Acord del Consell de Govern de 22 de desembre de 2011 pel qual s'aprova la Normativa d'ús de les tecnologies de la informació i la comunicació.

NORMATIVA D'ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ (TIC)

La Universitat Rovira i Virgili (en endavant, URV) posa a disposició dels membres de la comunitat universitària que hi desenvolupen la seva activitat acadèmica i/o professional les tecnologies de la informació i comunicació (en endavant, TIC) necessàries per dur-la a terme amb qualitat i eficàcia.

L'ús que els usuaris han de fer d'aquestes TIC es basa en la confiança mútua i el respecte a la legislació vigent. Tanmateix, cal establir una normativa d'ús que sigui coneguda i acceptada per tots els usuaris i una guia de recomanacions que en faciliti l'ús i la gestió.

A continuació es desenvolupa aquesta normativa d'ús. Així mateix, s'hi incorpora la guia de recomanacions com a annex I, la relació de serveis de xarxa de la URV com a annex II i un glossari de temes específics com a annex III.

CAPÍTOL 1. DISPOSICIONS GENERALS

Article 1. Objecte i àmbit d'aplicació

1. Objecte. Aquesta normativa regula les condicions d'ús de les TIC que la URV posa a disposició de les persones incloses en el seu àmbit d'aplicació, d'acord amb el que s'estableix a l'apartat següent.

2. Àmbit d'aplicació. Aquesta normativa és d'aplicació a la comunitat d'usuaris de TIC de la URV, que inclou els estudiants, el col·lectiu docent i investigador (CDI), el personal d'administració i serveis (PAS), el col·lectiu d'Amics i Amigues de la URV i qualsevol altra persona que, per la seva relació amb la URV, hagi estat autoritzada a fer ús d'aquestes TIC.

Article 2. Condició d'usuari

El registre com a usuari de TIC de la URV es fa efectiu un cop la persona interessada hagi rebut aquestes normes i n'hagi signat l'acceptació, signatura que es produeix en el mateix moment que s'incorpora a la URV:

a) En el cas del CDI i el PAS, en l'acte de formalització del nomenament, contracte o credencial, segons correspongui.

b) En el cas dels estudiants, en el moment d'adquirir la condició d'estudiant de la URV d'acord amb l'Estatut de la URV.

c) En el cas del col·lectiu d'Amics i Amigues URV, en el moment d'adquirir-ne la condició, d'acord amb la normativa corresponent.

d) Per a la resta d'usuaris, en el moment de l'autorització expressa.

Article 3. Contrasenya

Cada usuari rep un nom d'usuari únic i una contrasenya. La contrasenya ha de ser secreta i segura i no es pot transferir a altres persones. Les persones no registrades en tenen absolutament prohibit l'ús.

Els usuaris han de complir les següents regles pel que fa a la confidencialitat de la contrasenya del correu electrònic:

a) Els usuaris no han de revelar les contrasenyes a ningú. El darrer responsable de l'ús indegut del compte de correu és el mateix titular, encara que pugui demostrar que no és la persona que l'ha utilitzat.

   Els procediments operacionals de la URV poden exigir que les contrasenyes es comparteixin amb els administradors. Això és acceptable només en les circumstàncies següents:

   - Amb l'autorització prèvia de l'interessat
   - En presència de l'interessat

   En qualsevol cas, un cop finalitzada l'assistència, l'interessat és el responsable de canviar la contrasenya.

b) Els usuaris no han d'escriure les contrasenyes en cap suport paper.

c) Els usuaris no han d'emmagatzemar les contrasenyes, llevat que el suport físic estigui xifrat i protegit amb contrasenyes segures.

d) Els usuaris no han de marcar la casella "Recorda la meva contrasenya" del programari de client, com la missatgeria instantània, navegadors i xarxes privades virtuals.

e) Els usuaris no han d'utilitzar la mateixa contrasenya en sistemes administrats per altres organitzacions.

f) Els usuaris han de tenir cura de no divulgar accidentalment les contrasenyes. Cal canviar-les immediatament:

   - Si se sospita que algú ha descobert la contrasenya
   - Després d'usar-les per a l'accés remot des d'un ordinador públic compartit (per exemple, un quiosc o una cafeteria d'Internet)

Article 4. Intents d'autenticació

A un usuari se li permet un màxim de deu intents de connexió en qualsevol sistema, inclosos espais com el Moodle o la intranet; després d'això el compte de l'usuari és bloquejat/revocat i l'usuari ha de contactar amb el servei d'assistència (o fer servir el mecanisme aprovat per la URV com a eina d'autoservei) per desbloquejar/reactivar el compte.

En tant que ho permetin els sistemes d'informació, el Servei de Recursos Informàtics i TIC pot forçar bloquejos temporals del compte per tal d'evitar atacs sistemàtics per obtenir la contrasenya.

Article 5. Ús de les TIC

1. L'usuari es fa responsable del bon ús del maquinari i del programari que utilitzi en el desenvolupament de les seves funcions i, per tant, no ha de posar en perill, de manera deliberada, la integritat dels equips, dels programes o d'altres sistemes d'informació.

2. L'ús del correu electrònic i l'ús d'Internet estan orientats a l'activitat acadèmica i/o professional, però no a usos de caràcter personal, i s'han d'evitar els continguts que puguin desacreditar la URV o els seus membres, els de caràcter il·legal o els de naturalesa ofensiva, així com opinions alienes a l'àmbit acadèmic o professional. El mateix s'aplica a les publicacions a la xarxa.

3. La URV opera basant-se en la confiança, però en cas de tenir una o més proves o suficients indicis d'un ús que contravingui les normes, pot fer les oportunes indagacions, fins i tot accedint a l'ordinador de les persones implicades, prèvia incoació de l'expedient corresponent.

Article 6. Adreces massives

1. L'adreça electrònica toturv@urv.cat està limitada als missatges de tipus institucional emesos pel Consell de Direcció i té com a unitat gestora la Secretaria General. L'ús d'altres adreces massives (pdi@urv.cat, pas@urv.cat i estudiants@estudiants.urv.cat) està limitat als missatges d'interès general per al col·lectiu i ha de ser autoritzat prèviament pel vicerectorat competent en matèria de CDI (CDI), per Gerència (PAS) i pel vicerectorat competent en matèria d'estudiants (estudiants), respectivament. Altres llistes de distribució d'àmbit més reduït estan descrites a la intranet de la URV, a l'apartat Llistes de distribució.

2. Per donar a conèixer a la comunitat universitària actes acadèmics, científics o culturals s'han d'utilitzar els mitjans existents amb aquesta finalitat, com pot ser l'Agenda URV, a través del Gabinet de Comunicació i Relacions Externes.

Article 7. Ús del programari subjecte a drets d'autor

El programari de la URV que està subjecte a drets d'autor no es pot copiar sense permís del propietari, ni ser utilitzat en màquines alienes ni lliurat a terceres persones, excepte que s'hagi obtingut permís exprés de la URV. La relació completa del programari subjecte a drets d'autor és a la intranet de la URV, a l'apartat Programari oficial, programari privatiu.

Article 8. Còpies de seguretat

La URV posa a disposició dels usuaris de TIC un sistema que diàriament fa còpies de seguretat de les dades dipositades en els servidors centrals. Els usuaris es comprometen a utilitzar aquest sistema, especialment quan es gestionen dades d'interès general de la URV. La URV no es fa responsable de les possibles pèrdues de dades que no hagin seguit els protocols de còpia de seguretat establerts, sense perjudici de la responsabilitat que es pugui derivar de la pèrdua d'informació deguda a una negligència de l'usuari.

Article 9. Protecció de dades

L'ús de TIC que comporti la gestió de dades per part de qualsevol membre de la comunitat universitària ha de respectar la normativa vigent i, en especial, la relativa a la protecció de dades de caràcter personal. El control de l'ús que per motius acadèmics es faci d'aquestes dades és responsabilitat del professor o professora que tutoritza les activitats que han motivat l'accés a les dades.

Article 10. Mesures disciplinàries en cas d'infracció, mal ús o pirateria

1. La pirateria i altres usos no autoritzats dels equips, dels programes o d'altres sistemes d'informació de la URV estan prohibits.

2. Si es confirma la vulneració d'aquestes normes, la URV pot prendre mesures disciplinàries, sense perjudici d'altres mesures legals si es tracta de fets constitutius de delicte.

3. En tots els casos, la URV es reserva el dret d'exercitar les accions que consideri oportunes contra qualsevol persona o entitat que amb la seva acció o omissió perjudiqui els interessos o la imatge de la URV.

4. Així mateix, l'usuari és l'únic responsable davant de les autoritats competents en cas d'infracció de la normativa general de la URV, del marc legislatiu i jurídic nacional i internacional aplicable, així com de les normes de comportament acceptades per la comunitat d'usuaris d'Internet.

5. Qualsevol infracció o incompliment d'aquesta normativa pot ser considerada com a falta administrativa, d'acord amb les diverses normatives que regulen el règim disciplinari dels diferents col·lectius de la comunitat universitària.

CAPÍTOL 2. NORMES PER A L'ÚS DEL CORREU ELECTRÒNIC

Article 11. Definició del servei de correu electrònic

1. La URV posa a disposició dels seus usuaris de TIC el servei de correu electrònic com a vehicle d'intercomunicació institucional i personal entre ells i, per extensió, amb tota la comunitat d'Internet.

2. El servei de correu electrònic queda definit en tot moment per les condicions establertes en aquesta normativa. La utilització del servei implica el coneixement i l'acceptació implícita i incondicionada de totes i cadascuna d'aquestes condicions.

3. La URV pot introduir les modificacions que consideri convenients en la prestació d'aquest servei, inclosa la seva cancel·lació, sense que l'usuari pugui reclamar-li cap responsabilitat sobre els perjudicis causats per aquestes. En qualsevol cas, les modificacions i la cancel·lació han de ser comunicades abans de la seva aplicació a través de canals que assegurin la màxima difusió entre els usuaris del servei (normalment, el mateix correu electrònic).

Article 12. Altes i baixes al servei

1. Tots els membres de la comunitat universitària de la URV són donats d'alta automàticament com a usuaris d'aquest servei en el moment que s'incorporen a la URV (vegeu l'article 2). Cada persona ha de conservar l'adreça assignada durant tot el període de vinculació amb la URV.

2. La sol·licitud d'adreces genèriques o institucionals s'ha d'adreçar a la Secretaria General de la URV, que n'ha de valorar l'autorització.

3. L'usuari és donat de baixa automàticament del servei tres mesos després que hagi deixat de ser membre de la comunitat universitària.

4. La URV pot suspendre el servei, temporalment o definitiva, als usuaris que incompleixin qualsevol de les condicions d'aquesta normativa, prèvia incoació del corresponent expedient.

Article 13. Identificació

L'accés al servei de correu electrònic exigeix la identificació de l'usuari mitjançant un nom d'usuari i una contrasenya. La contrasenya pot ser modificada per l'usuari tantes vegades com consideri necessàries per assegurar la privacitat i seguretat del seu compte. Aquesta identificació és personal i intransferible i l'usuari és l'únic responsable de totes les accions fetes des del seu compte de correu.

Article 14. Format dels missatges electrònics

Els missatges electrònics enviats des de l'adreça de correu de la URV es regeixen per les directrius de format que aprovi el Consell de Govern.

Article 15. Accés via web

L'accés via web es fa a través d'una interfície web, dissenyada perquè l'usuari pugui realitzar la gestió del correu electrònic. El Servei de Recursos Informàtics i TIC ha d'informar puntualment sobre els navegadors recomanats que permeten aquest accés.

Article 16. Accés via client POP3/IMAP4 i POP3S/IMAP4S

L'accés al correu electrònic es realitza configurant el client de correu POP3/IMAP, un cop l'usuari hagi estat donat d'alta en el servei. Aquest accés pot ser POP3 i/o IMAP4 des de la xarxa commutada de la URV i ha de ser utilitzant els protocols POP3S i IMAP4S des de qualsevol altra ubicació.

Article 17. Localització

El servei és accessible des de qualsevol equipament connectat a Internet, amb independència de la seva localització física. Així, l'usuari pot accedir-hi tant des de les dependències de la URV com des d'altres localitzacions.

Article 18. Volum de les bústies

El volum de les bústies està d'acord amb el perfil d'usuari i la disponibilitat, i es pot consultar al catàleg de serveis de la URV. Si escau, es pot sol·licitar l'ampliació d'aquest volum mitjançant el corresponent procediment publicat a la intranet de la URV.

Article 19. Redirecció

Sota petició de l'interessat, es pot sol·licitar la redirecció de l'adreça de correu electrònic de la URV cap a una adreça externa de correu electrònic. Es pot sol·licitar aquesta redirecció d'adreça mitjançant el corresponent procediment publicat a la intranet de la URV.

Article 20. Seguretat

Per assegurar la privacitat de les dades, el servei de correu electrònic s'ha d'oferir amb encriptació de les comunicacions quan l'accés sigui via web i amb protocols segurs per als clients de correu electrònic. Per aquest motiu, quan s'hi accedeix per primera vegada cal incorporar l'autoritat de certificació de la URV al navegador o al client de correu, d'acord amb les instruccions que figuren a la Guia de recomanacions que s'adjunta a aquesta normativa com a annex I.

Article 21. Filtre antivirus i antispam

Per tal d'assegurar la qualitat del servei i evitar la propagació de virus i la recepció de missatges electrònics considerats correu brossa (spam, en anglès), la URV ha

d'aplicar filtres d'entrada a les bústies de correu amb l'objectiu de minimitzar els perjudicis que aquests tipus de missatges produeixen.

Article 22. Còpies de seguretat

Dins del procediment establert de còpia de seguretat, el Servei de Recursos Informàtics i TIC fa diàriament una còpia de l'estat de les bústies per poder recuperarne, si és necessari, el contingut.

Article 23. Registre (log)

Tots els missatges electrònics enviats/rebuts a la URV són processats pel servidor de correu, el qual en registra l'hora, l'emissor i el receptor. D'acord amb la legislació vigent en matèria de conservació de les dades relatives a les comunicacions electròniques i de protecció de dades de caràcter personal, aquest registre es guarda un mínim de sis mesos.

Article 24. Atenció a l'usuari

L'atenció a l'usuari es proporciona d'acord amb el perfil d'usuari amb el qual s'accedeix a la intranet de la URV.

Article 25. Responsabilitats de la URV

1. La URV, com a institució prestadora d'aquest servei, és la responsable de supervisar el compliment de la seva normativa d'ús per part de cadascun dels usuaris, prenent les mesures disciplinàries corresponents en cas d'incompliment.

2. La URV no es fa responsable en cap cas del contingut dels missatges enviats o rebuts pels seus usuaris, tot i que aquests puguin contravenir la legislació vigent o fer apologia d'actuacions incíviques o socialment reprovables.

3. Així mateix, la URV queda exonerada de tota responsabilitat derivada de l'obtenció, intromissió o modificació fraudulenta de missatges electrònics per part de l'usuari o de tercers, així com de qualsevol acció que vulneri la privacitat i secret d'aquest tipus de comunicacions.

Article 26. Responsabilitats de l'usuari

L'usuari s'obliga a:

a) Fer-ne una utilització conforme a aquesta normativa.

b) Garantir la seguretat del seu compte, guardant el secret del nom d'usuari.

c) Respectar la privacitat de les comunicacions.

d) Evitar difondre continguts protegits per propietat intel·lectual, sense l'expressa autorització dels propietaris dels drets, o altres continguts que puguin atemptar contra l'honor i la imatge de persones o institucions.

e) Usar el compte amb la finalitat per la qual ha estat creat, i no utilitzar-lo com a eina d'activitats comercials, empresarials o de qualsevol altre tipus.

f) No realitzar cap actuació que pugui resultar molesta o intencionadament perjudicial per als usuaris o entitats presents a Internet.

CAPÍTOL 3. PARTICIPACIÓ EN CANALS WEB

Article 27. Participació en canals d'Internet

1. Els canals d'Internet (xarxes temàtiques i socials en general com Facebook, Twitter, Viquipèdia, webs temàtics, etc.) representen una oportunitat fonamental per a la URV per desenvolupar les seves activitats a través del seu àmbit d'usuaris i clients, actuals i potencials, proveïdors de tecnologia, sectors empresarials, mitjans de comunicació, etc., i interaccionar-hi. Tanmateix, la participació dels membres de la URV en canals d'Internet s'ha de regir per les directrius que constitueixen aquesta normativa.

2. L'únic representant legal de la URV és el rector o rectora. Qualsevol representació en nom de la URV en un canal d'Internet ha d'haver estat autoritzat prèviament pel rector o rectora o per l'òrgan competent en què delegui.

CAPÍTOL 4. ENTORN VIRTUAL D'APRENENTATGE (MOODLE)

Article 28. Definició

L'entorn virtual d'aprenentatge (EVA) de la URV és un entorn de treball a Internet que serveix de suport a la docència i orientació universitària.

Article 29. Accessibilitat

1. L'EVA, que funciona sobre la plataforma Moodle, és accessible 24 hores al dia, 7 dies a la setmana, i per accedir-hi només cal un ordinador amb accés a Internet i un navegador.

2. Per accedir a Moodle, els usuaris de la URV han d'utilitzar el nom d'usuari i la contrasenya institucionals d'accés als serveis de xarxa de la URV.

3. En el cas dels membres de la comunitat universitària, l'adreça de correu electrònic institucional és la destinatària de les notificacions que es generen a Moodle.

Article 30. Continguts

1. Els continguts que es publiquen a Moodle han d'estar exclusivament destinats a la docència i la recerca vinculades a la URV o als seus processos de gestió.

2. El contingut protegit per drets d'autor s'ha d'utilitzar d'acord amb la normativa vigent. Si és el cas, s'ha de fer referència de l'autoria.

3. En cap cas no es pot publicar informació o documents que atemptin contra la dignitat de les persones i que contravinguin la normativa de la URV.

4. L'usuari que publica continguts a Moodle es fa responsable dels continguts publicats i de les conseqüències de la seva publicació.

5. La URV no es fa responsable dels continguts publicats a Moodle.

Article 31. Condicions d'ús

El primer accés a Moodle requereix l'acceptació de les seves condicions d'ús.

Article 32. Guia d'ús

L'accés a Moodle, amb la seva guia completa d'ús i descripció del servei, és a l'apartat de la intranet Serveis de xarxa.

CAPÍTOL 5. ALTRES SERVEIS DE XARXA

Article 33. Altres serveis de xarxa

La URV posa a disposició dels membres de la comunitat universitària altres serveis de xarxa, esmentats a l'annex II d'aquesta normativa, als qual es pot accedir des del catàleg de serveis de la URV i des de l'apartat de la intranet Serveis de xarxa. El Servei de Recursos Informàtics i TIC és el responsable de mantenir actualitzada en tot moment aquesta llista de serveis.

ANNEX I

GUIA DE RECOMANACIONS

A qui va dirigida:

Persones afectades: els propietaris de sistemes i tots els membres de la comunitat d'usuaris de TIC de la URV, segons s'estableix a l'apartat 1.1 de la Normativa TIC de la URV, així com altres persones autoritzades per accedir als sistemes d'informació de la URV.

Persones responsables de l'aplicació, el canvi i la comunicació d'aquesta guia: El secretari o secretària general, el o la gerent i l'àrea competent del Servei de Recursos i TIC.

1. CONTRASENYA

I. Guia de la contrasenya

Les contrasenyes són una eina important de la URV per protegir els seus sistemes tecnològics i actius d'informació, perquè garanteixen que només hi puguin accedir les persones autoritzades. L'acompliment d'aquesta política pren especial rellevància arran de la implantació del nom d'usuari i contrasenya únics, així com la implantació d'un sistema únic de validació (SSO, etc.) per a tots els sistemes d'informació de la URV, on la fortalesa de la contrasenya és un punt clau.

II. Longitud i complexitat de la contrasenya

La fortalesa d'una contrasenya depèn de la seva longitud i complexitat.

Podeu veure les diferents opcions d'acompliment de seguretat a la intranet de la URV.

III. Històric de contrasenyes

Una nova contrasenya no ha de ser la mateixa que qualsevol de les contrasenyes utilitzades anteriorment per un mateix usuari, per evitar la reutilització d'una contrasenya que l'usuari hagi canviat a causa d'una revelació coneguda o sospitada.

2. ÚS DEL CORREU ELECTRÒNIC

I. Els comptes de correu electrònic es creen amb propòsits de desenvolupament acadèmic i/o professional.

II. Els missatges haurien de ser exactes, correctes i necessaris.

III. No s'haurien d'enviar missatges de forma indiscriminada, si no és per causa justificada, i especialment si porten documents adjunts.

IV. La proliferació de missatges produeix molèsties innecessàries als membres de la comunitat universitària, ja que incrementa el nombre d'entrades, exigeix l'esforç de triar els missatges i invita a llençar a la paperera tots els que a primera vista no es consideren importants, la qual cosa comporta que de vegades la tria no és precisa i s'eliminen missatges que poden ser realment importants.

V. No s'hauria de deixar el correu electrònic obert i desatès, especialment si no es té instal·lat un protector de pantalla amb contrasenya.

VI. En rebre un missatge d'una adreça particular coneguda però amb un estil diferent de l'habitual, cal tractar-lo com a correu il·legítim, excepte que es tingui la possibilitat de verificar que no ho és.

VII. Cal tenir molta cura a l'hora d'escriure una adreça de correu electrònic per tal d'evitar trameses a destinataris equivocats, especialment si és la primera vegada que s'utilitza l'adreça. Si s'ha de respondre un correu rebut, sempre és millor utilitzar l'opció "Respon".

VIII. En el camp "assumpte" és millor escriure una frase que sigui significativa i que aporti informació sobre el text del missatge.

IX. És recomanable signar el missatge amb el nom i, si s'escau, el càrrec de la persona que l'envia. S'han d'evitar les signatures genèriques.

X. L'opció de rebre un missatge de confirmació quan el correu s'hagi rebut només s'hauria d'utilitzar quan fos estrictament necessari.

XI. No s'hauria d'enviar per correu electrònic material que no s'enviaria en un sobre obert, llevat que aquest viatgi a través d'un sistema xifrat (segur).

XII. Cal evitar deixar correus electrònics desatesos en impressores compartides o oblidats en qualsevol altre lloc, especialment si contenen informació confidencial.

XIII. Cal fer especial atenció a la tramesa de documents. En alguns casos poden enviar-se en formats estàndards i oberts (com per exemple, PDF, RTF, ODT, etc.) menys dependents del versionat d'aplicacions i més interoperables, amb més possibilitat de ser llegits en qualsevol versió d'editors/visors de text/documents (com per exemple, Word o OpenOffice).

XIV. Abans d'obrir els documents adjunts, cal comprovar que són fiables independentment de l'extensió que tinguin associada (com per exemple .doc, .xls) i no fitxers que puguin tenir virus. És important instal·lar un antivirus de confiança, mantenir-lo actualitzat i aplicar el procés de verificació sobre els fitxers adjunts rebuts abans de treballar-hi.

XV. Un ús negligent del correu electrònic pot donar lloc al coneixement, per part de persones indegudes, de dades mèdiques, dades personals i professionals confidencials, informació mercantil sensible, exàmens, informes d'avaluadors externs, qualificacions, etc. Enviar dades d'aquest tipus a través de correu electrònic us exposa, juntament amb la URV, a aquest risc.

XVI. En els reenviaments cal protegir la intimitat de l'emissor i no difondre'n aspectes personals inclosos en el missatge.

XVII. Un missatge electrònic pot ser considerat com a prova escrita en un procés jurídic i pot ser requerit a instàncies del jutjat corresponent. Per tant, es recomana guardar-lo en una carpeta de forma que no pugui eliminar-se accidentalment.

3. PARTICIPACIÓ EN CANALS WEB

I. Reflexionar abans de publicar

Cal pensar en les reaccions a la publicació abans de publicar el contingut. Tot el que s'escriu pot viure durant molts anys als diferents canals d'Internet, fins i tot després d'eliminar aquest contingut del canal en què hagi estat publicat.

II. Respectar els altres

S'han d'evitar insults, atacs personals, difamacions, obscenitats i altres, així com temes que es poden considerar inacceptables o incorrectes, i cal mostrar la deguda consideració per la vida privada d'altres persones.

III. No "regalar actius"

S'ha d'evitar publicar informació que formi part dels actius de la URV. Quan es participa en converses web sobre temes de productes, serveis o línies estratègiques rellevants de la URV, s'ha d'anar amb compte amb l'intercanvi d'informació i opinions i no s'ha de divulgar informació no necessària.

IV. Protegir i millorar el valor de la marca URV

És important presentar la URV des d'una visió positiva i cal evitar fer comentaris despectius sobre la URV, els seus serveis, productes, gestió, empleats o sistemes. Per minimitzar el risc que els missatges personals siguin percebuts com una postura oficial de la URV, és millor deixar clar que s'està parlant a títol personal i no en nom de la URV.

V. Protegir la informació confidencial

Cal protegir la informació confidencial de la URV i dels seus clients i associats. La informació que no es revelaria públicament mitjançant altres canals, per qüestions de confidencialitat, no ha de ser divulgada o discutida a la web. En cas de dubte, cal consultar abans de publicar. S'han de respectar els drets d'autor, l'ús just i la legalitat.

VI. Fer un ús adequat

La participació en canals d'Internet és per manifestar-se a títol personal, però no institucional. Cal que la persona s'identifiqui sempre, escrigui en primera persona i usi el registre adequat a cada situació.

4. CERTIFICACIÓ DIGITAL

Les claus públiques de les entitats de certificació són necessàries per verificar que els certificats que arriben als equips informàtics de la URV han estat emesos per alguna de les autoritats de certificació de la jerarquia d'entitats de CATCert.

Els navegadors porten incorporada per defecte la confiança en algunes entitats de certificació. Si es vol comprovar quines són aquestes entitats, s'han d'executar les opcions següents als diferents navegadors:

- Microsoft Internet Explorer: Menú Eines > opció Opcions d'Internet > pestanya Contingut > botó Certificats -> pestanya Entitats emissores de certificats arrel de confiança.
- Mozilla Firefox: Menú Eines -> opció Opcions... -> secció Avançat, pestanya Xifratge, botó Visualitza els certificats, pestanya Entitats.

Posteriorment, és necessari instal·lar les claus de les tres entitats de certificació que formen la branca a què pertany l'entitat certificadora de la URV. Es poden descarregar des dels enllaços següents:

- Arrel de l'Agència Catalana de Certificació (CATCert)
- Entitat de Certificació d'Universitats i Recerca
- Entitat de Certificació de la URV. Dues claus: 2005-2013 i 2009-2019 (és necessari instal·lar les dues claus)

5. CÒPIES DE SEGURETAT

La URV posa a disposició dels membres de la comunitat d'usuaris de TIC el servei d'espai personal. Aquest servei permet l'emmagatzemament d'arxius en un espai corporatiu de la URV, amb còpia de seguretat diària i adequada a la normativa legal vigent. El servei es dóna de forma que des de qualsevol ordinador connectat a la intranet de la URV es pugui treballar amb aquests arxius.

Aquest servei consta de dos elements diferenciats: d'una banda, una sèrie de servidors connectats a una bateria de discos on els usuaris emmagatzemen els seus fitxers, i d'altra banda, un robot de cintes on es fan periòdicament còpies de seguretat de la informació emmagatzemada.

Per tal d'assegurar que la informació rellevant està convenientment assegurada, és recomanable fer una còpia o treballar directament sobre els espais de xarxa personal i comú, atès que aquests estan inclosos en els mecanismes abans descrits i permeten assegurar una còpia diària de tota la informació emmagatzemada.

6. ÚS DEL MAQUINARI

Per tal d'estalviar energia, és recomanable que en marxar del lloc de treball s'apaguin els elements del maquinari utilitzats: ordinador, impressora, escàner, etc.

ANNEX II

ALTRES SERVEIS DE XARXA OFERTS ACTUALMENT

(accés a través de la intranet de la URV, apartat Serveis de xarxa)

Canvi de la contrasenya

Correu electrònic

Xarxa oberta

Servei FTP

Servei Proxy antivirus

Accés remot als recursos electrònics

Antivirus

Llistes de distribució

Programari antiespies

Espai col·laboratiu

Certificació digital

Agenda corporativa

Servei d'espai personal i comú

Fòrums corporatius

ANNEX III

GLOSSARI

Antivirus

Un programa antivirus és un programa informàtic que intenta identificar, desactivar i eliminar virus informàtics i altre programari maliciós (malware).

Autoritat de certificació (AC)

Una autoritat de certificació és un sistema informàtic dedicat a l'emissió i gestió posterior de certificats digitals, incloent-hi la renovació, l'expiració, la suspensió, l'habilitació i la revocació de certificats, a petició de l'autoritat de registre. L'emissió de certificats es fa d'una forma automatitzada i sempre amb la prèvia confirmació de l'autoritat local de registre.

Bot

Abreviatura del terme anglès robot. Es tracta d'un programa informàtic amb capacitat per realitzar tasques diverses imitant el comportament humà.

Certificat digital

Un certificat digital és un document electrònic signat per una autoritat de certificació que garanteix a les terceres persones que el rebin o l'utilitzin una sèrie de manifestacions que s'hi contenen, com per exemple la identitat de la persona, les autoritzacions, la seva capacitat per realitzar un determinat acte, etc. El certificat digital permet a les parts tenir confiança en les transaccions a Internet, ja que garanteix la identitat del seu posseïdor a Internet mitjançant un sistema segur de claus administrat per una tercera part de confiança, l'autoritat de certificació. El certificat permet realitzar un conjunt d'accions de forma segura i amb validesa legal: signar documents, entrar a llocs restringits, identificar-se davant l'Administració, etc.

Clau privada del certificat digital de la URV

La clau privada del certificat digital de la URV serveix per signar documents electrònics. És l'element secret del certificat. Es troba relacionat, mitjançant procediments matemàtics, amb un altre element (clau pública). La clau privada es guarda en la targeta intel·ligent de la persona certificada i, per tant, té totes les garanties de seguretat. Serveix, bàsicament, per desxifrar els missatges rebuts, tot i que també es fa servir per crear la firma digital.

Clau pública del certificat digital de la URV

La clau pública del certificat digital de la URV és necessària per comprovar la identitat de l'emissor o l'autenticitat d'un document signat. Permet validar una signatura que hagi estat generada amb la clau privada complementària. La clau pública es l'únic element del certificat digital que es troba a l'abast de tothom. Les claus públiques estan disponibles en directoris publicats a Internet i en algun cas en bases de dades corporatives. Es relaciona, mitjançant procediments matemàtics, amb un altre element (clau privada) per garantir la seva confidencialitat i integritat. La clau pública serveix bàsicament per xifrar, tot i que també es fa servir per verificar signatures digitals.

Qualsevol persona pot xifrar un missatge fent servir la clau pública, però tan sols el posseïdor de la clau privada pot desxifrar-lo.

Cucs

En informàtica, un cuc o worm és un virus o programa autoreplicant (es multiplica per ell sol) que no altera els arxius, sinó que resideix en la memòria i es duplica a si mateix.

IMAP4/IMAP4S

Acrònim d'Internet Message Access Protocol versió 4. Es tracta d'un protocol per a la lectura de missatges de correu electrònic, caracteritzat perquè els missatges no es mouen del servidor al client de correu electrònic. L'acrònim IMAP4S respon a la versió del protocol que empra seguretat aplicant xifratge a la capa de transport entre el client i el servidor.

Malware

La paraula malware (en català, programa maliciós) prové d'una agrupació de les paraules en anglès malicious software. Aquest programari o arxiu, que és nociu per a l'ordinador, està dissenyat per inserir virus, cucs, troians, programes espia o fins i tot bots, intentant aconseguir algun objectiu, com ara recollir informació sobre l'usuari o sobre l'ordinador.

Pirateria

Ús no autoritzat o prohibit d'un contingut o programari, d'acord amb la seva llicència d'ús, distribució i reproducció i amb la legislació vigent.

POP3/POP3S

Acrònim de Post Office Protocol versió 3. Es tracta d'un protocol per a la recepció i lectura de missatges de correu electrònic, caracteritzat perquè els missatges es mouen del servidor al client de correu electrònic. L'acrònim POP3S respon a la versió del protocol que empra seguretat aplicant xifratge a la capa de transport entre el client i el servidor.

Programari

El programari (software, en anglès) és un terme general emprat per descriure el conjunt dels programes informàtics, procediments i documentació que duen a terme alguna tasca en un ordinador.

Revocació

Anul·lació definitiva d'un certificat digital, bé a demanda del subscriptor, bé per pròpia iniciativa de l'autoritat de certificació en cas de dubte sobre la seguretat de les claus.

Signatura electrònica

La signatura digital és la part del certificat digital que permet a l'emissor garantir la seva identitat en l'enviament de les dades electròniques. La signatura digital es basa en la confiança que dóna la infraestructura de clau pública i privada.

La signatura digital fa ús de les funcions resum (hash) per accelerar el procés de xifratge i per garantir la confidencialitat i integritat de la informació. La Llei 59/2003, de signatura electrònica reconeix tres tipus de signatura electrònica, en funció del certificat digital que la genera: signatura ordinària, signatura avançada i signatura reconeguda, aquesta última equiparada a la signatura manuscrita.

SMTP

Acrònim de Simple Mail Transfer Protocol. Es tracta d'un protocol per a l'enviament de missatges de correu electrònic, emprat per a l'enviament entre els clients i el servidor de correu electrònic, o per a l'intercanvi de correus electrònics entre servidors.

Spyware

Els programes espia o spyware són aplicacions (programes informàtics) que recopilen informació sobre una persona o una organització sense que aquesta ho sàpiga. Un programa espia pot recol·lectar molts tipus diferents d'informació d'un usuari.

Troians

Un troià informàtic o cavall de Troia (traducció més fidel de l'anglès Trojan horse encara que no tan utilitzada) és un programa nociu amb aparença de programari legítim que permet l'accés a usuaris externs, a través d'una xarxa d'àrea local o d'Internet, amb la finalitat de recaptar informació o controlar remotament la màquina amfitriona, però sense afectar-ne el funcionament.

Virus informàtic

Un virus informàtic és un programa que es copia automàticament per alterar el funcionament normal de l'ordinador, sense el permís o el coneixement de l'usuari.

Xifratge

És el procés que s'aplica a unes dades per tal de fer-les incomprensibles i evitar que siguin espiades. D'aquesta manera és possible assegurar la confidencialitat de les dades, perquè només les pot fer comprensibles un receptor que tingui una clau per desxifrar-les. Únicament aplicant el procés contrari, denominat desxifratge, a les dades xifrades és possible regenerar les dades originals (i, per tant, fer-les de nou comprensibles).