Política de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València

VNIVERSITAT DE VALÈNCIA

VNIVERSITAT DE VALÈNCIA

Política de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de València

Contingut

1. Introducció

Aquesta política de seguretat de la informació s'elabora en compliment de l'exigència del Reial decret 951/2015, de 23 d'octubre de modificació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'esquema nacional de seguretat (ENS) en l'àmbit de l'administració electrònica que, en l'article 11, estableix l'obligació per a les administracions públiques de disposar d'una política de seguretat i indica els requisits mínims que ha de complir.

Aquesta política de seguretat segueix també les indicacions de la guia CCN-STIC-805 del Centre Criptològic Nacional, centre adscrit al Centre Nacional d'Intel·ligència.

El Reglament (UE) 2017/679 de 27 d'abril 2017 (GDPR) obliga al responsable del tractament a prendre tant les mesures jurídiques com les tècniques i orgranitzatves necessàries que garanteixen la seguretat de les dades de carácter personal i eviten la seua alteració, pèrdua, tractament o accés no autoritzat.

La llei orgànica 3/2018 de 5 de desembre de protecció de dades personals i garantia dels drets digitals.

> La Llei 40/2015 de Règim jurídic del sector públic establix que les administracions públiques es relacionaran entre si i amb els seus òrgans, organismes públics i entitats vinculades o dependents a través de mitjans electrònics que garanteixen la interoperabilitat i seguretat dels sistemes i solucions adoptades per cadascuna d´aquestes, garantirà la protecció de les dades de caràcter personal, i facilitarà preferentment la prestació conjunta de serveis als interessats i recull l´ENS al seu article 156.
>
> La Llei 39/2015, del Procediment Administratiu Comú de les Administracions Públiques, recull al seu article 13 sobre drets de les persones en les seues relacions amb les Administraciones Públiques en relació a la protección de dades de carácter personal, i en particular a la seguretat i confidencialitat de les dades que figuren en els fitxers, sistemes y aplicacions de les Administracions Públiques.

Tot açò motiva el compliment de l'Esquema Nacional de Seguretat (ENS, aprovat mitjançant Reial Decret 3/2010 i modificat posteriorment pel Reial Decret 951/2015.

L'adaptació a l'ENS implica que la Universitat de València i el seu personal han d'aplicar les mesures mínimes de seguretat exigides per l'ENS i realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Les diferents unitats de gestió de la Universitat s'han de cerciorar que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema de tramitació electrònica, des de la seua concepció fins a la seua retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació.

Els requisits de seguretat i els costos associats han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en plecs de licitació per a projectes de TIC.

Les unitats de gestió de la Universitat han d'estar preparades per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l'ENS.

Prevenció

L'organització ha d'evitar, o almenys prevenir sempre que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. En aquest sentit, s'han d'implementar les mesures mínimes de seguretat determinades per l'ENS, i també qualsevol control addicional identificat mitjançant una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats. Per garantir el compliment de la política, l'organització ha de:

1. Autoritzar els sistemes abans d'entrar en operació.
2. Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de forma rutinària.
3. Sol·licitar la revisió periòdica per part de tercers a fi d'obtenir una avaluació independent.

Detecció

Atès que els serveis es poden degradar ràpidament a causa d'incidents, s'ha de monitoritzar l'operació de manera continuada per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que estableix l'article 9 de l'ENS.

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

Resposta

L'organització està obligada a:

1. Establir mecanismes per respondre eficaçment als incidents de seguretat.
2. Designar punts de contacte per a les comunicacions respecte a incidents detectats en àrees de l'entitat o en altres organismes relacionats amb la Universitat de València.
3. Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els equips de resposta a emergències (CERT) reconeguts en l'àmbit estatal com Iris-CERT, CCN-CERT i d'altres d'equivalents.

Recuperació

Per restaurar la disponibilitat dels serveis, s'ha de desenvolupar plans de contingència dels sistemes TIC que incloguen activitats de recuperació de la informació que contribuïsquen a la continuïtat del servei.

2. Missió

Tal com es reflecteix en els seus Estatuts, la Universitat de València, com a servei públic que és, té per missió impartir els ensenyaments necessaris per a la formació dels estudiants, la preparació per a l'exercici d'activitats professionals o artístiques i l'obtenció, si és el cas, dels títols acadèmics corresponents, com també per a l'actualització permanent del coneixement i de la formació del seu personal i del professorat de tots els nivells d'ensenyament.

La Universitat de València fomenta la investigació, tant bàsica com aplicada, i el desenvolupament científic i tecnològic. Així mateix, amb les garanties de racionalitat i universalitat que li són pròpies, és una institució difusora de cultura en el si de la societat.

La Universitat de València facilita, estimula i acull les activitats intel·lectuals i crítiques en tots els camps de la cultura i del coneixement.

En el compliment de totes aquestes funcions, la Universitat de València té present l'harmonia dels sabers, originats en el desenvolupament del pensament humà i destinats al perfeccionament de les persones i de la seua convivència en una societat plural i democràtica.

De forma estretament relacionada amb el compliment d'aquesta missió, l'organització desitja manifestar la necessitat d'una infraestructura TIC que prevalga i fomente les operatives obertes, enfocades a la funcionalitat, connectivitat i servei als usuaris, com a funcions prioritàries per a la consecució dels objectius estratègics i institucionals.

3. Abast

L'organització aplicarà aquesta política de seguretat en aquells sistemes d'informació que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu.
En concret, atesa la missió de la Universitat definida en el punt 2, aquesta política de seguretat és aplicable sobre els següents sistemes d'informació TIC i els serveis que els conformen:

1. Gestió acadèmica:
   - Serveis de gestió acadèmica
   - Serveis de préstecs bibliotecaris
2. Gestió d'automatrícula (subsistema de gestió acadèmica):
   - Servei d'automatrícula
   - Servei d'admissió a la Universitat
3. Gestió d'actes (subsistema de gestió acadèmica):
   - Servei d'actes d'avaluació
4. Gestió de títols (subsistema de gestió acadèmica):
   - Serveis de sol·licitud i emissió de títols
5. Seu electrònica:
   - Serveis per a PAS-PDI
   - Serveis vinculats a la investigació
   - Serveis per a estudiants
   - Serveis a externs
6. Gestió econòmica:
   - Serveis de contractació administrativa
7. Sistema de docència virtual:
   - Aula Virtual
8. Portal web de la Universitat:
   - Serveis d'informació administrativa
9. Sistema de gestió de Recursos Humans
   - Servei de gestió de Recursos Humans.

L'organització desestima l'aplicació d'aquesta política de seguretat sobre aquells sistemes d'informació no reflectits en aquest apartat.

4. Marc normatiu complementari

En el desenvolupament i la implementació d'aquesta política es tindran en compte els Estatuts de la Universitat de València (Estudi General) i les seus normatives de desenvolupament relacionades amb els seus objectius.

5. Organització de la seguretat

Es poden distingir 3 nivells en l'organigrama de la Universitat de València:

1. Nivell 1 – Òrgans de govern:
   Consell de Govern/alta direcció, que s'ocupa de l'organització, determina els objectius que es proposa aconseguir i respon del fet que s'assolisquen.
2. Nivell 2 – Direcció executiva:
   Serveis/direccions, que s'ocupen de què fa cada unitat de gestió i com les diferents unitats es coordinen entre si per aconseguir els objectius marcats per la direcció.
3. Nivell 3: Operacional
   Se centra en una activitat concreta i controla com es fan les coses.

Seguint el mateix esquema i d'acord amb l'ENS, s'estructura un organigrama de seguretat de la Universitat en 3 nivells:

- Nivell 1:
  - Comitè de gestió i coordinació de la seguretat de la informació.
  - Responsable de la informació.
  - Responsable del servei.
- Nivell 2:
  - Responsable de la seguretat.
- Nivell 3:
  - Tècnic de seguretat dels sistemes.
  - Responsables dels sistemes d'informació.

L'especificació de requisits de seguretat (nivell 1) correspon als responsables de la informació i dels serveis, junt amb el responsable del fitxer si hi haguera dades de caràcter personal. L'operació (nivell 3) correspon als responsables dels sistemes, mentre que la supervisió correspon al responsable de la seguretat (nivell 2) i al tècnic de seguretat (nivell 3).

Per damunt de tots aquests hi ha el comitè de coordinació i gestió de la seguretat (nivell 1). Aquest comitè de seguretat pot assumir també la responsabilitat de la informació i dels serveis.

Comitè de gestió i coordinació de la seguretat de la informació

El comitè de gestió i coordinació de la seguretat de la informació (d'ara endavant, Comitè de Seguretat) coordina la seguretat de la informació pel que fa a l'organització.

D'acord amb l'RD 3/2010 (ENS), les funcions indicades que corresponen al Comitè de Seguretat són:

Elaborar (i revisar periòdicament) la política de seguretat de la informació perquè siga aprovada pel Consell de Govern de la Universitat.
Aprovar i divulgar els procediments de seguretat de la Universitat.

Promoure la millora contínua de la gestió de la seguretat de la informació de la Universitat.

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

Avaluar els principals riscos residuals assumits per la Universitat i recomanar possibles actuacions respecte a aquests.

Avaluar l'acompliment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte a aquests. En particular, vetlar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.

Promoure la realització de les auditories periòdiques i avaluar el compliment de les obligacions de l'organisme en matèria de seguretat.

Prioritzar les actuacions en matèria de seguretat d'acord amb els recursos disponibles.

Vetlar perquè la seguretat de la informació es tinga en compte en tots els projectes TIC des de la seua especificació inicial fins a la seua posada en operació. En particular, ha de vetlar per la creació i utilització de serveis horitzontals que reduïsquen duplicitats i secunden un funcionament homogeni de tots els sistemes TIC.

Resoldre els conflictes de responsabilitat que puga haver-hi entre els diferents responsables i/o entre diferents àrees de la Universitat, i elevar aquells casos en què no tinga prou autoritat per a decidir.

Avaluar les necessitats de recursos requerits per al compliment dels plans d'actuació derivats de l'aplicació de la política de seguretat.

Elaborar un informe anual que elevarà al Consell de Direcció de la Universitat.

El comitè de seguretat està format per:

Vicerector/a responsable de les tecnologies de la informació i les comunicacions, que presideix el comitè.

Gerent.

Secretari/ària general.

Delegat/Delegada de Protecció de Dades

Delegat/Delegada del rector/rectora per als temes TIC

Dos responsables dels serveis de la Universitat designats pel rector o la rectora.

Responsable de seguretat de la informació, que actua com a secretari del comitè.

El comitè de seguretat no és un comitè tècnic, però demanarà regularment al personal tècnic propi o extern la informació pertinent per a prendre decisions. El comitè de seguretat s'assessorarà en els temes sobre els quals haja de decidir o emetre una opinió.

Responsable de la informació

El responsable de la informació estableix els requisits sobre la informació proporcionada per mitjans electrònics a través dels serveis de la Universitat i, per tant, té l'última paraula a l'hora de decidir el tipus d'informació accessible i l'ús que s'hi puga donar, en virtut de la reglamentació vigent i de les bones pràctiques en matèria de protecció de dades. Li corresponen les funcions següents:

Establiment dels requisits de la informació en matèria de seguretat.

Treball en col·laboració amb el responsable de seguretat i els responsables dels sistemes en el manteniment dels sistemes catalogats segons l'annex I de l'ENS.

El responsable de la informació és el secretari o la secretària general de la Universitat.

Responsable dels serveis

El responsable dels serveis estableix els requisits de seguretat aplicables als serveis proporcionats per la Universitat a través de mitjans electrònics i, en aquest sentit, té per funcions:

- Establir els requisits dels serveis TIC en matèria de seguretat.
- Treballar en col·laboració amb el responsable de seguretat i els responsables dels sistemes on s'englobe el servei per al manteniment dels sistemes catalogats segons l'annex I de l'ENS.

El rol de responsable dels serveis l'assumeix el comitè de seguretat.

Responsable de seguretat

El director del Servei d'Informàtica té el rol de responsable de seguretat de la informació de la Universitat de València. Les seues funcions són:

- Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes TIC.
- Realitzar les auditories periòdiques que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Promoure la formació i conscienciació del Servei d'Informàtica dins el seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establertes són adequades per a la protecció de la informació manejada i els serveis prestats.
- Aprovar tota la documentació relacionada amb la seguretat dels sistemes.
- Verificar els informes de monitoratge i auditoria dels estats de seguretat dels sistemes.
- Fomentar i supervisar la investigació dels incidents de seguretat des de la seua notificació fins a la seua resolució.
- Elaborar l'informe periòdic de seguretat per al comitè de seguretat incloent-hi els incidents més rellevants del període.
- Aprovació dels procediments de seguretat elaborats pels responsables dels sistemes quan en virtut del contingut no requerisca l'aprovació del comitè de seguretat.
- Proposar la redacció d'aquella normativa de seguretat de la Universitat que considere necessari formalitzar.
- Determinar la categorització dels sistemes i els requisits de seguretat amb caràcter previ a l'engegada d'un nou servei vinculat a l'ENS.

Aquesta figura de "responsable de seguretat" descrita per l'ENS coincideix amb la del responsable de seguretat dels fitxers de la Universitat de València.

Responsables dels sistemes

Es designarà un responsable per a cada un dels sistemes d'informació definits en l'apartat d'Abast d'aquest document.

Entre les seues àrees d'actuació i en el marc d'aquesta política de seguretat, els responsables dels sistemes han de dur a terme les funcions següents:

Vetlar pel funcionament correcte del sistema durant tot el seu cicle de vida, de les seues especificacions i instal·lació, i incorporar els requisits de seguretat necessaris per a l'operativa en el sistema.

Definir la topologia i la política de gestió del sistema, i establir els criteris d'ús i els serveis que hi estan disponibles.

Definir la política de connexió o desconnexió d'equips i usuaris nous en el sistema.

Proposar al responsable de seguretat els canvis que afecten la seguretat del sistema.

Decidir les mesures de seguretat que aplicaran els subministradors de components del sistema durant les etapes de desenvolupament, instal·lació i prova d'aquest.

Implantar i controlar les mesures específiques de seguretat del sistema i cerciorar-se que aquestes s'integren adequadament dins el marc general de seguretat.

Determinar els requisits de la configuració autoritzada del maquinari i programari que cal utilitzar en el sistema, en allò que afecte la seua seguretat.

Aprovar tota modificació substancial de la configuració de qualsevol element del sistema que afecte la seguretat i la disponibilitat del servei.

Dur a terme el preceptiu procés de revisió periòdica de l'anàlisi i gestió de riscos en el sistema.

Elaborar i aprovar la documentació de seguretat del sistema.

Delimitar les actuacions que afecten la política de seguretat de cada entitat involucrada en el manteniment, l'explotació, la implantació i la supervisió del sistema.

Investigar els incidents de seguretat que afecten el sistema, i si és el cas, comunicació al responsable de seguretat o a qui aquest determine.

Establir plans de contingència i emergència.

A més, el responsable del sistema pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que puguen afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els responsables de la informació afectada, del servei afectat i el responsable de seguretat, abans de ser executada.

Tècnic de seguretat dels sistemes

El tècnic de seguretat dels sistemes és una figura operativa que depèn del responsable de la seguretat. Té com a missió principal assistir el responsable de seguretat en el nivell operatiu que suposa la supervisió integral de la seguretat dels sistemes d'informació inclosos en l'abast d'aquesta política.

El tècnic de seguretat té aquestes funcions:

Verificar l'aplicació dels procediments operatius de seguretat en els sistemes d'informació.

Supervisar les instal·lacions de maquinari i programari, les seues modificacions i millores perquè la seguretat no estiga compromesa i que a cada moment s'ajusten als procediments establerts.

Supervisar l'estat de la seguretat dels sistemes.

Informar el responsable de seguretat i els responsables dels sistemes d'informació sobre qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.

Col·laborar en la investigació i la resolució d'incidents de seguretat, des de la detecció fins a la resolució.

Assessorar els responsables dels sistemes per complir els requisits de seguretat establerts.

El tècnic de seguretat dels sistemes és designat pel responsable de la seguretat.

5.1 Procediments de designació

L'acompliment de les responsabilitats definides en aquesta política de seguretat és determinat per l'accés als diferents càrrecs que s'han vinculat a aquelles. En cas que desaparega o canvie de denominació algun d'aquests càrrecs, serà competència del rector assignar el nou lloc a què quedarà vinculada la figura.

6. Dades de caràcter personal

La Universitat de València realitza tractaments en què fa ús de dades de caràcter personal sotmeses al que disposa el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 de abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació de aquestes dades així com la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. Les mesures tècniques i organitzatives de seguretat aplicables a les activitats de tractament de dades desenvolupades en la Universitat de València estan documentades en el Registre de les Activitats de Tractament. Aquestes mesures estan contínuament adaptant-se al estat de la tècnica, tenint en compte els costos d'aplicació i la naturalesa, l'abast, el context i les finalitats del tractament, així com a riscos de probabilitat i gravetat variables per als drets i llibertats de les persones físiques. Qualsevol encarregat del tractament de la Universitat de València, haurà de aplicar mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc.

7. Gestió de riscos

Tots els sistemes subjectes a aquesta política de seguretat han de dur a terme una anàlisi de riscos, en la qual s'avaluaran les amenaces i els riscos a què estan exposats. Aquesta anàlisi es repetirà:

Regularment, almenys una vegada cada dos anys.
Quan canvie la informació manejada.
Quan canvien els serveis prestats.
Quan tinga lloc un incident greu de seguretat.
Quan es reporten vulnerabilitats greus.

Per a l'harmonització de les anàlisis de riscos, el comitè de seguretat establirà una valoració de referència per als diferents tipus d'informació gestionats i els diferents serveis prestats.

8. Desenvolupament de la política de seguretat

Aquesta política es desenvolupa per mitjà de normativa de seguretat que afronte aspectes específics. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conèixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

Altres documents que complementen aquesta política de seguretat són:

Normes d'ús personal dels recursos informàtics i telemàtics de la Universitat de València.

Els acords del Consell de Govern de la Universitat posteriors a l'aprovació d'aquesta política en la mesura en què puguen afectar-la.

Els anàlisis de riscos realitzats de les activitats de tractament.

Les avaluacions de impacte en la protecció de dades.

La normativa de seguretat haurà d'estar disponible en la intranet de la Universitat.

9. Obligacions del personal

Tots els membres de la Universitat de València tenen l'obligació de conèixer i complir aquesta política de seguretat de la informació i la normativa de seguretat desplegada a partir d'aquesta, i és responsabilitat del comitè de seguretat disposar els mitjans necessaris perquè la informació arribe a les persones afectades, tenint en compte sempre les disponibilitats pressupostàries de la Universitat.

Tots els treballadors i treballadores de la Universitat de València sota l'abast de l'ENS atendran una acció de conscienciació en matèria de seguretat TIC, almenys una vegada cada dos anys. S'establirà un programa d'accions en conscienciació contínua per atendre tots els membres de la Universitat relacionats amb serveis d'administració electrònica, en particular els de nova incorporació, tenint en compte sempre les disponibilitats pressupostàries de la Universitat. Es realitzarà una acció de conscienciació durant els 2 anys següents a l'aprovació d'aquesta política de seguretat i de manera continuada per al personal de nova incorporació.

En cas que es requerisca formació específica per al maneig segur dels sistemes, les persones amb responsabilitat en l'operació o administració de sistemes TIC la rebran en la mesura en què la necessiten per a realitzar el seu treball.

10. Terceres parts

Quan la Universitat de València **preste serveis** a altres organismes o manege informació d'altres organismes, se'ls farà partícips d'aquesta política de seguretat de la informació. Amb aquesta finalitat, s'establiran canals per a informe i coordinació dels respectius comitès de coordinació de l'ENS i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan la Universitat de València **utilitze serveis** de tercers o cedisca informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que implique aquests

serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en la normativa esmentada i s'haurà d'incorporar als plecs i comandes de la Universitat. Amb això, el proveïdor haurà de garantir que el seu personal està adequadament format en matèria de seguretat d'acord amb els requeriments de la Universitat.

11. Entrada en vigor

Aquesta política de seguretat de la informació és efectiva des de l'endemà de la data en què l'aprove el Consell de Govern de la Universitat de València i fins que siga reemplaçada per una nova política.

12. ANNEX A. GLOSSARI DE TERMES I ABREVIATURES

Anàlisi de riscos

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

Dades de caràcter personal

Qualsevol informació que concerneix persones físiques identificades o identificables. Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

Gestió d'incidents

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

Gestió de riscos

Activitats coordinades per a dirigir i controlar una organització respecte als riscos. ENS.

Incident de seguretat

Succés inesperat o no desitjat amb conseqüències que van en detriment de la seguretat del sistema d'informació. ENS.

Informació

Cas concret d'un cert tipus d'informació.

Política de seguretat

Conjunt de directrius plasmades en un document escrit, que regeixen la manera com una organització gestiona i protegeix la informació i els serveis que considera crítics. ENS.

Principis bàsics de seguretat

Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis. ENS.

Responsable de la informació

Persona que té la potestat d'establir els requisits d'una informació en matèria de seguretat.

Responsable de la seguretat

El responsable de seguretat determina les decisions per satisfer els requisits de seguretat de la informació i dels serveis.

Responsable del servei

Persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.

Responsable del sistema

Persona que s'encarrega de l'explotació del sistema d'informació.

Servei

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

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.

Aprovat en Consell de Govern de 21 de gener de 2014. (ACGUV 13/2014)
Modificat en Consell de Govern de 18 de febrer de 2019. (ACGUV 22/2019)