Butlletí Oficial de la Universitat de Girona

Disposició	eBOU-1641	**BOU**	3/2019	**Data publicació**	22/07/2019
Òrgan	Consell de govern	**Sessió**	4/2019	**Data aprovació**	05/07/2019

Universitat de Girona

Aprovació de la política de seguretat en matèria de protecció de dades

eBOU-1641

Exposició de motius

Segons l'article 156.2 de la *Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic*, l'Esquema Nacional de Seguretat determina la política de seguretat en la utilització de mitjans electrònics en l'àmbit del sector públic, amb l'objectiu de garantir adequadament la seguretat de la informació tractada.

El *Reial Decret 3/2010, de 8 de gener*, aprovà l'Esquema Nacional de Seguretat. L'article 11 indica que els òrgans superiors de les administracions públiques han de disposar d'una política de seguretat que compleixi els principis que figuren en el propi Reial Decret i que prevegi el seu desenvolupament. La política de seguretat ha de ser aprovada per l'òrgan superior corresponent.

La política de seguretat és rellevant també des de la perspectiva de la protecció de les dades personals. La *Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals* indica a la seva disposició addicional primera que en l'aplicació de l'Esquema Nacional de Seguretat s'han d'incloure les mesures a implantar en cas de tractament de dades personals, per evitar-ne la pèrdua, l'alteració o l'accés no autoritzat, amb l'adaptació dels criteris de determinació del risc en el tractament de les dades a allò que estableix el Reglament General de Protecció de Dades.

En compliment de les esmentades normes la Comissió Tècnica de Gestió de la Informació en sessió núm. 1/2019 de 17 de maig de 2019 va aprovar la proposta següent de política de seguretat en matèria de seguretat de la informació, i

En virtut de les competències que l'article 66 dels Estatuts de la Universitat de Girona reserva al Consell de Govern, **s'ACORDA:**

Primer. Objectiu de la política de seguretat TIC

1. Constitueix l'objecte d'aquest document fixar la Política de Seguretat de la Informació (en endavant, PSI) en l'àmbit de l'administració electrònica de la Universitat de Girona reconeixent així com actius estratègics la informació i els sistemes que la suporten. La PSI serà d'obligat compliment per a tot el personal que accedeixi tant als sistemes d'informació com a la mateixa informació que sigui gestionada per cada àrea o centre, amb independència de quin sigui el seu destí, adscripció o relació amb la Universitat de Girona.

2. L'objectiu de la gestió de seguretat de la informació és alinear la seguretat de les tecnologies de la informació amb la general de la Universitat de Girona i garantir que la seguretat de la informació es gestioni de forma efectiva en totes les activitats de la gestió dels serveis TIC. La PSI protegeix la informació d'un ampli ventall d'amenaces, a fi de garantir la continuïtat dels sistemes d'informació, minimitzar els riscos i assegurar l'eficient compliment de les competències i funcions de la UdG.

3. Són objectius generals en matèria de seguretat de la informació:

a. Contribuir des de la gestió de la seguretat de la informació al compliment de la missió i objectius de la UdG.

b. Disposar de les mesures de control necessàries per al compliment dels requisits legals que siguin d'aplicació com a conseqüència de l'activitat desenvolupada, especialment pel que fa a la protecció de dades de caràcter personal i a la prestació de serveis a través de mitjans electrònics.

c. Assegurar l'accés, integritat, confidencialitat, disponibilitat, autenticitat, traçabilitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

d. Protegir els recursos d'informació i la tecnologia utilitzada per al seu processament, davant amenaces, internes o externes, deliberades o accidentals, amb la finalitat d'assegurar el compliment de la confidencialitat, integritat, disponibilitat, legalitat i fiabilitat de la informació.

4. Per tal de poder aconseguir aquests objectius la Universitat de Girona es compromet a:

1. Vetllar pel compliment d'aquesta política impulsant-la i donant-li suport amb els recursos humans, econòmics i materials que en siguin necessaris.

2. Complir amb la legislació vigent en matèria de seguretat, i en particular amb aquella relacionada amb l'esquema nacional de seguretat, la protecció de dades de caràcter personal, la propietat intel·lectual i industrial, i els serveis de la societat de la informació.

3. Realitzar de forma periòdica l'anàlisi de riscos sobre els actius que conformen els sistemes d'informació i tractar la seguretat com una part integral del seu cicle de vida.

4. Verificar que els sistemes compleixen les mesures de seguretat prèviament a la seva entrada en funcionament.

5. Avaluar regularment la seguretat dels sistemes.

6. Sol·licitar revisions periòdiques amb la finalitat d'obtenir una avaluació independent.

7. Difondre aquesta política a tot el personal de l'organització.

8. Fer formació en seguretat per al seu personal.

9. Revisar periòdicament aquesta política amb la finalitat de mantenir-la actualitzada i alineada amb els objectius de la Universitat de Girona i la legalitat vigent.

Segon. Desenvolupament de la política de seguretat TIC

1. La Política de Seguretat de la Informació de la Universitat de Girona es desenvoluparà mitjançat els següents instruments:

a. Normes de seguretat. Defineixen què s'ha de protegir i els requisits de seguretat desitjats. El conjunt de totes les normes de seguretat ha de cobrir la protecció de tots els entorns dels Sistemes d'Informació.

b. Procediments de seguretat. Descriuen de forma concreta tot el que s'ha definit a les normes de seguretat, així com les persones o grups responsables de la implantació, manteniment i seguiment del compliment. Especifiquen com dur a terme les tasques habituals, qui ha de fer cada tasca i com detectar i reportar comportaments anòmals. Es realitzaran els desenvolupaments següents:

- Procediment de classificació de la informació
- Procediment de seguretat lògica
- Procediment de gestió dels usuaris

- Procediment de gestió de riscos
- Procediment de gestió de les incidències
- Procediment de còpies de seguretat
- Procediment de gestió de suports i dispositius
- Procediment de monitorització
- Procediment de seguretat física

c. Guies de recomanacions i bones pràctiques. Addicionalment s'elaboraran altres guies de caràcter informatiu, amb l'objectiu d'ajudar els usuaris a aplicar correctament les mesures de seguretat.

2. La normativa de seguretat estarà a disposició de tot el personal de la Universitat.

Tercer. Marc normatiu

Es pren com a referència principal el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguridad a l'àmbit de l'Administració Electrònica. La present Política i el seu desenvolupament es fonamentaran en la normativa vigent en cada moment.

Quart. Àmbit d'aplicació.

1. La gestió de la seguretat de la informació ha de garantir l'adequat funcionament de les activitats de control, monitorització i manteniment de les infraestructures i instal·lacions generals, necessàries per a l'adequada prestació de serveis, així com de la informació derivada del funcionament dels mateixos.

2. Aquesta política serà d'aplicació i d'obligat compliment per a totes les àrees i serveis de la Universitat de Girona i dels ens que en depenguin en relació a les activitats i processos inclosos en el Real Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguridad a l'àmbit de l'Administració Electrònica.

Cinquè. Organització de la seguretat.

1. A efectes d'organització de la seguretat de la informació la Universitat de Girona identifica i diferencia les responsabilitats següents:

a) Responsable de la informació.

b) Responsable del servei.

c) Responsable de seguretat.

d) Responsable del sistema.

e) Comissió Tècnica de Gestió de la Informació.

2. Són funcions del responsable de la informació:

1. Determinar els requeriments de seguretat de la informació.
2. Aprovar els nivells de seguretat de la informació.

3. Col·laborar amb els responsables de seguretat i del sistema.

4. Aprovar instruccions que garanteixin la seguretat de la informació.

5. Vetllar per la inclusió de clàusules sobre seguretat en la contractació en general i especialment en els encàrrecs de tractament de dades, i verificar-ne el compliment.

3. Són funcions del responsable del servei:

1. Determinar els requeriments de seguretat dels serveis que es presten.

2. Aprovar els nivells de seguretat dels serveis.

3. Aplicar i fer aplicar els requeriments generals en matèria de seguretat en els serveis.

4. Col·laborar amb el responsable de la seguretat i del sistema en el manteniment i millora de la seguretat dels sistemes.

4. Són funcions del responsable de seguretat:

1. Determinar els requisits de seguretat de la informació i fer el seguiment de la seva aplicació. Aprovar els protocols de seguretat dels sistemes.

2. Proposar l'elaboració de normes, guies o instruccions de seguretat o la seva actualització.

3. Analitzar, completar i aprovar, si escau, la documentació relacionada amb la seguretat dels sistemes.

4. Ordenar les avaluacions internes i proposar les auditories periòdiques que permetin verificar el compliment de les obligacions en matèria de seguretat.

5. Donar suport a la investigació d'incidents de seguretat.

6. Vetllar perquè les empreses subcontractades que administrin infraestructures TIC de la Universitat o proporcionin recursos, sistemes o serveis, coneguin i apliquin les normatives de seguretat.

7. Elaborar informes periòdics de seguretat.

5. Són funcions del responsable del sistema:

1. Desenvolupar, operar i mantenir els sistemes d'informació fent atenció a les mesures de seguretat determinades pel responsable de seguretat.

2. Aplicar les mesures que figurin a les conclusions dels informes d'auditoria i que li comuniqui el responsable de seguretat.

6. La Comissió Tècnica de Gestió de la Informació és competent en matèria de seguretat de la informació, i té les funcions i composició establertes per l'acord del Consell de Govern de la Universitat, adoptat en la sessió ordinària núm. 2/2019 de 21 de març de 2019, composició i funcions que podran ser objecte de modificació per nous acords del Consell de Govern.

7. Les funcions descrites en els apartats 2, 3, 4 i 5 s'assignaran per mitjà de resolució del / de la rector/a.

Sisè. Dades de caràcter personal

1. A qualsevol sistema d'informació que gestioni dades de caràcter personal, li serà d'aplicació el que disposa el *Reglament General de Protecció de Dades* i la *Llei Orgànica 3/20018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals*, sense perjudici dels requisits establerts al *Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat* a l'àmbit de l'Administració Electrònica. Es seguiran també les pautes establertes en les Normes sobre Tractament de Dades de la UdG i les seves instruccions de desenvolupament.

2. Els tractaments de dades hauran de constar en el Registre d'Activitats de Tractament, Registre que recull tots els processos en els que es fa ús de dades de caràcter personal.

3. Els sistemes d'informació que s'utilitzen per aquests tractaments, s'ajusten als nivells de seguretat que la normativa imposa segons la naturalesa i finalitat de les dades recollides.

Setè. Gestió de la seguretat

1. En compliment de l'article 8 de l'ENS les infraestructures TIC disposaran d'una estratègia de protecció constituïda per diverses capes de seguretat, que minimitzin l'impacte de possibles incidents de seguretat.

2. L'anàlisi i la gestió de riscos és part essencial del procés de seguretat. Han de minimitzar els riscos fins a nivells admissibles. L'anàlisi de riscos s'efectuarà novament a proposta del responsable de seguretat que haurà de prendre en consideració almenys les circumstàncies següents:

a) La pèrdua d'informació.

b) La constatació de vulnerabilitats greus.

c) Els canvis substancials en la informació que es tracta.

d) Els canvis en els serveis prestats.

e) Els incidents greu de seguretat.

3. En compliment de l'art. 7.3 de l'ENS el responsable del sistema monitoritzarà el funcionament dels serveis TIC, per detectar anomalies en els nivells de prestació de serveis, i corregir-ho. En compliment de l'art. 7.4 de l'ENS el Servei d'Informàtica disposarà de protocols de restauració de la informació i de recuperació del servei per fer front a incidents de seguretat.

Vuitè. Auditoria de compliment

Almenys cada dos anys la Universitat es sotmetrà a una auditoria de verificació de compliment de l'ENS, supervisada pel responsable de seguretat. El resultat de l'auditoria es presentarà a la Comissió Tècnica de Gestió de la Informació, que proposarà mesures correctores per tal d'esmenar les deficiències o els riscos excessius constatats."