Universitat de Girona

Política de Seguretat en la Informació de la Universitat de Girona

Preàmbul 2

1. Marc normatiu 2
2. Objecte 3
3. Àmbit d'aplicació 3
4. Principis bàsics 4
   - 4.a-Seguretat com a procés integral
   - 4.b-Gestió de la seguretat basada en els riscs
   - 4.c-Prevenció, detecció, resposta i conservació
   - 4.d-Existència de línies de defensa
   - 4.e-Vigilància contínua
   - 4.f-Reavaluació periòdica
   - 4.g-Diferenciació de responsabilitats
5. Els objectius o la missió de l'organització 4
6. Òrgans i càrrecs responsables de la política de Seguretat de la Informació 5
   - 6.1- Rols de Seguretat de la Informació
   - 6.2- Responsables de la Seguretat en la Informació
   - 6.3- Comitè de la Seguretat de la Informació
   - 6.4- Funcions dels rols de la seguretat de la informació
   - 6.5- Funcions i règim de funcionament del Comitè de Seguretat de la Informació
7. Dades de caràcter personal 10
8. Les directrius per a l'estructuració de la documentació de seguretat del sistema, la gestió i l'accés 11
9. Gestió de la Seguretat 11
10. Formació 12
11. Obligacions del personal 12
12. Tercers 12
13. Auditoria de compliment de l'ENS 13
14. Aprovació i entrada en vigor 13

Preàmbul

La informació és un actiu essencial per a la Universitat, la capacitat de gestionar, protegir i compartir la informació de manera eficaç i segura és crucial per assegurar el bon funcionament de la institució, mantenir la confiança dels usuaris, preservar la reputació i complir amb les normatives específiques.

En un món cada vegada més interconnectat i digital, els reptes en matèria de seguretat de la informació són constants i en evolució. Les amenaces cibernètiques són cada vegada més sofisticades i són una preocupació creixent per a les institucions. A més, la creixent complexitat de la tecnologia i la dependència dels sistemes informàtics fan que sigui imprescindible implementar mesures de seguretat robustes i adaptatives.

Així mateix 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 (LOPDGDD) 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.

El present document estableix els principis, les polítiques i els procediments necessaris per garantir la seguretat de la informació en l'àmbit de la Universitat de Girona. Aquesta política és aplicable a tota la comunitat universitària, col·laboradors i tercers que tinguin accés als sistemes d'informació de la institució.

El compromís amb la seguretat de la informació és absolut i implica la participació activa i la col·laboració de tots els membres de la Universitat. Mitjançant aquesta política, es reafirma la responsabilitat amb la confidencialitat, la integritat i la disponibilitat de la informació, així com amb el compliment de les normatives aplicables per protegir els actius més preuats i per a la creació d'un entorn segur i confiable.

1. Marc normatiu

La UdG disposa d'una política de seguretat de la informació, en el context de l'ENS (Esquema Nacional de Seguretat), aprovada per Consell de Govern sessió núm. 4/19 de 5 de juliol de 2019. Tanmateix, aquesta política requereix una revisió per adaptar-la al que estableix el Reial decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat.

La Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, disposa a l'article 156.2 que l'Esquema Nacional de Seguretat té per objecte establir la política de seguretat en la utilització de mitjans electrònics en l'àmbit d'aquesta mateixa llei i que està constituït pels principis bàsics i pels requisits mínims que garanteixin adequadament la seguretat de la informació tractada.

Així mateix, la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, entre els drets de les persones en les seves relacions amb les administracions públiques previstos a l'article 13 inclou el relatiu a la protecció de les dades personals i, en particular, el dret a la seguretat i confidencialitat de les dades que figurin als fitxers, sistemes i aplicacions de les administracions públiques.

El 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 la lliure

circulació d'aquestes dades (RGPD) i la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

El Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), a l'article 12, determina que cada administració pública comptarà amb una política de seguretat formalment aprovada per l'òrgan competent; i que aquesta política s'establirà d'acord amb els principis bàsics indicats en el mateix Reial Decret i que es desenvoluparà aplicant uns requisits mínims especificats.

D'acord amb la disposició addicional segona del Reial decret 311/2022, el Centre Criptològic Nacional (CCN) elabora guies de seguretat de les tecnologies de la informació i la comunicació (guies CCN-STIC) que, a la vegada, s'han d'incorporar al conjunt documental utilitzat per a la realització de les auditories de seguretat. Un dels requeriments d'aquestes guies CCN-STIC contempla l'aprovació d'un cos normatiu en tres nivells: un primer nivell constituït per la present Política de Seguretat de la Informació; un segon nivell format per les normes derivades de l'anterior que han de ser aprovades per Consell de Govern a proposta del Comitè de seguretat TIC i, un tercer nivell constituït per procediments, guies i instruccions tècniques.

Dins el tercer nivell, els procediments de gestió operativa i els documents que descriuen explícitament pas a pas com realitzar una certa activitat, són aprovats pel Comitè de seguretat TIC a proposta del responsable de la seguretat TIC; i les instruccions tècniques pròpies del Servei d'Informàtic, són aprovades pel responsable del sistema.

A la vegada, aquest marc legal es complementa amb les normes de la Universitat sobre administració electrònica i protecció de dades personals, de manera que aquests blocs normatius s'hauran d'aplicar i interpretar de forma integrada.

2. Objecte

L'objecte d'establir una política de seguretat de la informació (PSI) és garantir la protecció adequada dels actius de la informació de la Universitat, els sistemes informàtics i la infraestructura tecnològica.

Aquesta política té com a finalitat establir els principis, les directrius i els procediments necessaris per gestionar de manera eficaç els riscos de seguretat de la informació, minimitzar les amenaces i les vulnerabilitats, i assegurar el compliment de les normatives i els estàndards de seguretat pertinents.

3. Àmbit d'aplicació

La PSI i la normativa que la desenvolupa s'aplica a totes les persones vinculades amb la Universitat de Girona, als seus actius d'informació i a tots els sistemes d'informació afectats.

Així mateix és aplicable a tots els proveïdors, persones externes i altres usuaris que tinguin algun tipus de vinculació amb la UdG, que mitjançant el registre de persones interaccionin amb els sistemes informàtics o la xarxa de la UdG així com tots els equips i serveis propietaris o arrendats que, d'alguna manera, hagin d'utilitzar localment o remotament la xarxa o recursos tecnològics de la Institució, així com els serveis i l'intercanvi d'arxius i programes.

4. Principis bàsics

a) Seguretat com a procés integral: Aquest principi implica que la seguretat no és només un aspecte puntual o aïllat, sinó que ha de ser integrada a tots els processos i activitats del sistema, considerant-la com una part essencial de totes les operacions.

b) Gestió de la seguretat basada en els riscos: Aquest principi destaca la importància d'identificar, avaluar i gestionar els riscos de seguretat. En lloc de centrar-se només en les amenaces concretes o en les vulnerabilitats, la gestió de la seguretat basada en els riscos pren en consideració tots els factors que poden afectar la seguretat i prioritzar les accions segons el seu potencial d'impacte i probabilitat.

c) Prevenció, detecció, resposta i conservació: Aquest principi subratlla la importància de tenir un enfocament complet en la gestió de la seguretat. Aquest enfocament inclou la prevenció d'incidents de seguretat sempre que sigui possible, la detecció ràpida d'amenaces o incidents en cas que ocorrin, una resposta eficaç per mitigar els efectes dels incidents i la conservació de la informació i les proves per a futurs anàlisis o accions correctives.

d) Existència de línies de defensa: Aquest principi implica la implementació de múltiples capes o nivells de defensa per protegir contra amenaces de seguretat. Això pot incloure barreres físiques, tecnològiques, procediments i altres mesures destinades a prevenir, detectar i respondre als atacs o incidents de seguretat.

e) Vigilància contínua: Aquest principi ressalta la importància de mantenir una vigilància constant sobre els sistemes, les xarxes i les activitats per detectar i respondre ràpidament a qualsevol amenaça o anomalia de seguretat. Això pot incloure la supervisió de registres d'activitat, l'anàlisi de trànsit de xarxa i altres tècniques de monitoratge.

f) Reavaluació periòdica: Aquest principi indica la necessitat de revisar i actualitzar regularment les estratègies, polítiques i controls de seguretat per assegurar-se que siguin efectius i adequats en un entorn canviant. Les reavaluacions periòdiques permeten adaptar-se a nous reptes de seguretat, canvis tecnològics i altres factors que puguin afectar la seguretat d'una organització o sistema.

g) Diferenciació de responsabilitats: Aquest principi implica clarament definir i assignar responsabilitats per a la seguretat a diferents nivells i rols dins de la Universitat. És important que cada persona o grup tingui una comprensió clara de les seves responsabilitats en relació amb la seguretat i que hi hagi una coordinació efectiva entre els diferents equips i departaments responsables de la seguretat.

5. Els objectius o la missió de l'organització

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 als incidents amb rapidesa.

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.

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 rapidesa 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.

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

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

b) 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 i els serveis de la societat de la informació.

c) 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.

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

e) Avaluar regularment la seguretat dels sistemes.

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

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

h) Fer formació en seguretat per al seu personal.

i) 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.

6. Òrgans i càrrecs responsables de la política de Seguretat de la Informació

En l'aplicació del principi de diferenciació de responsabilitats, cal assignar i definir les responsabilitats i rols dins de la Universitat.

6.1- Rols de Seguretat de la Informació:

a) El responsable de la informació determinarà els requisits de la informació tractada.
b) El responsable del servei determinarà els requisits dels serveis prestats.

c) El responsable de la seguretat determinarà les decisions per satisfer els requisits de seguretat de la informació i dels serveis, supervisarà la implantació de les mesures necessàries per garantir que se satisfan els requisits i reportarà sobre aquestes qüestions.
d) El responsable del sistema, per si mateix o a través de recursos propis o contractats, s'encarregarà de desenvolupar la forma concreta d'implementar la seguretat en el sistema i de la supervisió de l'operació diària del mateix, podent delegar en administradors o operadors sota la seva responsabilitat.

El responsable de seguretat serà diferent del responsable del sistema, i no hi pot haver dependència jeràrquica entre ambdós. En aquelles situacions excepcionals en les que l'absència justificada de recursos faci necessari que ambdues funcions recaiguin en la mateixa persona o en diferents persones entre les que existeixi relació jeràrquica, hauran d'aplicar-se mesures compensatòries per garantir la finalitat del principi de diferenciació de responsabilitats.

6.2- Responsables de la Seguretat en la Informació:
a) Responsable de la informació: el secretari o secretària general o persona en qui delegui.
b) Responsable dels serveis: el gerent o gerenta o persona en qui delegui.
c) Responsable de seguretat de la informació: designat pel rector o rectora.
d) Responsable del sistema: el o la Cap del Servei Informàtic

6.3- Comitè de la Seguretat de la Informació

Presidència: el rector o rectora o persona en qui delegui.

Membres permanents:
Responsable de la informació (RI), que actuarà com a secretari o secretària del Comitè
Responsable del sistema (RSIS)
Responsable de seguretat de la informació (RSEG)
Responsable dels serveis (RSER)
Delegat o delegada de protecció de dades (DPD)
Membres no permanents:
Membres de la Comissió Tècnica de Gestió de la Informació i Administració Electrònica (CTGIiAE)

El Comitè pot convocar a les reunions altres representants de la Universitat com especialistes externs dels sectors públic, privat i/o acadèmic, la presència dels quals sigui necessària o aconsellable, per raó de l'experiència o la vinculació amb els assumptes tractats.

Els integrants del Comitè de Seguretat de la Informació els ha de nomenar el rector de la UdG. El nomenament s'ha de revisar cada quatre anys o quan la plaça quedi vacant.

6.4- Funcions dels rols de la seguretat de la informació

a) *Funcions del responsable de la informació:*

- Determinar els requisits de la informació tractada en matèria de seguretat de la informació (nivells de seguretat de la informació), prèvia proposta i aprovació del Comitè de Seguretat de la Informació dins del marc establert en l'annex I del Reial decret 311/2022, de 3 de maig.

- Vetllar pel bon ús de tota la informació de la Universitat d'acord amb els principis de protecció, integritat i confidencialitat.

- Posar en coneixement del responsable de seguretat de la informació qualsevol variació respecte de la informació tractada dels quals és responsable; especialment, la incorporació de nova informació a càrrec seu. El responsable de seguretat de la informació ha de traslladar els canvis esmentats al Comitè de Seguretat de la Informació en la propera sessió.

- Qualsevol altra funció que li atorgui l'ENS o la legislació vigent.

b) *Funcions del responsable dels serveis:*

- Determinar els requisits dels serveis prestats en matèria de seguretat TIC (nivells de seguretat dels serveis), prèvia proposta i aprovació del Comitè de Seguretat de la Informació dins del marc establert en l'annex I del Reial decret 311/2022, de 3 de maig.

- Posar en coneixement del responsable de seguretat de la informació qualsevol variació respecte dels serveis prestats dels quals és responsable; especialment, la incorporació de nous serveis. El responsable de seguretat de la informació ha de traslladar els canvis esmentats al Comitè de Seguretat de la Informació en la propera sessió.

- Qualsevol altra funció que li atorgui l'ENS o la legislació vigent.

El responsable dels serveis pot delegar funcions concretes de les responsabilitats que se li atribueixen als caps de servei, quan siguin els promotors de sistemes d'informació sectorials que requereixin coneixements concrets.

c) Funcions del responsable de seguretat de la informació:

- Mantenir i verificar el nivell adequat de seguretat de la informació manejada 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 i de la declaració d'aplicabilitat regulada en l'article 28 de l'ENS, identificar mesures de seguretat, determinar configuracions necessàries, i elaborar documentació del sistema.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el responsable del sistema i/o el Comitè de Seguretat de la Informació.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, dels plans de continuïtat, que ha de validar.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació i auditories.
- Elevar al Comitè de Seguretat de la Informació l'aprovació de canvis i altres requisits del sistema.
- Aprovar els 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 fet al llarg del període en curs.

- Redactar propostes i presentar-les al Comitè de Seguretat de la Informació.
- Promoure la millora continuada del sistema de gestió de la seguretat de la informació, d'acord amb l'article 27 de l'ENS.
- Aprovar els canvis que, mitjançant una anàlisi de risc, es determini que són rellevants per a la seguretat del sistema i siguin d'un risc de nivell «alt».
- Analitzar els informes d'autoavaluació i elevar les conclusions al responsable del sistema perquè adopti les mesures correctores adequades.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el responsable del sistema i/o el Comitè de Seguretat de la Informació.
- Revisar els informes d'auditoria. Les conclusions de les auditories s'han de presentar al responsable del sistema perquè adopti les mesures correctores adequades.

d) Funcions del responsable del sistema:

- Desenvolupar, per si mateix o a través de recursos propis o contractats, la forma concreta d'implementar la seguretat en el sistema i de supervisar l'operació diària del mateix sistema, que pot delegar en administradors o operadors sota la seva responsabilitat.
- Revisar les conclusions dels informes d'auditoria que emet el responsable de seguretat de la informació.
- Desenvolupar, operar i mantenir el sistema d'informació durant tot el cicle de vida, per a la qual cosa cal elaborar els procediments operatius necessaris.
- Definir la topologia i la gestió del sistema d'informació i establir-ne els criteris d'ús i els serveis que hi són disponibles.
- En els casos de sistemes de categoria «alta», suspendre temporalment, si escau, el tractament d'informacions, la prestació de serveis o l'operació total del sistema fins a l'esmena o la mitigació adequada.
- Garantir que els dispositius estan sota control i que satisfan els requisits de seguretat mentre són desplaçats d'un lloc a l'altre, fora de les zones controlades per la Universitat.
- Rebre les conclusions dels informes d'autoavaluació i prendre les mesures correctores adequades.
- Rebre les conclusions dels informes d'auditoria i prendre les mesures correctores adequades.
- Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins el marc general de seguretat.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el responsable de seguretat de la informació i/o el Comitè de Seguretat de la Informació.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, dels plans de continuïtat.
- Dur a terme, si escau, les funcions de l'administrador de la seguretat del sistema:
    - Gestionar, configurar i actualitzar, si escau, el maquinari i el programari en què es basen els mecanismes i serveis de seguretat.
    - Gestionar les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la correspondència amb l'autoritzat.
    - Aprovar els canvis en la configuració vigent del sistema d'informació.
    - Assegurar que es compleixen estrictament els controls de seguretat establerts.
    - Assegurar que s'apliquen els procediments aprovats per manejar el sistema d'informació.

- Supervisar les instal·lacions de maquinari i programari i les seves modificacions i millores, per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.
- Informar el responsable de seguretat de la informació de qualsevol anomalia, compromís o vulnerabilitat relacionat amb la seguretat.
- Gestionar la investigació i la resolució d'incidents de seguretat, des de la detecció fins a la resolució.

Quan la complexitat del sistema ho justifiqui, el responsable del sistema pot designar els responsables de sistema delegats que consideri necessaris, els quals en tenen dependència funcional directa i són responsables en el seu àmbit de totes les accions que els deleguin.

e) Funcions del delegat o delegada de protecció de dades: en l'àmbit de l'Esquema Nacional de Seguretat són les que determinades a l'art. 39 del Reglament (UE) 2016/679 general de protecció de dades i, de conformitat amb l'Esquema Nacional de Seguretat són:

- Supervisar el compliment de la legislació vigent en la protecció de dades de caràcter personal
- Assessorar al responsable o encarregat del tractament en l'elaboració de les anàlisi de riscos i avaluacions d'impacte relatives a la protecció de dades que determinen els risc i el nivell de seguretat a aplicar en els sistemes d'informació.
- Actuar com a punt de contacte per als interessats en tot el que tingui relació amb el tractament de les dades personals.

6.5- Funcions i règim de funcionament del Comitè de Seguretat de la Informació

Funcions del Comitè de Seguretat de la Informació:

a) Estar informat permanentment de la normativa que regula la certificació de conformitat amb l'ENS, incloent-hi les normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.

b) Estar informat permanentment de la relació d'entitats de certificació acreditades i organitzacions, públiques i privades, certificades.

c) Estar informat permanentment de la relació d'esquemes de certificació de la seguretat amb els quals l'Administració pública té establerts arranjaments i acords de reconeixement mutu de certificats.

d) Proposar directrius i recomanacions, que s'han de recollir en les actes corresponents de les reunions del Comitè, a les quals la Presidència ha de donar una resposta adequada.

e) Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació per assegurar que siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

f) Atendre les inquietuds en matèria de seguretat de la informació de l'Administració i de les diferents àrees, i informar regularment sobre l'estat de la seguretat de la informació al Consell de direcció.

g) Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents unitats administratives, i elevar els casos en què no tingui prou autoritat per decidir.

h) Assessorar en matèria de seguretat de la informació, sempre que se li requereixi.

i) Revisar la Política de seguretat de la informació, abans que l'aprovi el Consell de Govern.

j) Aprovar la Normativa sobre l'ús de mitjans electrònics per a tot el personal.

k) Aprovar el mapa de normativa amb la llista de normativa i procediments de seguretat per a la implantació de l'ENS.

l) Proposar i aprovar els requisits de seguretat aplicables a la informació i als serveis.

m) Aprovar els plans de millora de la seguretat.

n) Dictaminar respecte dels drets d'accés a la informació i als serveis.

o) Acceptar els nivells de riscs residuals que afecten la informació i els serveis.

Periodicitat de les reunions i l'adopció d'acords:

a) Durant el desenvolupament del projecte d'adequació a l'ENS, per avaluar-ne el desenvolupament i possibilitar-ne el seguiment adequat, el Comitè de Seguretat de la Informació s'ha de reunir, almenys, un cop al trimestre.

b) Un cop assolida la certificació de conformitat amb l'ENS dels serveis prestats per la Universitat, el Comitè de Seguretat de la Informació s'ha de reunir, almenys, dues vegades l'any amb caràcter semestral, sense perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, es requereixi més freqüència en les reunions.

c) En qualsevol cas, les reunions les ha de convocar la Presidència, a través del secretari o secretària, a iniciativa seva o per majoria dels membres permanents.

d) Les decisions s'han d'adoptar per consens dels membres permanents.

El secretari o secretària del Comitè ha de fer les convocatòries i ha d'aixecar actes de les reunions del Comitè de Seguretat de la Informació. A les sessions del Comitè de Seguretat de la Informació, poden assistir-hi en qualitat d'assessors les persones que en cada cas estimi pertinents la Presidència.

7. Dades de caràcter personal

La LOPDGDD estableix que els subjectes vinculats al sector públic, com ho són les universitats públiques, han de fer públic un inventari de les seves activitats respecte del tractament de dades personals (RAT) accessible per mitjans electrònics, on hi ha de constar la informació prevista a l'article 30 de l'RGPD, i on s'ha d'especificar, a més, la base legal del tractament.

Aquest registre d'activitats de tractament es publicarà a la pàgina web de la UdG, apartat "Protecció de Dades". Tots els sistemes d'informació de la Universitat s'han d'ajustar als nivells de seguretat que estableix la normativa segons la naturalesa i la finalitat de les dades personals.

8. Les directrius per a l'estructuració de la documentació de seguretat del sistema, la gestió i l'accés

La documentació de seguretat TIC s'estructura en tres tipus:

- La present política de seguretat de la informació (PSI), que estableix els requisits i criteris de seguretat TIC en l'àmbit de la Universitat i que serveix de guia per a la creació de normes de seguretat.

- Les normatives de seguretat, que defineixen què cal protegir i els requisits de seguretat TIC necessaris.

- Els procediments de seguretat TIC, en els quals s'ha de concretar com s'ha de protegir el que estableixen les normes i les persones o rols responsables de la implantació, manteniment, revisió i seguiment d'aquestes normes.

S'ha d'assegurar la creació i la gestió de documents de seguretat del sistema autèntics, fiables, íntegres i utilitzables capaços de donar suport a les funcions i les activitats de seguretat TIC de la Universitat, durant el temps que sigui necessari, així com preservar-los.

Els documents seran públics llevat que el seu contingut faci difusió de dades personals o comporti un risc per a la seguretat dels sistemes.

El Comitè de Seguretat de la Informació estableix les limitacions a l'accés, ús i reutilització per a l'usuari o receptor d'aquests documents.

La revisió de cada document i la proposta de noves versions realitzada per qualsevol de les àrees afectades o pels òrgans de la Universitat s'han de notificar al responsable de Seguretat de la informació, que canalitzarà les propostes a través del Comitè de Seguretat de la Informació.

El Comitè de Seguretat de la Informació aprova les normatives tècniques i procediments de seguretat i altres documents derivats d'aquesta política.

Les noves versions de qualsevol d'aquests documents s'hauran de comunicar, segons el seu àmbit d'ús i el nivell de difusió que requereixin, de manera que el personal afectat sempre disposi de la darrera versió.

9. Gestió de la Seguretat

9.1- Línies de defensa

Les infraestructures TIC han de comptar amb una estratègia de protecció constituïda per diverses capes de seguretat, que poden ser de naturalesa física, lògica o organitzativa, que permetin la minimització de l'impacte de possibles incidents de seguretat, tal i com estableix l'article 9 de l'ENS.

9.2- Anàlisi i gestió de riscos

L'anàlisi i la gestió de riscos són part essencial del procés de seguretat i han de mantenir-se actualitzades. La gestió de riscos permetrà el manteniment d'un entorn controlat, minimitzant-los fins a nivells admissibles.

S'ha de realitzar una anàlisi de riscos sobre les infraestructures TIC en què s'avaluïn les amenaces i els riscos als quals estan exposades. Aquesta anàlisi s'haurà de repetir quan es doni alguna de les circumstàncies següents:

a) Modificació en la informació que es tracta.

b) Canvi en els serveis prestats.
c) Existència d'un incident greu de seguretat.
d) Detecció de vulnerabilitats greus.

10. Formació

1. L'oferta formativa de la UdG haurà d'incloure cursos de conscienciació i formació en seguretat, tant per al personal docent i investigador com per al personal tècnic, de gestió i d'administració i serveis, i haurà de tenir en compte tant la formació contínua com la formació del personal de nova incorporació.

La Universitat determinarà quina formació ha de ser obligatòria en funció del lloc de treball.

2. El Servei d'Informàtic ha de vetllar perquè el personal d'empreses contractistes i subcontractades que administrin infraestructures TIC de la Universitat conegui i apliqui tant les normatives de seguretat com els procediments de treball TIC de la Universitat.

11. Obligacions del personal

Els membres de la comunitat universitària han de conèixer i complir aquesta política de seguretat de la informació i les normatives de seguretat TIC que en deriven.

En el pla d'acollida dels treballadors de la Universitat es farà entrega del document elaborat per la Comissió Tècnica de Gestió de la Informació i Administració Electrònica relatiu a la Informació sobre protecció de dades i drets digitals per tal que en donin la seva conformitat.

12. Tercers

Quan la Universitat per al desenvolupament d'un nou projecte comporti la contractació o la creació, o evolució de qualsevol recurs o sistema informàtic haurà de complir *els requeriments que han de complir els sistemes informàtics de tractament d'informació responsabilitat de la UdG* aprovat pel Consell de Govern en sessió núm. 10/20 de 14 de desembre de 2020.

Quan la Universitat presta serveis TIC a altres institucions o organismes, el Servei d'Informàtic els ha de fer partícips de la política de seguretat de la informació i d'altres normatives TIC associades i ha d'establir canals de coordinació i procediments d'actuació per reaccionar adequadament en cas de possibles incidents de seguretat, i quan la Universitat utilitzi serveis TIC d'altres institucions, organismes o empreses o els cedeixi informació, sigui mitjançant la contractació de serveis, la col·laboració o qualsevol altra relació que no tingui caràcter contractual, els ha de fer partícips de la política i de la normativa de seguretat referides en aquests serveis i aquesta informació tal i com està regulat en la disposició addicional 25.2 Llei 9/2017, de 8 de novembre, de contractes del sector públic. Aquesta institució, organisme o empresa quedarà subjecta a les obligacions establertes en la normativa esmentada i podrà desenvolupar procediments operatius propis per complir-la. S'han d'establir procediments específics per reportar i resoldre incidències. S'ha de garantir que el seu personal està conscienciat adequadament en matèria de seguretat, si més no al mateix nivell que el que estableix aquesta política. Quan la institució, organisme o empresa no pugui satisfer algun aspecte d'aquesta política, segons el que estableixen els paràgrafs anteriors, el responsable de la seguretat ha d'elaborar un informe en què especifiqui els riscos a què està exposada i la forma de tractar-los. Els responsables de la informació i dels serveis afectats han d'aprovar aquest informe per poder utilitzar els serveis.

13. Auditoria de compliment de l'ENS

Amb una periodicitat biennal la Universitat sotmetrà els sistemes sotmesos a l'àmbit d'aplicació de la present normativa a una auditoria de verificació del compliment de l'ENS, la qual serà coordinada pel responsable de la seguretat TIC.

El resultat de l'auditoria ha de ser presentat al Comitè de seguretat TIC, que podrà decidir mesures correctores per tal d'esmenar possibles deficiències o riscos excessius identificats durant el procés d'auditoria. Aquestes mesures correctores seran de compliment obligatori.

14. Aprovació i entrada en vigor

Aquesta Política de Seguretat (PSI) entrarà en vigor l'endemà de la publicació al Butlletí Oficial de la Universitat de Girona i deroga l'aprovada per Consell de Govern sessió núm. 4/19 de 5 de juliol de 2019.