les quals s'apliquen mesures de seguretat de nivell alt segons la normativa vigent han de quedar enregistrats amb el nivell de detall suficient per a garantir el compliment normatiu i la traçabilitat de les accions efectuades.

Article 11. Registre d'activitat

Les actuacions de les persones, com que formen part de tractaments d'informació, poden ser enregistrades en aplicació de les exigències legals de traçabilitat o per a verificar el compliment d'aquesta política.

Article 12. Confidencialitat i deure de secret

Les persones que tracten informació de la Universitat que no tinga el caràcter de pública han d'observar la necessària reserva, confidencialitat i sigil respecte de les dades. Aquesta obligació perdura després d'haver finalitzat el vincle amb la Universitat.

Article 13. Instal·lacions i equipament

Les infraestructures informàtiques i de comunicacions que no formen part dels llocs de treball han d'ubicar-se en àrees aïllades, d'accés restringit i suficientment protegides.

Article 14. Sistemes d'informació

1. Els responsables de les diferents unitats organitzatives de la Universitat són responsables dels sistemes d'informació que donen suport als processos que desenvolupen.

2. Els sistemes d'informació han de proporcionar la funcionalitat estrictament necessària per a complir la finalitat que haja motivat el seu disseny o adquisició. Aquesta finalitat ha d'estar documentada i formalment aprovada pels seus responsables.
3. Les funcions d'operació, administració, manteniment i registre d'activitat han d'estar documentades i subjectes a control.

Article 15. Protecció de la informació no automatitzada

La informació en suport no electrònic ha de ser protegida amb el mateix nivell de seguretat que la que haja sigut sotmesa a tractament automatitzat.

Capítol III

Organització de la seguretat de la informació

Article 16. Separació de funcions

L'organització de la seguretat de la informació estableix una clara segregació de funcions entre responsable de la informació, responsable del servei i responsable de seguretat:

- Les funcions de seguretat de la informació, les de control i auditoria, i les relacionades amb la protecció de dades, les exerceix l'Oficina d'Innovació i Auditoria TI.
- La seguretat física de les instal·lacions correspon a l'Oficina Tècnica d'Obres i Projectes.
- Les funcions d'analitzar, desenvolupar i mantenir el programari corporatiu corresponen a la Unitat d'Anàlisis i Desenvolupament TI, de forma que establirà els requisits tècnics necessaris d'arquitectura i de desplegament de la solució per al seu correcte funcionament.
- El Servei d'Informàtica desenvolupa, en l'àmbit de les funcions previstes en l'article 34 dels Estatuts de la Universitat Jaume I, les que li corresponen segons l'objecte d'aquesta norma.
- Aquesta divisió de responsabilitats garanteix la separació de funcions i independència assenyalada en el paràgraf anterior.

Article 17. Responsable de la informació

1. La funció de responsable de la informació ha de ser exercida pel secretari o secretària general de la Universitat.

2. El responsable de la informació assoleix les funcions que la normativa vigent atribueixen al responsable dels fitxers amb dades de caràcter personal i promourà la designació d'un delegat o delegada de Protecció de Dades segons el que es preveu en el Reglament (UE) 679/2016.

3. Les funcions del responsable de la informació són les següents:

- Assolir la responsabilitat última de qualsevol error o negligència que provoque un incident de confidencialitat o d'integritat.
- Prendre decisions de caràcter directiu sobre l'ús que cal fer de la informació de la Universitat, tant de caràcter personal, com de qualsevol altra naturalesa, i independentment del mitjà que es faça servir per al seu tractament.
- Determinar el nivell de seguretat que cal aplicar a la informació.

- Complir les directrius del Sistema de gestió de la seguretat de la informació.
- Proposar millores en l'organització de la seguretat de la informació.

Article 18. Responsable del servei

1. La funció de responsable del servei de la Universitat Jaume I, l'ha d'exercir el vicerector o vicerectora competent en matèria de tecnologies de la informació.

2. Les funcions del responsable del servei són les següents:

- Responsabilitzar-se de la prestació de serveis basats en sistemes de la informació de la Universitat.
- Complir les directrius del Sistema de gestió de la seguretat de la informació.
- Determinar el nivell de seguretat que cal aplicar als serveis.
- Garantir la prestació del servei en condicions òptimes de disponibilitat, accessibilitat o d'interoperabilitat.
- Promoure l'establiment d'acords de servei.
- Assumir la responsabilitat última de qualsevol error o negligència que provoque un incident de disponibilitat, accessibilitat o d'interoperabilitat.

Article 19. Responsable de seguretat

1. El responsable de seguretat de la Universitat té l'obligació de vetlar per la seguretat de la informació, dels serveis prestats pels sistemes d'informació i dirigir el Sistema de gestió de la seguretat de la informació, d'acord amb allò que estableix aquesta política de seguretat i la normativa vigent que aplica.

2. La figura de responsable de seguretat de la Universitat Jaume I l'ha d'exercir la persona titular de la Gerència, que delegarà les funcions de responsable de seguretat de la informació que estableix la normativa vigent en l'Oficina d'Innovació i Auditoria TI per tal de garantir, en tot cas, la separació de funcions i la independència amb el responsable del servei. No podrà, per tant, prendre decisions sobre l'existència de tractaments de dades o sobre la manera en què van a ser tractades les dades.

3. Les funcions del responsable de seguretat són les següents:

- Informar i retre comptes tant al responsable del servei com al responsable de la informació.
- Planificar les auditories necessàries per a garantir el compliment de la legalitat vigent i el cicle de vida del Sistema de gestió de la seguretat de la informació.
- Analitzar els riscos que afronta la Universitat i prendre decisions sobre la manera de tractar-los, i aprovar la declaració d'aplicabilitat de les mesures de protecció.
- Fixar objectius de seguretat i planificar-ne l'execució.
- Promoure'n l'adequació a les normatives.
- Gestionar la reputació de la Universitat i les expectatives dels usuaris i usuàries dels sistemes.

- Vetlar perquè s'establisquen mecanismes de continuïtat de les activitats davant d'incidents de seguretat.
- Supervisar l'eficàcia de les mesures de seguretat establides per a protegir la informació i garantir la disponibilitat i correcte funcionament dels serveis prestats pels sistemes d'informació.
- Promoure activitats de formació i conscienciació en matèria de seguretat

Article 20. Responsable d'auditoria de tecnologies de la informació

1. La funció de responsable d'auditoria de tecnologies de la informació l'exerceix el cap de l'Oficina d'Innovació i Auditoria TI que pot delegar determinades funcions. Aquestes delegacions, que s'han de fer d'acord amb criteris tècnics, s'han de fer constar en els procediments del Sistema de gestió de la seguretat de la informació o bé han d'estar predeterminades en el catàleg de funcions i competències del servei.

2. Les funcions de responsable d'auditoria de tecnologies de la informació són les següents:

- Assolir les funcions delegades de responsable de seguretat de la informació previstes en la normativa vigent.
- Mantenir i coordinar el Sistema de gestió de la seguretat de la informació i la política, les normes i procediments que el componen.
- Informar i retre comptes al responsable de seguretat en matèria de seguretat de la informació.
- Informar i retre comptes al responsable de la informació en assumptes relacionats amb la protecció de dades de caràcter personal.
- Determinar la categoria de cada sistema, d'acord amb els nivells de seguretat decidits pel responsable de la informació i el responsable del servei.
- Analitzar els riscos dels sistemes i elaborar la declaració d'aplicabilitat de les mesures de protecció.
- Promoure l'adopció de les mesures tècniques necessàries per a la protecció de la informació.
- Coordinar l'auditoria dels sistemes i la informació.
- Elaborar les polítiques i normes de seguretat.
- Fer l'anàlisi dels informes d'auditoria, l'elevació al responsable del fitxer de les recomanacions i mesures correctores oportunes, la supervisió dels registres d'accés, la revisió dels registres d'incidències i l'actualització del document de seguretat per a la protecció de dades de caràcter personal.
- Promoure la formació del personal a càrrec seu en matèries de seguretat.
- Responsabilitzar-se de coordinar l'actualització del catàleg d'actius modelitzats i les seues regulacions administratives, dels procediments del SGSI i informar de qualsevol incident de seguretat crític al responsable de seguretat.

Article 21. Responsable del sistema

1. La funció de responsable del sistema, l'exerceix el cap del Servei d'Informàtica, que pot delegar determinades funcions en els administradors de seguretat. Aquestes delegacions, que s'han de fer d'acord amb criteris tècnics, s'han de fer constar en els procediments del Sistema de gestió de la seguretat de la informació o bé han d'estar predeterminades en el catàleg de funcions i competències del servei.

2. Les funcions del responsable del sistema són les següents:

- Informar i retre comptes al responsable de seguretat en matèria de seguretat de la informació.
- Informar i retre comptes al responsable del servei.
- Analitzar els riscos que afronten els sistemes de tractament de la informació i prendre decisions sobre la manera de tractar-los.
- Assumir la responsabilitat tècnica sobre la prestació dels serveis basats en sistemes de la informació de la Universitat i la seua interoperabilitat.
- Supervisar l'adquisició, operació i manteniment dels sistemes durant tot el cicle de vida.
- Definir els principis de gestió de cada sistema i establir els criteris d'ús i els serveis disponibles.
- Assegurar-se que les mesures generals i polítiques de seguretat estan integrades en els sistemes.
- Prendre decisions urgents en matèria de suspensió o interrupció temporal del servei, si es detecten deficiències greus de seguretat.
- Vetlar per l'elaboració dels procediments operatius de seguretat.
- Proposar plans i objectius de millora de la seguretat.
- Promoure la formació del personal a càrrec seu en matèries de seguretat.
- Elaborar els plans de continuïtat.
- Gestionar els acords de nivell de servei i d'interoperabilitat.
- Responsabilitzar-se de la seguretat física de les instal·lacions, en coordinació amb l'Oficina Tècnica d'Obres i Projectes, i de la gestió del personal a càrrec seu.
- Responsabilitzar-se de mantenir actualitzats els catàlegs d'actius modelitzats i les seues regulacions administratives, els procediments del SGSI i informar de qualsevol incident de seguretat crític al responsable de seguretat.

Article 22. Administradors de seguretat

1. Cal que hi haja un administrador o administradora de seguretat almenys per cadascuna de les àrees següents:

- Sistemes i Microinformàtica
- Comunicacions i Sistemes d'Informació
- Explotació
- Desenvolupament

El catàleg de funcions i competències del Servei d'Informàtica i de la Unitat d'Anàlisi i Desenvolupament TI ha de descriure quins llocs de treball inclouen aquestes responsabilitats.

2. El Servei d'Informàtica exerceix la funció d'administrador de seguretat de Sistemes i Microinformàtica, Comunicacions i Sistemes d'Informació, i d'Explotació. I les seues funcions són les següents:

- Assolir la responsabilitat del disseny, implantació i control de les mesures de seguretat que siguen d'aplicació en cadascuna de les àrees tècniques.
- Informar el responsable del sistema i els responsables de seguretat.
- Exercir les funcions delegades pel responsable del servei en el seu àmbit de competència.
- Implementar les mesures tècniques de seguretat en cada sistema i aplicar els procediments operatius.
- Portar a terme la gestió, configuració i actualització del maquinari i programari en què es basen els mecanismes de seguretat dels sistemes.
- Gestionar les autoritzacions d'ús i perfils d'accés als sistemes.
- Elaborar els plans de recuperació de sistemes.
- Promoure la formació del personal a càrrec seu en matèries de seguretat.
- Monitorar l'estat de seguretat dels sistemes i el compliment dels controls de seguretat de manera estricta.
- Registrar els incidents de seguretat i informar el responsable de seguretat i el responsable del servei.
- Col·laborar en la resolució i investigació d'incidents de seguretat.

3. La Unitat Anàlisis i Desenvolupament TI exerceix la funció d'administrador de seguretat de Desenvolupament. Les seues funcions són les següents:

- Informar i retre comptes al responsable de seguretat en matèria de seguretat de la informació.
- Analitzar els riscos que afronten les aplicacions de tractament de la informació i prendre decisions sobre la manera de tractar-los.
- Supervisar les aplicacions durant tot el cicle de vida.
- Assegurar-se que les mesures generals i polítiques de seguretat estan integrades en les aplicacions.
- Vetlar per l'elaboració dels procediments operatius de seguretat.
- Proposar plans i objectius de millora de la seguretat.
- Promoure la formació del personal a càrrec seu en matèries de seguretat.
- Responsabilitzar-se de la seguretat de la prestació de servei d'aplicacions, en coordinació amb el Servei d'Informàtica, i de la gestió del personal a càrrec seu.
- Responsabilitzar-se de mantenir actualitzat els catàlegs d'actius modelitzats i les seues regulacions administratives, els procediments del SGSI i informar de

qualsevol incident de seguretat crític al responsable d'auditoria de tecnologies de la informació.

Article 23. Comitè de Seguretat de la Informació

1. El Comitè de Seguretat de la Informació coordina la seguretat de la informació en la Universitat Jaume I.

2. El Comitè de Seguretat de la Informació està integrat per:

- El responsable de seguretat, que exerceix la presidència.
- El responsable de la informació.
- El responsable del servei.
- El responsable del sistema.
- El responsable d'auditoria de tecnologies de la informació, que exerceix la secretaria.
- El cap de la Unitat d'Anàlisi i Desenvolupament TI.
- Els directors i directores acadèmics implicats, si n'hi ha.

3. Són funcions del Comitè de Seguretat de la Informació les que a continuació s'enumeren:

- Dirigir l'estratègia corporativa en matèria de tecnologies de la informació i vetlar per l'aprovació i el compliment del marc de govern de bones pràctiques en la gestió del procés tecnològic a la Universitat, atès l'impacte que qualsevol iniciativa pot tenir en la seguretat.
- Transmetre les inquietuds del Consell de Direcció als diferents responsables de la seguretat.
- Proposar al Consell de Direcció els canvis en la política de seguretat.
- Aprovar les normes en matèria de seguretat de la informació i proposar-ne la ratificació per part del Consell de Direcció de la Universitat.
- Dirigir la política de comunicació de les qüestions relacionades amb la seguretat de la informació.
- Analitzar els resultats més significatius de les auditories periòdiques i de l'anàlisi de riscos.
- Prioritzar les línies d'actuació en matèria de seguretat sobre altres iniciatives o projectes, quan els recursos siguen limitats.
- Resoldre els conflictes de responsabilitats que puguen sorgir i que li siguen plantejats per la Comissió Tècnica de Projectes.
- Promoure activitats de formació i conscienciació en matèria de seguretat.

4. El Comitè de Seguretat de la Informació s'ha de reunir amb caràcter ordinari almenys una vegada a l'any i, amb caràcter extraordinari, quan així ho decidisca la presidència del Comitè.

5. El Comitè de Seguretat de la Informació pot sol·licitar del personal tècnic la informació pertinent per a la presa de decisions. En cas que aquest personal siga convocat

a les reunions del Comitè de Seguretat de la Informació, ho farà en qualitat de personal assessor, amb veu però sense vot.

6. El funcionament del Comitè de Seguretat de la Informació s'ha de regir pels principis següents:

- El president o presidenta, amb l'informe previ dels responsables de seguretat, ha d'establir l'ordre del dia i convocar les reunions.
- Les actes de les reunions del Comitè de Seguretat de la Informació tenen la classificació de confidencials i la difusió està restringida als membres que l'integren. El Comitè, durant les reunions, pot decidir quins aspectes de les seues decisions i deliberacions poden ser públics i l'abast de la comunicació.
- El Comitè queda vàlidament constituït quan compareguen almenys la meitat dels membres i estiga present el responsable del servei o el responsable de la informació. A més, per a garantir la segregació de funcions, han d'estar-hi presents el responsable de seguretat o el responsable de seguretat de la informació.
- Per a totes les comunicacions del Comitè de Seguretat de la Informació s'han de fer servir els mitjans electrònics corporatius.

7. El Comitè de Seguretat de la Informació ha d'ajustar el seu funcionament al Reglament d'organització i funcionament de la Universitat Jaume I i, supletòriament, als preceptes relatius als òrgans col·legiats previstos en la normativa en matèria de règim jurídic de les administracions públiques i de procediment administratiu vigent en cada moment.

Article 24. Comissió Tècnica de Projectes

1. La Comissió Tècnica de Projectes té la missió de vetlar per l'organització del procés tecnològic a la Universitat. En matèria de seguretat de la informació, la seua tasca és la d'analitzar l'impacte i coordinar les iniciatives concretes adreçades a evitar disfuncions que puguen possibilitar l'aparició d'errades o punts febles en els sistemes tant en l'àmbit organitzatiu com tècnic.

2. La Comissió Tècnica de Projectes està integrada per:

- El responsable de seguretat.
- El responsable del sistema.
- El responsable del servei.
- El responsable d'auditoria de tecnologies de la informació.
- El cap de la Unitat d'Anàlisi i Desenvolupament TI.
- Els administradors de seguretat.
- Un responsable tècnic de seguretat de la informació de l'Oficina d'Innovació i Auditoria TI, que actua com a secretari.
- Els directors i directores acadèmics implicats, si n'hi ha.

3. Són funcions de la Comissió Tècnica de Projectes les que a continuació s'enumeren:

- Atendre les inquietuds del Consell de Direcció i de les diferents unitats organitzatives i departaments de la Universitat en matèria de seguretat de la informació.
- Informar regularment de l'estat de la seguretat al Comitè de Seguretat de la Informació.
- Promoure la millora contínua del Sistema de gestió de la seguretat de la informació.
- Coordinar esforços en matèria de seguretat i elaborar les propostes d'estratègia de la seguretat.
- Proposar el nivell de risc residual acceptable per a la Universitat.
- Revisar periòdicament la política de seguretat per tal que s'adeqüe a la realitat dels sistemes i de l'organització de la Universitat i a l'estat de la tecnologia.
- Elaborar i revisar periòdicament les normes del Sistema de gestió de la seguretat de la informació perquè siguen aprovades pel Comitè de Seguretat de la Informació.
- Aprovar els procediments del Sistema de gestió de la seguretat de la informació.
- Monitorar les prestacions dels sistemes de seguretat i analitzar els indicadors de rendiment d'aquests.
- Promoure la realització d'auditories i determinar el seu abast.
- Prioritzar les actuacions en matèria de seguretat sobre altres iniciatives o projectes, quan els recursos siguen limitats.
- Promoure activitats de formació i conscienciació en matèria de seguretat.
- Aquelles que es decidisquen en el marc de govern de bones pràctiques en la gestió del procés tecnològic a la Universitat.

4. El funcionament de la Comissió Tècnica de Projectes es regeix per les regles següents:

- La Comissió queda vàlidament constituïda quan compareguen almenys la meitat dels membres sempre que, per a garantir la segregació de funcions, estiguen presents, d'una banda, el responsable de seguretat o el cap de l'Oficina d'Innovació i Auditoria TI o el responsable de seguretat de la informació, i d'una altra, el director acadèmic del Servei d'Informàtica, si n'hi ha, o el responsable del sistema o el responsable del Servei.
- El responsable de seguretat de la informació, com a secretari de la Comissió Tècnica de Projectes, ha d'elaborar l'ordre del dia, convocar les reunions de la Comissió i elaborar les actes on es reflectisquen els acords adoptats.
- Les actes de les reunions de la Comissió Tècnica de Projectes tenen la classificació de confidencials i la difusió d'aquestes està restringida al personal de la Universitat Jaume I o, després d'adoptar els acords de confidencialitat oportuns, a les empreses que presten serveis relacionats amb la seguretat o els sistemes d'informació.
- Per a totes les comunicacions s'han de fer servir els mitjans electrònics corporatius.

- En tot allò no previst, ha d'ajustar el seu funcionament al que estableix la normativa vigent en matèria de règim jurídic de les administracions públiques i de procediment administratiu.

Capítol IV

El Sistema de gestió de la seguretat de la informació

Article 25. Desenvolupament

1. El Sistema de gestió de la seguretat de la informació és l'instrument fonamental per a aconseguir les finalitats de la política de seguretat de la informació.

2. El Sistema de gestió de la seguretat de la informació s'ha de conformar segons estàndards generalment acceptats i, sempre que siga possible, s'ha de sotmetre anualment a la validació o certificació per part d'entitats externes independents de reconegut prestigi.

Article 26. Composició

1. El Sistema de gestió de la seguretat de la informació està constituït per un conjunt de documents que estableixen els principis que han de regir l'aplicació d'aquesta política.

2. Aquests documents han de preveure, almenys, els aspectes següents:

- Condicions per a l'accés a la informació.
- Ús de l'equipament informàtic i de comunicacions.
- Gestió d'incidències.
- Continuïtat de l'activitat.
- Classificació de la informació.
- Anàlisi i gestió de riscos.
- Seguretat física i de l'entorn.
- Còpies de seguretat.
- Auditories.
- Elaboració, publicació i revisió del sistema.
- Gestió documental del sistema.

Article 27. Aprovació i publicació dels documents del Sistema de gestió de la seguretat de la informació

1. Els documents que integren el Sistema de gestió de la seguretat de la informació han de ser aprovats pel Comitè de Seguretat de la Informació a proposta de la Comissió Tècnica de Projectes.

2. Els documents que hagen de ser coneguts per la generalitat dels usuaris i usuàries han de ser publicats en el portal de la Universitat Jaume I. Els canvis rellevants s'han de notificar mitjançant comunicació personalitzada i, preferiblement, requeriran l'acceptació expressa per part de la persona destinatària.

3. Els documents interns s'han de posar a l'abast del personal tècnic en els entorns habituals de treball.

Capítol V

Aprovació i revisió de la política de seguretat

Article 28. Aprovació, publicació i revisió periòdica

1. La política de seguretat de la informació ha de ser aprovada, a proposta del Comitè de Seguretat de la Informació, i amb l'informe previ del Consell de Direcció, per resolució del Rectorat de la Universitat Jaume I.

2. La política de seguretat de la informació s'ha de publicar en l'apartat de normativa de la seu electrònica de la Universitat i serà referenciada des del peu de totes les pàgines del portal corporatiu. En la mesura del que siga possible, totes les eines i aplicacions informàtiques desenvolupades per la Universitat Jaume I han d'incloure enllaços a aquesta política de seguretat.

3. La política de seguretat es revisarà com a mínim una vegada a l'any per tal d'ajustar-la a la normativa vigent en cada moment.

DISPOSICIÓ DEROGATÒRIA

Única

Queda sense efecte la resolució de 22 de febrer de 2018, del Rectorat de la Universitat Jaume I per la qual s'aprova la política de seguretat de la informació de la Universitat Jaume I i s'estableix la seua organització.

DISPOSICIÓ TRANSITÒRIA

Única

La competència en matèria d'explotació serà exercida pel Servei d'Informàtica a partir del moment en què dispose amb els mitjans adequats i suficients per a exercir-la. Mentrestant es continuarà funcionant com fins a la data.

DISPOSICIONS FINALS

Primera. Desenvolupament de la política

Es faculta la Secretaria General de la Universitat per a executar les disposicions necessàries en matèria de protecció de dades per al compliment del que preveu aquesta política.

Es faculta la Gerència per a executar les disposicions necessàries en matèria de seguretat de la informació, d'innovació i de desenvolupament d'aplicacions.

Es faculta la Gerència per a habilitar canals de participació que permeten, tant als membres de la comunitat universitària, com a terceres persones afectades per aquesta política, participar en la seua revisió i millora, així com aportar informació que servisca per a verificar-ne l'aplicació i efectivitat.

Es faculta la Gerència per a recollir el conjunt dels actius, de les seues regulacions, dels procediments del Sistema de gestió de la seguretat de la informació, de les estructures

previstes i de les pràctiques que s'apliquen en la seua gestió, en un marc de govern de bones pràctiques en la gestió del procés tecnològic a la Universitat, que caldrà aprovar i publicar, i que es mantindrà actualitzat.

Es faculta al vicerectorat competent en matèria de tecnologies de la informació per a executar les disposicions necessàries en matèria de prestació del servei basat en sistemes d'informació per al compliment del que preveu aquesta política.

Segona. Nomenaments

S'habilita la Gerència de la Universitat i el vicerectorat amb competències sobre el personal d'administració i serveis per a l'atribució de les funcions relacionades amb la seguretat de la informació, i no expressament previstes en aquesta política, als llocs de treball que les hagen de desenvolupar.

Tercera. Entrada en vigor

Aquesta resolució entra en vigor l'endemà de la seua publicació a la Seu Electrònica de la Universitat.

La rectora

Eva Alcón Soler

Castelló de la Plana, 1 d'octubre de 2018

ANNEX I. Definicions

Actiu: component o funcionalitat d'un sistema d'informació susceptible de ser atacat deliberadament o accidentalment amb conseqüències per a l'organització. Inclou: informació, dades, serveis, aplicacions, equips, comunicacions, recursos administratius, recursos físics i recursos humans.

Anàlisi de riscos: utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos als quals estan exposats els actius de la Universitat.

Auditoria: revisió i examen independents dels registres i activitats del sistema per a verificar la idoneïtat dels controls del sistema, assegurar que es compleixen les disposicions legals, la política de seguretat i els procediments operatius establits, detectar les infraccions de la seguretat i recomanar modificacions apropiades dels controls, de la política i dels procediments.

Categoria d'un sistema: és un nivell, dins de l'escala bàsica-mitjana-alta, amb el qual s'adjectiva un sistema a fi de seleccionar les mesures de seguretat necessàries per a aquest.

Confidencialitat: propietat o característica consistent en què la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.

Dades de caràcter personal: qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus concernent a persones físiques identificades o identificables.

Disponibilitat: propietat o característica dels actius consistent en el fet que les entitats o processos autoritzats tenen accés a aquests quan ho requereixen.

Fitxer no automatitzat: qualsevol conjunt de dades de caràcter personal organitzat de forma no automatitzada i estructurat d'acord amb criteris específics relatius a persones físiques, que permeten accedir sense esforços desproporcionats a les seues dades personals, tant al centralitzat, com al descentralitzat o al repartit de forma funcional o geogràfica.

Gestió d'incidents: protocol d'actuació per a atendre les incidències que ocórreguen. A més de resoldre-les, ha d'incorporar mesures d'exercici que permeten conèixer la qualitat del sistema de protecció i detectar tendències abans que es convertisquen en problemes greus.

Incidència: qualsevol anomalia que afecte o puga afectar la seguretat de les dades.

Integritat: propietat o característica consistent en el fet que l'actiu d'informació no ha sigut alterat de manera no autoritzada.

Mesures de seguretat: conjunt de disposicions encaminades a protegir-se dels riscos possibles sobre el sistema d'informació, a fi d'assegurar els seus objectius de seguretat. Pot tractar-se de mesures de prevenció, de dissuasió, de protecció, de detecció i reacció, o de recuperació.

Política de seguretat: conjunt de directrius plasmades en un document formalment aprovat, que regeixen la forma en què la Universitat gestiona i protegeix la informació i els serveis que considera crítics.

Procés tecnològic: conjunt d'iniciatives que permeten a la Universitat dotar-se de mitjans i sistemes per al tractament automatitzat de la informació.

Risc: estimació del grau d'exposició a què una amenaça es materialitze sobre un o més actius causant danys o perjudicis a l'organització.

Sistema de gestió de la seguretat de la informació (SGSI): sistema de gestió que, basat en l'estudi dels riscos, s'estableix per a crear, implementar, fer funcionar, supervisar, revisar, mantenir i millorar la seguretat de la informació. El sistema de gestió inclou l'estructura organitzativa, les polítiques, les activitats de planificació, les responsabilitats, les pràctiques, els procediments, els processos i els recursos.

Sistema d'informació: conjunt organitzat de recursos perquè la informació es puga recollir, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

Traçabilitat: propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

Vulnerabilitat: una debilitat que pot ser aprofitada per una amenaça.