Universitat de Girona

Resolució del rector per la qual s'acorda el procediment de notificació i gestió de les incidències de violacions de seguretat en sistemes d'informació i en tractament de dades de caràcter personal de la Universitat de Girona

En la Universitat de Girona es considera necessari elaborar un protocol de comunicació d'incidències TIC i de tractament de dades personals, com a conjunt de procediments i directrius que descriuen com cal reportar i gestionar les incidències relacionades amb la tecnologia de la informació. Aquest ha d'establir el procediment per a la detecció, notificació, anàlisi, resposta i recuperació davant d'incidents de seguretat TIC, a la vegada establint les responsabilitats de les entitats en relació amb la detecció i la notificació d'incidents, així com les mesures de seguretat a implementar per garantir la continuïtat del servei i la recuperació dels sistemes afectats.

Atès que en l'apartat relacionat amb el Desenvolupament de la política de seguretat TIC de la política de Seguretat aprovada en la sessió núm. 4/2019 del Consell de Govern de 5 de juliol de 2019, es determina que la Política de Seguretat de la Informació de la Universitat de Girona es desenvoluparà mitjançat entre altres d'un instrument de procediment de gestió de les incidències

Ates que l'article 156.2 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, estableix que 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.

Atès que en els articles 25 i 33 del Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat es regula els procediment de gestió d'incidents de seguretat.

Atès que de la perspectiva de la protecció de les dades personals, d'acord amb 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.

Atès l'acord de la Comissió Tècnica de Gestió de la Informació i Administració Electrònica en sessió núm. 2/2023 de 16 de febrer de 2023, i

En virtut de les competències que m'han estat atribuïdes pels articles 93 i 97 dels Estatuts de la Universitat de Girona (ACORD GOV/94/2011, de 7 de juny, pel qual s'aprova la modificació dels Estatuts de la Universitat de Girona i es disposa la publicació del seu text íntegre – DOGC núm. 5897, de 9 de juny de 2011), i en virtut del Decret 401/2021, de 14 de desembre de 2021, de nomenament del rector de la Universitat de Girona (DOGC núm. 8564, de 16 de desembre de 2021),

RESOLC:

Primer. Aprovar el procediment de notificació i gestió de les incidències de violacions de seguretat en sistemes d'informació i en tractament de dades de caràcter personal de la Universitat de Girona, d'acord amb l'ANNEX NÚM. 1 adjunt a la resolució.

Segon. Publicar aquesta resolució en el Butlletí Oficial de la Universitat de Girona (BOUdG)

Universitat de Girona
Rectorat

Joaquin Salvi Mas
Rector de la Universitat de Girona

Data:
2023.03.13
10:14:27 +01'00'

El rector,

Joaquim Salvi i Mas

Contra aquesta resolució, que posa fi a la via administrativa i independentment de la seva execució immediata, les persones interessades poden interposar, amb caràcter potestatiu, recurs de reposició davant del rector de la Universitat de Girona en el termini d'un mes a comptar de l'endemà de la seva notificació, d'acord amb el que disposen els articles 123 i 124 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú; o bé interposar directament recurs contenciós administratiu davant els jutjats contenciosos administratius de Girona, en el termini de dos mesos a comptar de l'endemà de la seva notificació, d'acord amb els articles 8.3, 14.1 i 46.1de la L1ei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Igualment, les persones interessades poden interposar qualsevol altre recurs que considerin convenient per a la defensa dels seus interessos.

Universitat de Girona

ANNEX NÚM. 1

PROCEDIMENT DE NOTIFICACIÓ I GESTIÓ DE LES INCIDÈNCIES DE VIOLACIONS DE SEGURETAT EN SISTEMES D'INFORMACIÓ I EN TRACTAMENT DE DADES DE CARÀCTER PERSONAL DE LA UNIVERSITAT DE GIRONA

Article 1. Objecte i àmbit d'aplicació

1. L'objecte d'aquest procediment és establir els mecanismes de notificació i gestió de les violacions de seguretat TIC i també en els tractaments de dades personals per part de la Universitat. S'entén per violació de seguretat i de les dades personals qualsevol situació que suposi la destrucció, pèrdua, alteració accidental o il·lícita, comunicació, accés o publicació no autoritzada de dades personals tractades per la Universitat, tant en qualitat de responsable del tractament com d'encarregada del tractament.

2. Aquest procediment és d'aplicació a PDI, PAS, estudiants, i qualsevol persona externa que interactuï amb la Universitat que tingui coneixement d'una violació de seguretat TIC.

Article 2. Procediment de comunicació interna

1. Qualsevol persona que tingui indicis d'una possible violació de seguretat TIC i o de les dades personals ho haurà de comunicar de manera immediata i sense dilació indeguda creant una incidència identificada com de seguretat en el portal d'incidències TIC (https://apps.udg.edu/jira).

La creació d'aquesta incidència serà notificada automàticament a les adreces de correu si.seguretat@udg.edu i dpd@udg.edu.

2. La comunicació haurà de contenir:

a. Dia i hora de la detecció de la violació de seguretat i, si es coneix, moment en què va començar.
b. Descripció de la violació de seguretat amb indicació, si és possible, del:
    - Tipus de violació (eliminació o pèrdua, alteració indeguda, comunicació indeguda, publicació, etc.)
    - Abast de la violació (número de persones afectades, número de persones que han tingut accés indegut a informació, etc.)
    - Tipus de dades afectades (dades identificatives, dades acadèmiques, dades econòmiques, dades de salut, etc.)

c. Si escau, mesures adoptades o proposades per evitar o minimitzar els possibles danys.
d. Dades identificatives i de contacte de la persona que fa la comunicació.
e. Qualsevol altra informació que es consideri d'utilitat per la gestió de la violació de seguretat.

Article 3. Comprovació de la comunicació interna

1. Immediatament després de rebre la notificació automàtica de la possible violació de seguretat, el cap de Seguretat-TIC i el delegat de Protecció de Dades hauran d'analitzar-la a fi de comprovar-ne el seu possible abast.

2. En el cas d'una incidència de protecció de dades hi ha un termini de només 72 hores entre la detecció d'una possible violació de seguretat i la seva notificació a les autoritats de control, per tant les tasques de comprovació d'una possible violació de seguretat hauran de rebre el suport immediat de la resta de personal de la Universitat.

3. Si es confirmés l'existència d'una violació de seguretat, el responsable de Seguretat-TIC i el delegat de Protecció de Dades avisaran de manera immediata el gerent, el cap del Servei Informàtic, el cap de servei o unitat administrativa o investigador principal del grup de recerca responsable de la gestió del tractament de dades personals afectades.

4. El responsable de seguretat TIC juntament amb el cap de servei o unitat administrativa o investigador principal del grup de recerca involucrat o persona en qui delegui, determinaran de manera conjunta l'abast de la situació i les propostes d'actuacions a realitzar per solucionar o mitigar la violació de seguretat, així com per mirar d'evitar que en el futur es torni a produir. La denúncia als cossos de seguretat la formularà l'òrgan o càrrec immediat del sistema d'informació on s'ha produït la violació.

Article 4. Notificació a l'autoritat de control

1. El responsable de Seguretat TIC, una vegada valorada la necessitat de posar la pertinent denúncia, la notificarà a l'Agència Catalana de Ciberseguretat (ACC)
2. El delegat de Protecció de Dades, dins el termini de 72 hores a partir de la detecció de la violació de seguretat establert per la legislació, notificarà a l'APDCAT la denúncia d'acord amb l'article 33.3 de l'RGPD.
3. Es comunicarà les denúncies a la Comissió Tècnica de Gestió de la Informació i Administració Electrònica i si es creu necessari es podrà convocar una sessió extraordinària de caràcter urgent.

Article 5. Comunicació als afectats

1. En cas que una violació de seguretat de dades personals pugui comportar un alt risc per als drets i llibertats de les persones afectades, la Universitat els ho comunicarà sense dilació indeguda.

2. No caldrà fer aquesta comunicació quan:

   a. La Universitat hagi adoptat mesures de protecció tècniques i organitzatives adequades a les dades personals afectades per la violació de seguretat, en especial les que facin inintel·ligibles les dades personals per a qualsevol persona que no estigui autoritzada a accedir-hi, com el xifrat;

   b. La Universitat hagi pres mesures posteriors que garanteixin que ja no existeix la possibilitat que es materialitzi l'alt risc per als drets i les llibertats dels interessats.

3. Aquesta comunicació descriurà la naturalesa de la violació, les possibles conseqüències, les mesures adoptades i les recomanacions perquè les persones puguin mitigar els potencials efectes adversos.

4. Les persones afectades podran demanar que la Universitat les tingui informades de l'evolució de la violació de seguretat.

5. Correspon a la CTGIiAE designar els membres d'una subcomissió expressa la qual en vista de la proposta realitzada pel responsable de Seguretat TIC i el delegat de Protecció de Dades, decidirà sobre la conveniència o no de comunicar una violació de seguretat a les persones afectades. Quan la comunicació a les persones afectades impliqui un esforç desproporcionat, caldrà valorar la conveniència d'una comunicació pública o una mesura equivalent, que informi els interessats de manera igualment efectiva.

Article 6. Seguiment de les violacions de seguretat notificades

1. Correspon al responsable de Seguretat TIC fer la interlocució amb ACC en relació amb les notificacions de violacions de seguretat que la Universitat realitzi.
2. Correspon al delegat de Protecció de Dades fer la interlocució amb l'APDCAT en relació amb les notificacions de violacions de seguretat que la Universitat realitzi.
3. Correspon a la CTGIiAE fer el seguiment de les actuacions que s'hagi determinat efectuar per resoldre o minimitzar els efectes de la violació de seguretat, així com per evitar que la situació es pugui reproduir en un futur.
4. El responsable de Seguretat TIC informarà periòdicament a la CTGIiAE del seguiment de les alteracions de seguretat fins que aquestes no es puguin donar per tancades i s'hagin pogut verificar l'efectivitat de les mesures adoptades en conseqüència.

Article 7. Registres en relació amb les violacions de seguretat

1. Correspon al responsable de Seguretat TIC anotar les actuacions realitzades de cada incidència. Així mateix mantenir un registre de les notificacions realitzades a ACC.

2. Correspon al delegat de Protecció de Dades mantenir un registre de les violacions de seguretat en matèria de protecció de dades personals que la Universitat hagi notificat a l'APDCAT.

3. El Registre de violacions de seguretat contindrà:

a. Dia i hora de coneixement dels fets.
b. Un codi d'identificació.
c. La tipificació de la violació de seguretat.
d. Dia i hora dels fets (si es coneixen).
e. Un resum de l'incident.
f. La relació de fets.
g. La relació de dades afectades.
h. La relació de persones afectades.
i. Els possibles efectes sobre les persones afectades.
j. Còpia de la notificació a l'APDCAT i de la ACC
k. Anàlisi de la necessitat o no de comunicació a les persones afectades.
l. Si és el cas, còpia de la notificació a les persones afectades.
m. Relació de mesures correctores o mitigadores dutes a terme.
n. Relació de mesures dutes a termes per evitar que la violació de seguretat es reprodueixi.
o. Dia i hora del tancament de la violació de seguretat.

Article 8. Encàrrecs de tractament i coresponsabilitat en el tractament de dades personals

1. En cas que es detectin indicis d'una possible violació de seguretat en un tractament de dades personals dut a terme per la Universitat en qualitat d'encarregada del tractament per compte d'un tercer o com a corresponsable del tractament juntament amb altres organismes, caldrà notificar la possible violació de seguretat al delegat de Protecció de Dades de la Universitat d'acord amb allò establert a l'article 2 d'aquesta resolució.

2. El delegat de Protecció de Dades assessorarà els caps dels serveis, unitats administratives o investigadors principals dels grups de recerca responsables de la gestió de l'encàrrec de tractament respecte de les actuacions a realitzar d'acord amb la legislació vigent i allò establert al document regulador de l'encàrrec de tractament o l'acord de corresponsabilitat.

3. En cas que la Universitat encarregui el tractament de dades personals a tercers, aquests hauran de notificar les possibles violacions de seguretat a la Universitat d'acord amb allò establert en aquest procediment. La notificació a l'APDCAT i, si escau, la comunicació a les persones afectades, la realitzarà la Universitat, excepte que a l'encàrrec de tractament s'estableixi un procediment diferent.