ÍNDEX

1. OBJECTIU

La present normativa ha estat aprovada pel Consell d'Administració d'aquesta empresa en data 13 de juny de 2024 i entrarà en vigor l'endemà de la seva aprovació, fins que sigui reemplaçada per una modificació o una nova normativa.

2. REVISIÓ I/O ACTUALITZACIÓ

Amb periodicitat anual se'n revisarà el contingut i en cas que sigui necessari es procedirà a la seva modificació, que haurà de ser aprovada pels òrgans anteriorment indicats, i hauran de ser difoses entre les persones afectades per aquestes.

3. OBJECTE

L'objecte del present document és establir la normativa d'ús segur dels mitjans electrònics a SMAP, dins de l'abast assenyalat a l'Esquema Nacional de Seguretat.

Els sistemes d'informació són elements bàsics per al desenvolupament de l'activitat de SMAP. Aquests mitjans es posen a disposició de les persones usuàries com a instruments de treball per a l'exercici de la seva activitat professional. Motiu pel qual cal utilitzar aquests recursos de manera responsable, mitjançant el seguiment de normes, i bones pràctiques que salvaguardin la seguretat de la informació, els sistemes d'informació i els recursos tecnològics proporcionats per l'entitat.

4. ABAST

Mitjançant aquesta normativa, l'SMAP estableix la regulació de l'ús dels mitjans electrònics del sistema d'informació (inclòs l'accés remot a aquests), a través de l'establiment de mesures de compliment obligatori per a tot el personal, i queden subjectes a aquesta , així com als principis morals i ètics en la utilització dels recursos posats a disposició.

El personal de tercers (empreses proveïdores, convenis, etc.) amb accés al sistema queden també subjectes a aquesta, en la mesura que li siguin aplicables, així com als principis morals i ètics en la utilització dels recursos posats a disposició d'aquestes persones usuàries per a l'exercici de les seves activitats a SMAP.

D'ara endavant, s'utilitzarà "l'Usuari" per referir-se al personal propi o de tercers.

5. CANAL DE SOL·LICITUDS I/O NOTIFICACIONS

Les sol·licituds d'autorització i les notificacions reflectides en aquesta normativa s'adreçaran al departament d'informàtica (informatica@smap.palma.cat) qui serà el responsable d'acceptar-les, prèvia aprovació – si correspon- pel responsable del departament.

6. INCIDENTS DE SEGURETAT

Quan un Usuari detecti qualsevol anomalia (mal funcionament, aplicacions que no arrenquen o que es tanquen de manera inesperada, pèrdua de documents, de memòries USB, etc.) o incident de seguretat (virus, suplantació d'identitat, pèrdues de clau, etc.) que pugui comprometre el bon ús i funcionament dels Sistemes d'Informació de SMAP o pugui danyar la seva imatge, n'ha d'informar immediatament (informatica@smap.palma.cat).

7. NORMATIVA D'ÚS DELS MITJANS ELECTRÒNICS

7.1. NORMES D'UTILITZACIÓ DE L'EQUIPAMENT INFORMÀTIC I DE COMUNICACIONS

Qualsevol persona que precisi un nou suport haurà de remetre la sol·licitud al departament informàtic mitjançant correu electrònic (informatica@smap.palma.cat) indicant el motiu o necessitat. El responsable acceptarà, denegarà o remetrà al corresponent responsable per a la seva acceptació.

Aquestes normes concerneixen específicament a tots els dispositius facilitats i configurats per SMAP, incloent-hi equips de sobretaula, portàtils i dispositius mòbils amb capacitats d'accés als sistemes d'informació.

L'SMAP proporcionarà al personal, l'equipament degudament configurat amb accés als serveis i les aplicacions que siguin necessaris per a l'exercici de les seves funcions.

Pel que fa als quals aplicarà les normes generals i per als equips portàtils i dispositius mòbils aplicarà les normes específiques per a aquest tipus d'equipament.

7.1.1. NORMES GENERALS

Els equips s'han d'utilitzar únicament per a fins institucionals/professionals i com a eina per a l'exercici de les tasques encomanades. Cada equip estarà assignat a una única persona. Aquesta persona és responsable del seu ús correcte. Quan el treballador que fa ús del dispositiu abandona el seu lloc de feina, haurà de deixar el dispositiu bloquejat i en bones condicions.

Excepte autorització expressa, no es disposaran de privilegis d'administrador sobre els equips.

Únicament el personal autoritzat podrà distribuir, instal·lar o desinstal·lar programari i maquinari, o modificar la configuració de qualsevol dels equips.

Quan sigui necessari instal·lar equips que no hagin estat proveïts per SMAP, cal sol·licitar autorització prèvia.

Les persones usuàries hauran de notificar, al més aviat possible, qualsevol comportament anòmal dels seus equips (va lent, no arrenca, no funciona correctament, etc.), especialment quan hi hagi sospites que s'hi hagi produït algun incident de seguretat. De la mateixa manera haurà de comunicar l'absència de cables i/o accessoris o qualsevol altra evidència de deteriorament.

Amb caràcter general, no es permet l'ús de dispositius propis, "BYOD (Bring Your Own Device)", per a l'accés o l'emmagatzematge d'informació excepte autorització expressa.

No es pot fer ús dels dispositius en horari no laboral i fora de les instal·lacions o punt de feina propi de la persona treballadora, a excepció del personal que disposa de dispositius mòbils localitzables sense limitació horària.

Amb la finalitat de complir amb la normativa de protecció de dades i respecte als drets de tots els companys, no es permet l'enregistrament de les converses essent responsabilitat de cada treballador seguir les pautes indicades i qui haurà de respondre de les responsabilitats que es poden derivar.

7.1.2. NORMES ESPECÍFIQUES PER A EQUIPS PORTÀTILS I DISPOSITIUS MÒBILS

Per als portàtils i mòbils a més de les normes generals, són aplicables les següents:

- Aquests dispositius estaran, en tot moment sota la custòdia de la persona usuària que els utilitzi, que serà la responsable d'adoptar les mesures necessàries per evitar danys o sostracció, així com de l'accés per part de persones no autoritzades.
- La sostracció d'aquests equips s'ha de notificar immediatament per a l'adopció de les mesures que corresponguin.
- Cal sol·licitar autorització quan es facin servir per connectar-se remotament a través de xarxes que no estiguin sota el control de SMAP o que no hagin estat autoritzades, autorització que es farà extensible també als serveis als quals s'accedeix.
- Quan es modifiquin les circumstàncies professionals (terme d'una tasca, cessament en el càrrec, etc.) que van originar el lliurament d'un recurs informàtic mòbil, la persona usuària el tornarà, a fi de procedir a l'esborrament segur de la informació emmagatzemada i restaurar el equip al seu estat original perquè pugui ser assignat a una persona nova.

7.2. NORMES PER A L'EMMAGATZEMATGE D'INFORMACIÓ I CÒPIES DE SEGURETAT

Per a garantir la disponibilitat de la informació davant d'un incident de seguretat, de forma periòdica es fan còpies de seguretat de les carpetes del servidor propi de l'SMAP (NAS).

Per aquest motiu, els Usuaris hauran d'emmagatzemar en aquestes les dades generades a l'exercici de les seves competències professionals. Respecte d'això, s'informa que no es fan còpies de seguretat de la informació que no es trobi a les unitats indicades.

No es permet l'emmagatzematge d'informació privada ni de tercers aliens als recursos indicats.

La informació emmagatzemada a les còpies de seguretat podrà ser recuperada en cas que es produeixi algun incident de seguretat. Per recuperar aquesta informació caldrà adreçar una sol·licitud de restauració.

7.3. NORMES D'ÚS PER A SUPORTS D'EMMAGATZEMATGE EXTRAÏBLES

Com a norma general, a l'SMAP l'ús de suports o mitjans d'emmagatzematge extraïbles (memòries USB, discos durs, etc.) no està autoritzat. Per utilitzar-los s'haurà de comptar amb la deguda autorització del departament d'informàtica.

En el cas que a la persona usuària se li autoritzi l'ús d'aquest tipus de suports de treball, les normes a observar són les següents:

- Com a norma general, es faran servir els suports extraïbles proporcionats per l'SMAP. Estant destinats a un ús exclusivament professional, com a eina de transport puntual de fitxers, no com a eina d'emmagatzematge. En aquests suports cal que s'apliquin mesures de seguretat (contrasenya, encriptació....) per evitar accessos de tercers no autoritzats.
- L'ús de mitjans d'emmagatzematge extraïbles particulars no està autoritzat, llevat que es disposi de l'autorització deguda.
- El seu ús no està autoritzat per a l'emmagatzematge de dades personals, llevat que es disposi de l'autorització deguda.

Aquest tipus de dispositius s'hauran d'emmagatzemar en llocs segurs, per prevenir robatoris o l'accés de tercers no autoritzats. La pèrdua o la sostracció d'aquests dispositius, amb indicació del contingut, s'ha de posar en coneixement, de manera immediata.

El transport d'aquests suports fora de les instal·lacions de SMAP l'ha de fer exclusivament personal autoritzat, autorització que contempla igualment la informació que en surt. En aquest cas caldrà enviar una sol·licitud perquè se us assessori sobre les mesures de seguretat que caldrà implementar.

7.3.1. NORMES PER A L'ESBORRAMENT I ELIMINACIÓ DE SUPORTS INFORMÀTICS

Els mitjans d'emmagatzematge que, per obsolescència o degradació, perdin la utilitat, i especialment aquells que continguin dades de caràcter personal, s'han d'eliminar de manera segura per evitar accessos a aquesta informació. En aquest sentit, la persona usuària haurà de tenir en compte les indicacions següents:

- Assegureu-vos que el contingut del suport pot ser eliminat.
- Qualsevol petició d'eliminació de suport informàtic s'haurà de sol·licitar.

Per a la reutilització de mitjans d'emmagatzematge, per a altres fins diferents dels que en van originar l'ús, s'ha de sol·licitar un esborrat segur.

7.4. NORMES RESPECTE A LA GESTIÓ DE DOCUMENTS

7.4.1. IMPRESSORES EN XARXA, FOTOCOPIADORES/ESCÀNERS

Amb caràcter general, s'han d'utilitzar les impressores en xarxa i les fotocopiadores corporatives. Excepcionalment, es poden instal·lar impressores locals, gestionades per un lloc de treball d'usuari. En aquest cas, la instal·lació anirà precedida de l'autorització pertinent.

En cap cas es podrà fer ús d'impressores, fotocopiadores que SMAP no hagi proporcionat. En relació als sistemes de còpia i impressió i documentació impresa, els Usuaris han de seguir les directrius següents:

- Els documents, amb caràcter general, es generaran en format electrònic, podent digitalitzar aquells que no siguin susceptibles de ser generats en aquest format.
- Quan s'imprimeixin documents, en sistemes d'impressió o còpia comuns, aquests han de romandre el menor temps possible a les safates de sortida de les impressores, per evitar que terceres persones puguin accedir-hi.
- En la realització de còpies de documents i/o escaneig, cal no oblidar retirar els originals.
- En cas de trobar-se documentació en un sistema de còpia o impressió, l'Usuari intentarà localitzar la persona propietària perquè procedeixi a la recollida immediata. En cas de desconèixer la persona propietària o no estar localitzable, ho posarà immediatament en coneixement.
- Per evitar un ús excessiu dels recursos, millorant l'impacte mediambiental en la generació de documents en paper, i per motius de seguretat, abans d'imprimir documents, l'Usuari s'ha d'assegurar que cal fer-ho absolutament.

7.4.2. CURA I PROTECCIÓ DE LA DOCUMENTACIÓ IMPRESA

La documentació ha de ser protegida, de manera que només hi tingui accés el personal autoritzat, a aquest efecte la persona usuària tindrà en compte les mesures següents:

- Els llocs de treball romandran clars, sense més material damunt la taula que el requerit per a l'activitat que s'està realitzant en cada moment.
- Quan no sigui utilitzada s'haurà de guardar en sistemes d'emmagatzematge (armaris o arxivadors) preferentment amb clau. No podran ser publicats a taulers o similars.
- Quan els documents no siguin necessaris, han de ser eliminats utilitzant els mitjans posats a disposició per part de l'entitat (destructora de documents), de manera que no sigui recuperable la informació que puguin contenir.
- Abans d'abandonar les sales de reunions o permetre que algú aliè hi accedeixi, es netejaran adequadament les pissarres i es recolliran tots els documents, tenint cura que no quedi cap tipus d'informació "sensible" o "interna" accessible a persones no autoritzades .

7.5. LLOC DE TREBALL NEGRE

Els llocs de treball han de romandre clars, sense més material sobre la taula que el requerit per a l'activitat que s'està fent a cada moment.

7.6. ACCÉS ALS SISTEMES D'INFORMACIÓ I A LES DADES TRACTADES

Per accedir als sistemes i recursos informàtics cal tenir assignat prèviament un compte d'usuari. L'alta dels usuaris serà sol·licitada i autoritzada segons les polítiques de SMAP. L'autorització de l'accés establirà el perfil necessari amb què es configurin les funcionalitats i els privilegis disponibles a les aplicacions segons les competències de cada persona, adoptant una política d'assignació de privilegis mínims necessaris per a la realització de les funcions encomanades.

Els Usuaris disposaran de credencials personals d'accés (codi d'usuari i una contrasenya, certificat electrònic, etc.) per a l'accés als sistemes d'informació de SMAP emprant la xarxa segura, protegida amb els serveis de seguretat destinats a aquest efecte. Responsables de la seva custòdia i de tota activitat relacionada amb l'ús del seu accés autoritzat, respecte dels quals haurà d'observar les mesures següents:

- El codi d'usuari és únic per a cada persona, intransferible i independent del PC o terminal des del qual es realitza l'accés.
- Els usuaris no han de revelar o lliurar, sota cap concepte, les credencials d'accés a una altra persona, ni mantenir-les per escrit a la vista o a l'abast de tercers. De la mateixa manera, no han d'utilitzar cap accés autoritzat d'una altra persona, encara que disposin de l'autorització del seu titular.
- Si una persona té sospites que les seves credencials estan sent utilitzades per una altra persona, ho ha de comunicar immediatament.
- Les persones usuàries han d'utilitzar contrasenyes segures, d'acord amb la política establerta a SMAP, no han d'estar compostes únicament per paraules del diccionari o d'altres fàcilment predictibles o associables a la persona usuària (noms de la família, adreces, matrícules de cotxe, telèfons , noms de productes comercials o organitzacions, identificadors d'usuari, de grup o del sistema, DNI, etc.).
- Els sistemes que així ho permetin, forçaran el canvi de la contrasenya almenys una vegada a l'any, previ avís amb els dies d'antelació suficients. En els que no sigui possible, serà responsabilitat dels Usuaris procedir al canvi amb aquesta periodicitat.

7.7. ACCÉS A UN COMPTE D'UN USUARI EN LA SEVA ABSÈNCIA O BAIXA

Quan sigui necessari accedir a la carpeta personal o compte de correu corporatiu d'un Usuari, aquest accés s'haurà de fer comptant amb l'autorització del responsable o per la persona en què aquesta delegui.

En cas que no resulti possible demanar aquesta autorització (mort, malaltia, impossibilitat de localització, etc.), l'accés podrà ser realitzat sempre que estigui autoritzat de forma expressa pel responsable del mateix o per la persona en què aquesta delegui.

En ambdós casos, s'haurà de motivar la necessitat d'accés i ser comunicada al responsable de l'Usuari, que elaborarà una acta en què es recullin totes les accions dutes a terme.

7.8. CONFIDENCIALITAT, PROTECCIÓ DE DADES PERSONALS I DEURE DE SECRET

La informació continguda al Sistema d'Informació de SMAP és responsabilitat d'aquesta entitat, per la qual cosa les persones usuàries han d'abstenir-se de comunicar, divulgar, distribuir o posar en coneixement o a l'abast de tercers (externs o interns no autoritzats) aquesta informació, excepte autorització expressa de la pròpia Institució. A més, haurà de tenir en compte les premisses següents:

- Tots els Usuaris, que per raó de la seva activitat professional hagin tingut accés a informació gestionada per SMAP (documents, metodologies, claus, anàlisis, programes, etc.) hauran de mantenir-hi, per temps indefinit, una reserva absoluta.
- Els Usuaris només podran accedir amb les degudes autoritzacions a aquella informació necessària per a l'exercici de les seves tasques. En tot cas, no s'ha d'accedir a informació sense les autoritzacions degudes.
- Tota informació continguda en els sistemes d'informació de SMAP o que circuli per les xarxes de comunicacions s'ha d'utilitzar únicament per al compliment de les funcions que té encomanades l'Usuari.
- Els drets d'accés dels usuaris a la informació i als sistemes d'informació que la tracten sempre s'hauran d'atorgar en base als principis de "mínim privilegi", "necessitat de conèixer i responsabilitat de compartir" i "capacitat d'autoritzar".
- La informació que comprengui dades de caràcter personal quedarà afectada també per la normativa vigent en matèria de Protecció de Dades Personals, estant obligat a guardar secret sobre aquestes, deure que es mantindrà de manera indefinida, fins i tot més enllà de la relació laboral o professional amb SMAP.

7.9. NETEJA DE METADADES I DADES OCULTES DELS DOCUMENTS ELECTRÒNICS

Es defineix metadada com a informació estructurada que descriu, explica, localitza i, a més, fa més fàcil recuperar, utilitzar o gestionar un recurs d'informació. Les metadades són comunament anomenades "dades sobre les dades" o "informació sobre la informació".

Es defineix informació o dades ocultes com aquelles dades existents en el contingut dels documents electrònics, que no són visibles amb la configuració estàndard o configuració per defecte dels programes utilitzats per a la seva creació i tractament, i cal aplicar alguna opció específica dins de la configuració d'aquests programes, per visualitzar-los. Un exemple de

dades ocultes és el text ocult, files o columnes ocultes, comentaris o informació del document, etc.

Quan fem una fotografia o creem documents amb aplicacions de Microsoft Office (Word, Excel, PowerPoint, etc.) i/o fotografies, aquests arxius porten integrats a les seves propietats una sèrie de dades ocultes i/o metadades, com poden ser el nom de la persona que ha creat el document, el programa amb què s'ha generat, la data de creació, la de modificació, etc. Això pot perjudicar la confidencialitat de la informació i la bona imatge de l'entitat.

Tots els arxius electrònics (documents ofimàtics, fulls de càlcul, imatges, etc…) poden tenir integrats a les seves propietats una sèrie de dades ocultes i/o metadades, com poden ser el nom de la persona que ha creat el document, el programa amb el que s'ha generat, la data de creació, la de modificació, etc.

Les metadades contingudes als fitxers poden arribar a afectar tant la seguretat de la informació com la imatge de SMAP. Per això, tot arxiu que hagi de ser difós internament, remès electrònicament a un tercer o publicat a Internet (pàgina web, seu electrònica, etc…), haurà de ser revisat per determinar les metadades associades a aquest, procedint a la seva modificació o supressió, per a assegurar que no consten dades personals o confidencials.

7.10. ÚS DEL CORREU ELECTRÒNIC CORPORATIU

El correu electrònic corporatiu és una eina de missatgeria electrònica centralitzada, posada a disposició dels usuaris del sistema d'informació de SMAP per a l'enviament i la recepció de correus electrònics mitjançant l'ús de comptes de correu corporatius. Com que es tracta d'un recurs compartit, un ús indegut del mateix repercuteix de manera directa en el servei ofert a totes les persones.

El correu electrònic s'haurà d'emprar en base al sentit comú i tenint en compte la responsabilitat i funcions exercides, tractant en qualsevol cas de no posar en compromís ni els sistemes ni la imatge de SMAP.

SMAP queda facultada per filtrar el contingut del correu electrònic del compte de correu proporcionat per al desenvolupament de les seves funcions laborals, a fi de prevenir virus o en cas que hi hagi raons fonamentades en una ferma sospita per SMAP sobre l'existència activitats delictives o doloses del personal.

El sistema que proporciona el servei de correu electrònic podrà, de forma automatitzada, rebutjar, bloquejar o eliminar part del contingut dels missatges enviats o rebuts en què es detecti algun problema de seguretat o d'incompliment d'aquesta Normativa.

Es podrà inserir contingut addicional als missatges enviats a fi d'advertir els receptors dels requisits legals i de seguretat que hauran de complir en relació amb aquests correus.

Les característiques peculiars d'aquest mitjà de comunicació (universalitat, baix cost, anonimat, etc.) han propiciat l'aparició d'amenaces que utilitzen el correu electrònic per a propagar-se o aprofitar-ne les vulnerabilitats. Per aquest motiu, s'estableixen les directrius següents amb l'objectiu de reduir el risc en l'ús del correu electrònic:

- Utilitzar el correu electrònic exclusivament per a propòsits professionals.

- No s'ha de cedir l'ús del compte de correu a terceres persones.
- Informar de correus amb virus, phishing, malware (programa maligne), etc. sense reenviar-los, per evitar-ne la possible propagació.
- No respondre a missatges de Spam.
- Assegurar la identitat del remitent abans d'obrir un missatge.
- No executeu fitxers adjunts sospitosos. No s'han d'executar els fitxers adjunts rebuts sense analitzar-los prèviament amb l'eina corporativa contra codi maliciós.

Pel que fa a l'ús del correu electrònic, queda terminantment prohibit:

- Falsificar, amagar, suprimir o substituir la identitat de l'emissor a qualsevol correu electrònic.
- Llegir o accedir a correus electrònics aliens, sense autorització prèvia.
- Enviar correus electrònics que continguin al cos o als adjunts informació amb dades de categories especials de dades o dades especialment sensibles (és a dir, salut, ideologia, religió, creences, origen racial, ètnic, etc.) o aquells considerats com d'especial protecció per SMAP, llevat que es compti amb l'autorització pertinent i s'hagin aplicat les mesures de seguretat oportunes (xifrat o similars).

7.11. ACCÉS A INTERNET I ALTRES EINES DE COL·LABORACIÓ

L'accés corporatiu a Internet és un recurs centralitzat que SMAP posa a disposició dels Usuaris, com a eina necessària per accedir a continguts i recursos d'Internet i com a suport a l'exercici de la seva activitat professional. SMAP vetllarà pel bon ús de l'accés a Internet, tant des del punt de vista de l'eficiència i la productivitat del personal, com des dels riscos de seguretat associats al seu ús. Les normes d'ús són les següents:

- Com a norma general, les connexions que es facin a Internet han d'obeir a fins professionals.
- Només es podrà accedir a Internet mitjançant els navegadors subministrats i configurats als llocs d'usuari. No es podrà alterar la configuració, ni utilitzar un navegador alternatiu, sense comptar amb la deguda autorització.
- El sistema que proporciona el servei de navegació podrà comptar amb filtres d'accés que bloquegin l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva o pàgines potencialment insegures o que continguin virus o codi nociu.
- S'haurà de notificar qualsevol anomalia (redirecció a pàgines sol·licitades, avís de lloc no segur, en pàgines habitualment utilitzades, etc.) detectada en l'ús de l'accés a Internet, així com la sospita de possibles problemes o incidents de seguretat relacionats amb aquest accés.

Es consideren usos prohibits, que impliquen un risc de seguretat, les actuacions següents:

- La descàrrega de programes informàtics sense l'autorització prèvia o fitxers amb contingut nociu que suposin una font de riscos per a SMAP. En tot cas, assegureu-vos que el lloc web visitat és fiable.

- L'accés, la descàrrega i/o l'emmagatzematge en qualsevol suport, de pàgines amb continguts il·legals, nocius, inadequats o que atemptin contra la moral i els bons costums i, en general, de tota mena de continguts que incompleixin les normes ètiques i de cortesia de SMAP.
- L'accés a recursos i pàgines web, o la descàrrega de programes o continguts que vulnerin la legislació en matèria de propietat intel·lectual.
- La utilització d'aplicacions o eines (especialment l'ús de programes d'intercanvi d'informació, P2P) per a la descàrrega massiva d'arxius, programes o altres tipus de contingut (música, pel·lícules, etc.) que no estiguin expressament autoritzats.

7.12. CONNEXIÓ REMOTA

Només es poden fer connexions remotes, sempre i quan es disposi de la corresponent autorització del responsable del departament, prèvia ponderació de la necessitat d'aquests accessos.

Els accessos remots caldrà que es realitzin garantint que la connexió és segura i compleix amb els paràmetres establerts en aquesta norma. No es podrà realitzar utilitzant connexions wifi públiques o no segures.

Caldrà que, en el cas de que es permeti el teletreball, disposar de la corresponent autorització de l'IMI mitjançant els protocols establerts. L'IMI facilitarà una VPN i certificat de seguretat que s'ha de descarregar tot usuari que vulgui connectar-se remotament al seu lloc de feina. La responsabilitat de disposar d'un equip amb les característiques mínimes que requereix l'IMI, així com de la cura i l'actualització del mateix és del propi usuari. També cal destacar que és l'usuari qui ha de tenir cura de la protecció de l'equip i de la protecció de dades que implica.

Si en la prestació del serveis, implica la connexió a un suport o equip d'un altre company, caldrà la seva petició prèvia per tal de solucionar aquesta incidència sense que es pugui accedir a aquells espais o carpetes que no es precisi per la resolució de la incidència. Com a norma general, està prohibit activar la càmera o micròfon del suport on es connecta amb l'excepció que es tracti de revisar aquest recurs de càmera i micròfon. En qualsevol cas, abans de la seva activació caldrà informar de forma expressa i clara per tal de ser comprensible per a l'usuari.

El departament d'informàtica podrà realitzar tasques de manteniment i actualització dels sistemes de forma remota, accedint als suports, carpetes i aplicacions que sigui necessari per a la realització de les tasques professionals assignades.

7.13. DRETS DE PROPIETAT INTEL·LECTUAL

Els usuaris i administradors han de respectar les condicions de llicència i copyright del software que usin en els seus equips. Tot software adquirit de forma central per SMAP haurà d'estar degudament llicenciat.

Es limita el nombre d'usuaris que poden ostentar la condició d'administrador del sistema i per tant, amb capacitat per instal·lar software, qui haurà de respectar els drets de propietat intel·lectual de qualsevol aplicació i/o software a aplicar.

8. MONITORITZACIÓ I APLICACIÓ D'AQUESTA NORMATIVA

L'SMAP per motius legals, de seguretat i de qualitat del servei, i complint en tot moment els requisits que a aquest efecte estableix la legislació vigent:

- Revisarà periòdicament l'estat dels equips, el programari instal·lat, els dispositius i les xarxes de comunicacions de la seva responsabilitat.
- Monitoritzarà els accessos a la informació continguda als seus sistemes.
- Auditarà la seguretat de les credencials i aplicacions.
- Monitoritzareu els serveis d'Internet, correu electrònic i altres eines de col·laboració.

Aquesta supervisió es realitzarà en tot cas amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge dels afectats, i d'acord amb la normativa sobre protecció de dades personals, de funció pública o laboral i altres disposicions que resultin aplicables, es registraran les activitats dels Usuaris, retenint la informació necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar en cada moment la persona que actua.

Els sistemes en què es detecti un ús inadequat o en què no es compleixin els requisits mínims de seguretat, poden ser bloquejats o suspesos temporalment. El servei es restablirà quan la causa de la seva inseguretat o degradació desaparegui.

El sistema que proporciona el servei de correu electrònic podrà, de forma automatitzada, rebutjar, bloquejar o eliminar part del contingut dels missatges enviats o rebuts en què es detecti algun problema de seguretat o d'incompliment d'aquesta Normativa. Es podrà inserir contingut addicional als missatges enviats a fi d'advertir els receptors dels requisits legals i de seguretat que hauran de complir en relació amb aquests correus.

El sistema que proporciona el servei de navegació podrà comptar amb filtres d'accés que bloquegin l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva o pàgines potencialment insegures o que continguin virus o codi nociu. Igualment, el sistema podrà registrar i deixar traça de les pàgines a què s'ha accedit, així com del temps d'accés, volum i mida dels fitxers descarregats. El sistema permetrà l'establiment de controls que possibilitin detectar i notificar sobre usos prolongats i indeguts del servei.

9. INCOMPLIMENT DE LA NORMATIVA

Els Usuaris del sistema d'informació de SMAP estan obligats a complir el que prescriu aquesta "Normativa d'Ús de Mitjans Electrònics".

En cas que una persona usuària no observi alguna dels preceptes assenyalats en aquesta Normativa, sens perjudici de les accions disciplinàries i administratives que siguin procedents i, si escau, les responsabilitats legals corresponents, es podrà acordar la suspensió temporal o definitiva de l'ús dels recursos informàtics que tingui assignats, prèvia instrucció del procediment legal que correspongui.

En el cas de personal de tercers, l' incompliment d'aquesta normativa podria derivar en la imposició de penalitats podent arribar fins i tot a la resolució del contracte, seguint el procediment establert a aquest efecte a la normativa sobre contractació administrativa.