PROCEDIMENT DE CLASSIFICACIÓ DE LA INFORMACIÓ A LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprovat per Consell de Govern de 6 de juny de 2024

1. Objecte

L'objecte d'aquest procediment és la definició de la classificació de la informació en els sistemes tecnològics de la Universitat Politècnica de València dins de l'abast que s'estableix en l'Esquema nacional de seguretat, tot aplicant el conjunt de mesures de seguretat que calen per a un compliment adequat de la normativa; en concret, les establides pels apartats "Protecció de la informació [mp.info]" i "Protecció dels suports d'informació [mp.si]".

Els principis o objectius que han guiat la redacció d'aquesta normativa són els següents:

- Determinar uns criteris de classificació de la informació a la Universitat Politècnica de València.
- Definir els criteris de marcatge i etiquetatge de la informació.
- Establir les mesures de seguretat mínimes que han d'aplicar-se en el tractament, segons el nivell de protecció, tant en la informació com en els suports.

2. Àmbit d'aplicació

Aquest procediment s'aplica a tot l'àmbit d'actuació de la Universitat Politècnica de València, i els seus continguts es deriven de les directrius de caràcter més general definides en l'ordenament jurídic vigent, i en la Política de seguretat de la informació i la Normativa de seguretat de la UPV.

Aquest document és aplicable i de compliment obligatori per a tot el personal i tots els usuaris que, de manera permanent o eventual, presten serveis o treballen internament a la Universitat Politècnica de València, incloent el personal de proveïdors externs quan siga usuari dels sistemes d'informació de la Universitat Politècnica de València.

3. Rols i responsables

En el procediment de classificació de la informació intervenen els rols següents:

Responsable de seguretat:

- Coopera amb els responsables de la informació, i els assessora, en la classificació de la informació de l'organització.
- Proposa la implantació de controls per a validar l'etiquetatge, el marcatge i el tractament adequats de la informació, i per a detectar-hi desviacions.
- Autoritza la destrucció o l'esborrament de suports amb informació sensible.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

Responsables de la informació:

- Aproven l'arquitectura i els mètodes de classificació de la informació que es troba sota la seua responsabilitat.

Responsables del sistema:

- Assessoren sobre quines mesures de seguretat es poden implementar en el sistema.

Administradors del sistema:

- Executen satisfactòriament la implantació de mesures de seguretat, com ara la destrucció o l'esborrament dels suports que contenen informació sensible.

Usuaris:

- Accedeixen a la informació i als suports, i, en conseqüència, han d'estar-hi degudament autoritzats i comprometre's a complir els requisits d'accés corresponents.

4. Normativa

4.1. Criteris de classificació de la informació

Com a estratègia de gestió del risc sobre amenaces que poden comprometre la informació, s'estableixen diferents nivells de protecció, que garanteixen controls majors segons la importància que presenten per al negoci.

A aquesta classificació no s'hi aplica la Llei 9/1968, de 5 d'abril, sobre secrets oficials.

S'ha establit un criteri de classificació de la informació i s'han determinat unes mesures de seguretat proporcionals al nivell de rellevància del contingut. Les categories establides es mostren en la taula següent:

Etiquetatge	Definició
Informació SENSE CLASSIFICAR o PÚBLICA	Informació antiga que encara no ha sigut categoritzada atenent els criteris de l'ENS o que és de domini públic, i per tant, d'accés lliure a tothom.
Informació D'ÚS OFICIAL	Informació a la qual pot tenir accés diferent personal de l'organització, depenent de les seues característiques o de les responsabilitats que hi tenen. No hi hauria d'accedir personal que no hi haja sigut autoritzat o personal extern a l'organització.

4.1.1. Informació SENSE CLASSIFICAR

Es considera informació SENSE CLASSIFICAR la que no té assignat cap dels altres nivells de classificació.

Aquest és un estat temporal que s'assigna a qualsevol mena d'informació que no estiga categoritzada en la present normativa.

Aquest fet s'ha de traslladar al responsable de seguretat o al responsable de la informació que corresponga, segons l'àrea o contingut, perquè hi assigne un nivell de protecció i incloga aquest nou tipus d'informació en la preassignació de nivells que estableix la present normativa.

La informació que haja sigut categoritzada com a SENSE CLASSIFICAR se sotmet als criteris següents:

- Etiquetatge: cap.
- Marcatge: cap.
- Tractament: la informació SENSE CLASSIFICAR ha de passar pel procés de classificació perquè es puga marcar segons el nivell de protecció que calga i s'autoritze i es vincule a un responsable de la informació.

4.1.2. Informació PÚBLICA

La Universitat Politècnica de València considera com a informació PÚBLICA la que és d'àmbit públic i no està sotmesa a requisits legals que requerisquen preservar-ne la sensibilitat o confidencialitat.

Això suposa que s'assumeix com un risc acceptable que se'n produïsca una filtració, modificació o difusió.

En suport de paper, *informació pública* és tota informació que s'ubique a les zones comunes o accessibles i no estiga custodiada per cap responsable.

La informació que haja sigut categoritzada com a PÚBLICA se sotmet als criteris següents:

- Etiquetatge: cap.
- Marcatge: cap.
- Tractament: la informació que haja sigut categoritzada com a PÚBLICA no està subjecta a cap tractament especial ni gestionada de manera obligatòria.

4.1.3. Informació D'ÚS OFICIAL

La informació marcada com a D'ÚS OFICIAL és la que està sotmesa a requisits legals que requereixen preservar-ne la sensibilitat i confidencialitat, té valor en les dimensions de confidencialitat o integritat, i suposa riscos àmpliament acceptables o tolerables si se'n produeix una filtració, modificació o difusió.

La Universitat Politècnica de València considera com a informació D'ÚS OFICIAL la que, pel contingut que presenta, el responsable de la informació considere expressament com a tal.

Per a la informació D'ÚS OFICIAL es defineixen condicions d'accessos especials que afectaran els arxius físics en suport de paper i els arxius en suport electrònic.

La informació D'ÚS OFICIAL només la poden conèixer per persones concretes en cada àrea de l'entitat, i suposa riscos inacceptables si se'n produeix una filtració, modificació o difusió.

La informació que haja sigut categoritzada com a D'ÚS OFICIAL se sotmet als criteris següents:

- Etiquetatge: explícit, de manera visible i intel·ligible, en qualsevol mena de suport.
- Marcatge: explícit, de manera visible i intel·ligible, en suports digitals.
- Tractament: cal tenir en compte això que segueix:

Com a regla general, s'hi empra el principi de *privilegis mínims*, és a dir, l'assignació d'accés es produeix sobre la base de la necessitat de conèixer, i la fa el responsable de la informació.

La regulació de la difusió i la còpia de les dades està restringida, excepte al personal que necessite conèixer les dades per a acomplir correctament la seua labor dins de l'organització.

S'estableix la prohibició de transmissió, a usuaris tant interns com externs, per qualsevol mitjà de suport que no siga el que el responsable de la informació haja autoritzat.

Emmagatzematge en carpetes electròniques:

- L'emmagatzematge de la informació es pot fer en qualsevol actiu de l'organització, i mai en dispositius externs a l'organització.
- La informació emmagatzemada en els diferents mitjans electrònics, com ara en un servidor de fitxers o al núvol, s'ha de limitar tot definint grups de seguretat per a determinar quins són els privilegis d'accés que cal assignar-hi.
- És el responsable de servei qui determina quins usuaris, siguen interns o externs, poden tenir accés a la informació.

Documentació en suport de paper:

- Tota la documentació rellevant de cadascuna de les àrees ha d'estar autoritzada pel responsable de la informació, que ha de vetlar per garantir el compliment de les mesures.
- La informació ha d'estar emmagatzemada a les zones de treball de cadascuna de les àrees de l'entitat.
- Aquesta informació no es pot allotjar en zones de pas o accés públic al ciutadà, sinó sols en espais d'accés restringit al personal de l'entitat.

Els criteris anteriors els defineix i aprova, per a aquesta mena de dades, el responsable de la informació amb el suport del responsable de seguretat; i es comuniquen adequadament a les persones que, pel treball que fan dins de l'organització, necessiten tenir accés a aquesta mena d'informació.

4.2. Localització de la informació

La Universitat Politècnica de València té tota la informació en suport electrònic en les carpetes compartides en els servidors de fitxers corporatius i en les carpetes al núvol corporatiu en OneDrive.

En tots dos sistemes, les mesures de seguretat són les adequades per a donar suport al criteri de classificació de la informació proposat.

4.3. Tractament de la Informació

En qualsevol dels casos descrits, cal implementar les mesures de seguretat previstes en l'Esquema nacional de seguretat.

Quant a l'etiquetatge, els actius s'han d'identificar segons el criteri de classificació establit en l'apartat anterior.

Quant a la custòdia, cal aplicar la diligència i el control deguts als suports d'informació que romanen sota la responsabilitat de l'organització, mitjançant les actuacions següents:

- Garantint-hi el control d'accés amb mesures físiques o lògiques, o d'ambdós tipus.
- Garantint que es respecten les exigències de manteniment del fabricant d'aquests suports, especialment pel que fa a la temperatura, la humitat i altres agressors mediambientals.

Quant a la digitalització, amb caràcter general, quan s'escanegen documents, l'usuari ha de ser especialment acurat amb la selecció del directori compartit on s'hagen d'emmagatzemar les imatges obtingudes. Convé no oblidar retirar els originals de l'escàner quan haja acabat el procés de digitalització. Si un usuari troba documentació abandonada en un escàner, ha d'intentar localitzar-ne el propietari perquè l'arreplegue immediatament; si en desconeix el propietari o bé no pot localitzar-lo, ha de posar-ho de manera immediata en coneixement del responsable de seguretat.

Quant al transport o transmissió, els intercanvis d'informació s'han de fer preferentment en suport electrònic. Quan hagen d'enviar-se documents D'ÚS OFICIAL, aquest enviament ha de garantir que només el receptor legítim puga conèixer aquesta informació. Amb aquesta finalitat cal fer servir tècniques de xifratge de dades siga del contingut del missatge (xifratge d'arxius) siga del canal de comunicació (xifratge de les comunicacions mitjançant l'ús de protocols segurs).

Quan l'enviament es faça mitjançant serveis de missatgeria, cal assegurar-se que el transportista compleix les mesures de seguretat establides per l'ENS i satisfà els requisits requerits pel nivell de classificació de la documentació enviada.

Quant a la neteja de documentació en suport electrònic, cal retirar-ne tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació siga pertinent per al receptor del document. Aquesta mesura és especialment rellevant quan el document es difon àmpliament, com ocorre quan s'ofereix al públic en un servidor web o en un altre tipus de repositori d'informació.

Quant a còpies de seguretat, el sistema implantat actualment permet recuperar dades perdudes –accidentalment o intencionada– amb una antiguitat determinada.

Quant a la destrucció, la mesura d'esborrament i destrucció de suports d'informació s'ha d'aplicar a tota mena d'equips susceptibles d'emmagatzemar informació, incloent mitjans tant electrònics com no electrònics. Els suports que hagen de ser reutilitzats per a una altra informació o alliberats a una altra organització han de ser objecte d'un esborrament segur del contingut anterior. Cal destruir de manera segura els suports quan la naturalesa del suport no permeta fer-ne un esborrament segur.

5. Definicions

Informació: és una dada que es tracta i que posseeix un significat per a l'organització.

Suport: és un objecte físic o abstracte susceptible de ser tractat en un sistema d'informació i sobre el qual es poden gravar o recuperar dades.

Com a exemples de suports físics s'enumeren els següents: memòries USB o llapis de memòria, DVD, CD, disquets, discos durs, cintes DAT, cintes LTO, i en definitiva, qualsevol dispositiu que emmagatzeme dades rellevants.

En aquest sentit, els suports d'emmagatzematge es caracteritzen per la portabilitat i per no integrar-se a l'interior de dispositius d'emmagatzematge primari com un servidor o un terminal d'usuari.

Com a exemple de suport abstracte cal esmentar els sistemes emmagatzematge al núvol, com és el cas del sistema corporatiu OneDrive.

Amb relació al tractament no automatitzat o no informatitzat, cal entendre com a suport físic d'emmagatzematge els arxivadors, les prestatgeries, els armaris, etc. que emmagatzemen arxius en paper amb informació classificada.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen