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 311/2022, pel qual es regula l'Esquema Nacional de Seguretat que, en l'article 12, 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) 2016/679 de 27 d'abril 2016 (GDPR) obliga al responsable del tractament a prendre tant les mesures jurídiques com les tècniques i organitzatives necessàries que garanteixen la seguretat de les dades de caràcter 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 Administracions Públiques en relació a la protecció de dades de caràcter 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 (aprovat mitjançant Reial Decret 311/2022).

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 8 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 10 i 21 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 9 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 311/2022 (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. Reglamento (UE) 2016/679 del Parlamento Europeo 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)

Modificat en Consell de Govern de 3 d'octubre de 2023. (ACGUV 246/2023)

Política de seguridad de la información en la utilización de medios electrónicos de la Universitat de València

VNIVERSITAT DE VALÈNCIA

VNIVERSITAT DE VALÈNCIA

Política de seguridad de la información en la utilización de medios electrónicos de la Universitat de València

Contenido

1. Introducción

Esta política de seguridad de la información se elabora en cumplimiento de la exigencia del Real Decreto 311/2022, por el cual se regula el Esquema Nacional de Seguridad que, en el artículo 12, establece la obligación para las administraciones públicas de disponer de una política de seguridad e indica los requisitos mínimos que tiene que cumplir.

Esta política de seguridad sigue también las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

El Reglamento (UE) 2016/679 de 27 de abril 2016 (GDPR) obliga al responsable del tratamiento a tomar tanto las medidas jurídicas como las técnicas y organizativas necesarias que garantizan la seguridad de los datos de carácter personal y evitan su alteración, pérdida, tratamiento o acceso no autorizado.

La Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

La Ley 40/2015, de Régimen jurídico del sector público establece que las administraciones públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos que garantizan la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de estas, garantizará la protección de los datos de carácter personal, y facilitará preferentemente la prestación conjunta de servicios a los interesados y recoge el ENS en su artículo 156.

La Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, compilación en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas en relación a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuran en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Todo esto motiva el cumplimiento del Esquema Nacional de Seguridad (aprobado intermediando Real Decreto 311/2022).

La adaptación al ENS implica que la Universitat de València y su personal tienen que aplicar las medidas mínimas de seguridad exigidas por el ENS y realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes unidades de gestión de la Universitat se tienen que cerciorar que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema de tramitación electrónica, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y los costes asociados tienen que ser identificados e incluidos en la planificación, en la solicitud de ofertas y en pliegos de licitación para proyectos de TIC.

Las unidades de gestión de la Universitat tienen que estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.

Prevención

La organización tiene que evitar, o al menos prevenir siempre que sea posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. En este sentido, se tienen que implementar las medidas mínimas de seguridad determinadas por el ENS, y también cualquier control adicional identificado mediante una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, tienen que estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización tiene que:

1. Autoritzar los sistemas antes de entrar en operación.
2. Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
3. Solicitar la revisión periódica por parte de terceros a fin de obtener una evaluación independiente.

Detección

Dado que los servicios se pueden degradar rápidamente a causa de incidentes, se tiene que monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo que establece el artículo 10 y 21 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que llegan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

La organización está obligada a:

1. Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
2. Designar puntos de contacto para las comunicaciones respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la Universitat de València.
3. Establecer protocolos para el intercambio de información relacionada con el incidente. Eso incluye comunicaciones, en los dos sentidos, con los equipos de respuesta a emergencias (CERT) reconocidos en el ámbito estatal como Iris-CERT, CCN-CERT y otros equivalentes.

Recuperación

Para restaurar la disponibilidad de los servicios, se tiene que desarrollar planes de contingencia de los sistemas TIC que incluyan actividades de recuperación de la información que contribuyan a la continuidad del servicio.

2. Misión

Tal como se refleja en sus Estatutos, la Universitat de València, como servicio público que es, tiene por misión impartir las enseñanzas necesarias para la formación de los estudiantes, la preparación para el ejercicio de actividades profesionales o artísticas y la obtención, si es el caso, de los títulos académicos correspondientes, como también para la actualización permanente del conocimiento y de la formación de su personal y del profesorado de todos los niveles de enseñanza.

La Universitat de València fomenta la investigación, tanto básica como aplicada, y el desarrollo científico y tecnológico. Asimismo, con las garantías de racionalidad y universalidad que le son propias, es una institución difusora de cultura en el seno de la sociedad.

La Universitat de València facilita, estimula y acoge las actividades intelectuales y críticas en todos los campos de la cultura y del conocimiento.

En el cumplimiento de todas estas funciones, la Universitat de València tiene presente la armonía de los saberes, originados en el desarrollo del pensamiento humano y destinados al perfeccionamiento de las personas y de su convivencia en una sociedad plural y democrática.

De forma estrechamente relacionada con el cumplimiento de esta misión, la organización desea manifestar la necesidad de una infraestructura TIC que prevalezca y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio a los usuarios, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

3. Alcance

La organización aplicará esta política de seguridad en aquellos sistemas de información que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

En concreto, atendida la misión de la Universitat definida en el punto 2, esta política de seguridad es aplicable sobre los siguientes sistemas de información TIC y los servicios que los conforman:

1. Gestión académica:
    - Servicios de gestión académica
    - Servicios de préstamos bibliotecarios
2. Gestión de automatrícula (subsistema de gestión académica):
    - Servicio de automatrícula
    - Servicios de admisión a la Universitat
3. Gestión de actas (subsistema de gestión académica):
    - Servicio de actas de evaluación
4. Gestión de títulos (subsistema de gestión académica):
    - Servicios de solicitud y emisión de títulos
5. Sede electrónica:
    - Servicios para PAS-PDI
    - Servicios vinculados a la investigación
    - Servicios para estudiantes
    - Servicios a externos
6. Gestión económica:
    - Servicios de contractación administrativa
7. Sistema de docencia virtual:
    - Aula Virtual
8. Portal web de la Universitat:

- Servicios de información administrativa

9. Sistema de gestión de Recursos Humanos
    - Servicio de gestión de Recursos Humanos.

La organización desestima la aplicación de esta política de seguridad sobre aquellos sistemas de información no reflejados en este apartado.

4. Marco normativo complementario

En el desarrollo y la implementación de esta política se tendrán en cuenta los Estatutos de la Universitat de València (Estudi General) y las sedes normativas de desarrollo relacionadas con sus objetivos.

5. Organización de la seguridad

Se pueden distinguir tres niveles en el organigrama de la Universitat de València:

1. Nivel 1 – Órganos de gobierno:
   Consejo de Gobierno/Alta dirección, que se ocupa de la organización, determina los objetivos que se propone conseguir y responde del hecho que se logren.
2. Nivel 2 – Dirección ejecutiva:
   Servicios/direcciones que se ocupen de qué hace cada unidad de gestión y cómo las diferentes unidades se coordinan entre sí para conseguir los objetivos marcados por la dirección.
3. Nivel 3 - Operacional:
   Se centra en una actividad concreta y controla como se hacen las cosas.

Siguiendo el mismo esquema y de acuerdo con el ENS, se estructura un organigrama de seguridad de la Universitat en tres niveles:

Nivel 1:
- Comité de gestión y coordinación de la seguridad de la información.
- Responsable de la información.
- Responsable del servicio.

Nivel 2:
- Responsable de la seguridad.

Nivel 3:
- Técnico de seguridad de los sistemas.
- Responsables de los sistemas de información.

La especificación de requisitos de seguridad (nivel 1) corresponde a los responsables de la información y de los servicios, junto con el responsable del fichero si hubiera datos de carácter personal. La operación (nivel 3) corresponde a los responsables de los sistemas, mientras que la supervisión corresponde al responsable de la seguridad (nivel 2) y al técnico de seguridad (nivel 3).

Por encima de todos estos está el comité de coordinación y gestión de la seguridad (nivel 1). Este comité de seguridad puede asumir también la responsabilidad de la información y de los servicios.

Comité de gestión y coordinación de la seguridad de la información

El comité de gestión y coordinación de la seguridad de la información (de ahora en adelante, Comité de Seguridad) coordina la seguridad de la información en cuanto a la organización.

De acuerdo con el RD 311/2022 (ENS), las funciones indicadas que corresponden al Comité de Seguridad son:

- Elaborar (y revisar periódicamente) la política de seguridad de la información para que sea aprobada por el Consejo de Gobierno de la Universitat.
- Aprobar y divulgar los procedimientos de seguridad de la Universitat.
- Promover la mejora continua de la gestión de la seguridad de la información de la Universitat.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Evaluar los principales riesgos residuales asumidos por la Universitat y recomendar posibles actuaciones respecto a estos.
- Evaluar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a estos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información. Promover la realización de las auditorías periódicas y evaluar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad de acuerdo con los recursos disponibles. Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, tiene que velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y secunden un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que pueda haber entre los diferentes responsables y/o entre diferentes áreas de la Universitat, y elevar aquellos casos en que no tenga suficiente autoridad para decidir.
- Evaluar las necesidades de recursos requeridos para el cumplimiento de los planes de actuación derivados de la aplicación de la política de seguridad.
- Elaborar un informe anual que se elevará al Consejo de Dirección de la Universitat.

El comité de seguridad está formado por:

- Vicerrector/a responsable de las tecnologías de la información y las comunicaciones, que preside el comité.
- Gerente.
- Secretario/aria general.
- Delegado/Delegada de Protección de Datos.
- Delegado/Delegada del rector/rectora para los temas TIC.
- Dos responsables de los servicios de la Universitat designados por el rector o la rectora.
- Responsable de seguridad de la información, que actúa como secretario del comité.

El comité de seguridad no es un comité técnico, pero pedirá regularmente al personal técnico propio o externo la información pertinente para tomar decisiones. El comité de seguridad se asesorará en los temas sobre los cuales tenga que decidir o emitir una opinión.

Responsable de la información

El responsable de la información establece los requisitos sobre la información proporcionada por medios electrónicos a través de los servicios de la Universitat y, por lo tanto, tiene la última palabra a la hora de decidir el tipo de información accesible y el uso que se pueda dar, en virtud de la reglamentación vigente y de las buenas prácticas en materia de protección de datos. Le corresponden las funciones siguientes:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y los responsables de los sistemas en el mantenimiento de los sistemas catalogados según el anexo I del ENS.

El responsable de la información es el secretario o la secretaria general de la Universitat.

Responsable de los servicios

El responsable de los servicios establece los requisitos de seguridad aplicables a los servicios proporcionados por la Universitat a través de medios electrónicos y, en este sentido, tiene por funciones:

- Establecer los requisitos de los servicios TIC en materia de seguridad.
- Trabajar en colaboración con el responsable de seguridad y los responsables de los sistemas donde se englobe el servicio para el mantenimiento de los sistemas catalogados según el anexo I del ENS.

El rol de responsable de los servicios lo asume el comité de seguridad.

Responsable de seguridad

El director del Servicio de Informática tiene el rol de responsable de seguridad de la información de la Universitat de València. Sus funciones son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC.
- Realizar las auditorías periódicas que permiten verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación del Servicio de Informática dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Verificar los informes de monitorización y auditoría de los estados de seguridad de los sistemas.
- Fomentar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el comité de seguridad incluyendo los incidentes más relevantes del periodo.

- Aprobación de los procedimientos de seguridad elaborados por los responsables de los sistemas cuando en virtud del contenido no requiera la aprobación del comité de seguridad.
- Proponer la redacción de aquella normativa de seguridad de la Universitat que considere necesario formalizar.
- Determinar la categorización de los sistemas y los requisitos de seguridad con carácter previo al arranque de un nuevo servicio vinculado al ENS.

Esta figura de "responsable de seguridad" descrita por el ENS coincide con la del responsable de seguridad de los ficheros de la Universitat de València.

Responsables de los sistemas

Se designará un responsable para cada uno de los sistemas de información definidos en el apartado de "Alcance" de este documento.

Entre sus áreas de actuación y en el marco de esta política de seguridad, los responsables de los sistemas tienen que llevar a cabo las funciones siguientes:

- Velar por el funcionamiento correcto del sistema durante todo su ciclo de vida, de sus especificaciones e instalación, e incorporar los requisitos de seguridad necesarios para la operativa en el sistema.
- Definir la topología y la política de gestión del sistema, y establecer los criterios de uso y los servicios que están disponibles.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema.
- Proponer al responsable de seguridad los cambios que afecten la seguridad del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del sistema y cerciorarse que estas se integran adecuadamente dentro del marco general de seguridad.
- Determinar los requisitos de la configuración autorizada del *hardware* y *software* que hay que utilizar en el sistema, en aquello que afecte su seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema que afecte la seguridad y la disponibilidad del servicio.
- Llevar a cabo el preceptivo proceso de revisión periódica del análisis y gestión de riesgos en el sistema.
- Elaborar y aprobar la documentación de seguridad del sistema.
- Delimitar las actuaciones que afectan la política de seguridad de cada entidad involucrada en el mantenimiento, la explotación, la implantación y la supervisión del sistema.
- Investigar los incidentes de seguridad que afectan el sistema, y si es el caso, comunicación al responsable de seguridad o a quién este determino.
- Establecer planes de contingencia y emergencia.

Además, el responsable del sistema puede acordar la suspensión del manejo de cierta información o la prestación de cierto servicio si es informado de deficiencias graves de seguridad que puedan afectar la satisfacción de los requisitos establecidos. Esta decisión tiene que ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

Técnico de seguridad de los sistemas

El técnico de seguridad de los sistemas es una figura operativa que depende del responsable de la seguridad. Tiene como misión principal asistir al responsable de seguridad en el nivel operativo que supone la supervisión integral de la seguridad de los sistemas de información incluidos en el alcance de esta política.

El técnico de seguridad tiene estas funciones:

- Verificar la aplicación de los procedimientos operativos de seguridad en los sistemas de información.
- Supervisar las instalaciones de *hardware* y *software*, sus modificaciones y mejoras para que la seguridad no esté comprometida y que en cada momento se ajusten a los procedimientos establecidos.
- Supervisar el estado de la seguridad de los sistemas.
- Informar al responsable de seguridad y los responsables de los sistemas de información sobre cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y la resolución de incidentes de seguridad, desde la detección hasta la resolución.
- Asesorar a los responsables de los sistemas para cumplir los requisitos de seguridad establecidos.

El técnico de seguridad de los sistemas es designado por el responsable de la seguridad.

5.1 Procedimientos de designación

El desempeño de las responsabilidades definidas en esta política de seguridad es determinado por el acceso a los diferentes cargos que se han vinculado a aquellas. En caso de que desaparezca o cambie de denominación alguno de estos cargos, será competencia del rector asignar el nuevo lugar a que quedará vinculada la figura.

6. Datos de carácter personal

La Universitat de València realiza tratamientos en qué hace uso de datos de carácter personal sometidos a lo que dispone el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Las medidas técnicas y organizativas de seguridad aplicables a las actividades de tratamiento de datos desarrollados en la Universitat de València están documentadas en el Registro de las Actividades de Tratamiento. Estas medidas están continuamente adaptándose al estado de la técnica, teniendo en cuenta los costes de aplicación y la naturaleza, el alcance, el contexto y las finalidades del tratamiento, así como a riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. Cualquier encargado del tratamiento de la Universitat de València, tendrá que aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

7. Gestión de riesgos

Todos los sistemas sujetos a esta política de seguridad tienen que llevar a cabo un análisis de riesgos, en el cual se evaluarán las amenazas y los riesgos a que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez cada dos años.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando tenga lugar un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el comité de seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados.

8. Desarrollo de la política de seguridad

Esta política se desarrolla por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Otros documentos que complementan esta política de seguridad son:

- Normas de uso personal de los recursos informáticos y telemáticos de la Universitat de València.
- Los acuerdos del Consejo de Gobierno de la Universitat posteriores a la aprobación de esta política en la medida en que puedan afectarla.
- Los análisis de riesgos realizados de las actividades de tratamiento.
- Las evaluaciones de impacto en la protección de datos.
- La normativa de seguridad tendrá que estar disponible en la intranet de la Universitat.

9. Obligaciones del personal

Todos los miembros de la Universitat de València tienen la obligación de conocer y cumplir esta política de seguridad de la información y la normativa de seguridad desplegada a partir de esta, y es responsabilidad del comité de seguridad disponer los medios necesarios para que la información llegue a las personas afectadas, teniendo en cuenta siempre las disponibilidades presupuestarias de la Universitat.

Todos los trabajadores y trabajadoras de la Universitat de València bajo el alcance del ENS atenderán a una acción de concienciación en materia de seguridad TIC, al menos una vez cada dos años. Se establecerá un programa de acciones en concienciación continua para atender a todos los miembros de la Universidad relacionados con servicios de administración electrónica, en particular los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de la Universitat. Se realizará una acción de concienciación durante los dos años siguientes a la aprobación de esta política de seguridad y de manera continuada para el personal de nueva incorporación.

En caso de que se requiera formación específica para el manejo seguro de los sistemas, las personas con responsabilidad en la operación o administración de sistemas TIC la recibirán en la medida en que la necesiten para realizar su trabajo.

10. Terceras partes

Cuando la Universitat de València preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta política de seguridad de la información. Con este objeto, se establecerán canales para información y coordinación de los respectivos comités de coordinación del ENS y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universitat de València utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad que implique estos servicios o información. Esta tercera parte quedará sujeta a las obligaciones establecidas en la normativa mencionada y se tendrá que incorporar a los pliegos y pedidos de la Universitat. Con esto, el proveedor tendrá que garantizar que su personal está adecuadamente formado en materia de seguridad de acuerdo con los requerimientos de la Universitat.

11. Entrada en vigor

Esta política de seguridad de la información es efectiva desde el día siguiente a la fecha en que la apruebe el Consejo de Gobierno de la Universitat de València y hasta que sea reemplazada por una nueva política.

12. ANNEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal

Cualquier información que concierne a personas físicas identificadas o identificables. Reglamento (UE) 2016/679 del Parlamento Europeo de protección de datos de carácter personal.

Gestión de incidentes

Plano de acción para atender las incidencias que se dan. Además de resolverlas, tiene que incorporar medidas de desempeño que permiten conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas. ENS.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización respecto a los riesgos. ENS.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias que van en detrimento de la seguridad del sistema de información. ENS.

Información

Caso concreto de cierto tipo de información.

Política de seguridad

Conjunto de directrices plasmadas en un documento escrito, que rigen la manera como una organización gestiona y protege la información y los servicios que considera críticos. ENS.

Principios básicos de seguridad

Fudamentos que tienen que regir toda acción orientada a asegurar la información y los servicios. ENS.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación ejercida por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Aprobado en Consejo de Gobierno de 21 de enero de 2014. (ACGUV 13/2014)
Modificado en Consejo de Gobierno de 18 de febrero de 2019. (ACGUV 22/2019)
Modificado en Consejo de Gobierno de 3 de octubre de 2023. (ACGUV 246/2023)