NORMATIVA D'ÚS DE MITJANS ELECTRÒNICS

ELABORACIÓ I APROVACIÓ DEL DOCUMENT

	DATA
ELABORAT PER Director de Sistemes d'Informació Responsable de Seguretat Responsable de Protecció de Dades *En base a la "Guia de Seguretat de les TIC CCN-STIC 890. Annex VI. Normativa d'Ús de Mitjans Electrònics"*	23/05/2023
APROVAT PER Comitè de Seguretat de la Informació	24/11/2025

DIFUSIÓ DEL DOCUMENT

PERSONES/ROLS	MITJÀ
Tots els usuaris amb clau d'accés pròpia del CSAPG	Procediment d'acollida de RH i/o correu electrònic a l'alta al Sistema d'Informació
Tots els usuaris amb clau d'accés pròpia del CSAPG	Minerva i Intranet

CONTROL DE VERSIONS

VERSIÓ	DATA	AUTOR	CANVIS
1.0	20/11/2023	Director de Sistemes d'Informació Responsable de Seguretat Responsable de Protecció de Dades	Versió inicial del document
1.1	28/11/2023	Responsable de Seguretat Responsable de Protecció de Dades	Es concreta punt 10.1
2.0	30/10/2025	Responsable de Seguretat Direcció de Sistemes d'Informació Responsable de Protecció de Dades Responsable del Sistema	Revisió general, simplificació i fusió amb la Instrucció 8/2020 de la Generalitat de Catalunya
2.1	24/11/2025	Comitè de Seguretat de la Informació	Aprovació

ÍNDEX

1. INTRODUCCIÓ

Aquesta Normativa, ha estat aprovada pel Comitè de Direcció de Seguretat de la Informació i serà vigent el dia següent de la seva aprovació fins que sigui reemplaçada per una modificació o una nova Normativa.

De forma complementària a l'establert en aquesta Normativa és d'aplicació l'establert a la "Instrucció 8/2020, de 24 de novembre, sobre l'ús de les tecnologies de la informació i la comunicació a l'administració de la Generalitat de Catalunya", a la qual el Consell Rector del Consorci Sanitari de l'Alt Penedès i Garraf es va adherir a data 16 de març de 2021.

Anualment el Grup Tècnic de Treball de Seguretat de la Informació revisarà el seu contingut i en cas de ser necessari es procedirà a la seva modificació, que haurà de ser aprovada pel Comitè de Direcció de Seguretat de la Informació, havent de ser difosa entre les persones afectades.

Tots els usuaris dels recursos informàtics i/o sistemes d'informació del CSAPG hauran d'acceptar la present normativa i hauran de tenir accés permanent a la mateixa durant el temps de desenvolupament de les seves funcions.

2. OBJECTE

L'objecte del present document és establir la normativa d'ús segur dels mitjans electrònics al Consorci Sanitari de l'Alt Penedès i Garraf (CSAPG) dins l'abast establert a l'Esquema Nacional de Seguretat, així com difondre els mitjans dels que disposa el CSAPG per vetllar pel seu ús correcte, control i seguiment.

Els sistemes d'informació són elements bàsics per al desenvolupament de l'activitat del CSAPG. Aquests mitjans es posen a disposició dels usuaris com a eines de treball pel desenvolupament de la seva tasca professional, motiu pel qual cal utilitzar aquests recursos de forma 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 pel CSAPG.

A més, aquesta normativa té com a finalitat protegir la informació del CSAPG, garantir el bon funcionament dels dispositius digitals i la gestió eficient de la infraestructura informàtica i de comunicacions, i assegurar el compliment de la legislació vigent en matèria de seguretat de la informació, propietat intel·lectual i protecció de dades de caràcter personal, així com qualsevol altra norma aplicable.

3. ABAST

Mitjançant aquesta Normativa, el CSAPG estableix la regulació de l'Ús dels Mitjans Electrònics del seu sistema d'informació, mitjançant l'establiment de mesures de compliment obligatori per a tot el personal, quedant-hi subjectes, així com als principis morals i ètics en la utilització dels recursos que es posen a disposició per al desenvolupament de les tasques i funcions assignades.

El personal de tercers (empreses proveïdores, convenis, etc.) amb accés al sistema també hi queden subjectes en la mesura que li siguin d'aplicació, així com als principis morals i ètics en la

utilització dels recursos posats a disposició dels usuaris per al desenvolupament de les seves activitats al CSAPG.

En endavant, s'utilitzarà "usuari" per referir-se tant al personal propi com de tercers.

4. COMUNICACIÓ DE SOL·LICITUDS, INCIDÈNCIES I INCIDENTS DE SEGURETAT

Totes les sol·licituds, notificacions i comunicacions relacionades amb l'ús dels sistemes d'informació s'han d'adreçar a cau@csapg.cat.

En cas de detectar qualsevol incidència tècnica o de seguretat (com ara mal funcionament d'aplicacions, temps de resposta excessivament lents, pèrdua de documents o dispositius amb informació, infeccions per virus, suplantacions d'identitat, etc.), l'usuari haurà de comunicar-ho el més aviat possible al mateix canal per tal que es puguin adoptar les mesures oportunes. D'igual manera, en cas de danys, robatori, furt o pèrdua de qualsevol dispositiu digital, haurà de notificar l'incident immediatament.

En cas d'**incidents greus** que puguin afectar el funcionament general dels Sistemes d'Informació del CSAPG o perjudicar la seva imatge, s'haurà de comunicar l'incident de manera immediata i prioritària a través del telèfon **6040**, a més del correu electrònic cau@csapg.cat, per tal d'activar amb la màxima celeritat els protocols interns de resposta i contenció, minimitzant així els possibles impactes sobre l'organització.

5. NORMATIVA D'ÚS DELS MITJANS ELECTRÒNICS

5.1. UTILITZACIÓ DE L'EQUIPAMENT INFORMÀTIC I DE COMUNICACIONS

Aquestes normes concerneixen específicament a tots els dispositius facilitats i configurats pel CSAPG, incloent equips de sobretaula, portàtils i dispositius mòbils amb capacitats d'accés als Sistemes d'Informació.

El CSAPG proporcionarà al personal l'equipament necessari degudament configurat amb accés als serveis i aplicacions que siguin adients per al desenvolupament de les seves funcions.

5.1.1. NORMES GENERALS

- Els diferents elements que configuren les TIC de cada àrea tenen la consideració d'eines de treball que el CSAPG posa a disposició del personal per a què les utilitzi únicament per al desenvolupament de les tasques i funcions encomanades, en la forma i les condicions que es preveuen en aquesta normativa.
- Per a les funcions d'emmagatzematge, col·laboració i treball en equip, comunicacions, processament de dades i accés a aplicacions, entre d'altres, el personal ha de fer ús dels espais digitals, les eines i els serveis que el CSAPG posa a la seva disposició.
- Excepte per autorització expressa, no es configuraran privilegis d'administrador en els equips.
- Només el personal autoritzat podrà distribuir, instal·lar o desinstal·lar software i hardware, modificar la configuració de qualsevol equip o reubicar-lo físicament. Els usuaris hauran d'abstenir-se d'alterar o modificar els dispositius digitals corporatius, el

sistema operatiu i les polítiques aplicades, el programari instal·lat i la seva configuració, en especial pel que fa a mecanismes de seguretat, o accedir físicament al seu interior per tal de manipular-los.

- Els usuaris hauran d'abstenir-se de fer ús dels equips informàtics assignats a altres usuaris sense el seu coneixement, llevat que el responsable de la unitat o del Departament de Sistemes d'Informació ho autoritzi.
- Caldrà autorització prèvia per instal·lar equips que no hagi proporcionat el CSAPG.
- Les persones usuàries hauran de notificar amb la major brevetat possible, qualsevol comportament anòmal dels equips (va lent, no arrenca, no funciona correctament, etc.), especialment quan hi hagi sospites de que s'hi hagi produït algun incident de seguretat. Així mateix, caldrà comunicar l'absència de cables i/o accessoris o qualsevol altre evidència del seu deteriorament.
- Els treballadors podran utilitzar els seus mitjans personals per a aquelles eines o aplicacions que es trobin accessibles des d'Internet. Per a les aplicacions i eines no obertes a Internet caldrà que utilitzin els dispositius digitals corporatius i/o eines informàtiques (com l'accés segur VPN) que el CSAPG posi a la seva disposició.
- En general, no està permès l'ús de dispositius propis, "BYOD (Bring Your Own Device)", per a l'accés o emmagatzematge d'informació en les instal·lacions del CSAPG, excepte autorització expressa. En cas que s'autoritzin dispositius de la propietat dels treballadors, resultarà d'aplicació la present normativa quan es tracti informació del CSAPG o quan s'utilitzin sistemes o serveis corporatius, exceptuant els casos coberts en el punt anterior.
- En cas d'ús habitual de dispositius digitals propis del personal, els responsables del Departament de Sistemes d'Informació i el Responsable de Seguretat de la Informació poden requerir modificar la configuració del dispositiu per garantir la seguretat i la privadesa, així com per facilitar l'accés als recursos corporatius.
- El personal podrà fer un ús privat de les diferents eines digitals corporatives sempre que es faci de manera excepcional, no abusiva (a criteri de la Direcció corresponent) i circumstancial als efectes d'atendre assumptes inexcusables o que facilitin la conciliació de la vida familiar i laboral.
- No es permet copiar, difondre, reproduir o obtenir d'alguna manera, totalment o parcialment, el programari instal·lat protegit per les lleis de propietat intel·lectual.

5.1.2. PORTÀTILS, DISPOSITIUS MÒBILS I RESTA D'EQUIPAMENT CEDIT

Per a portàtils, mòbils, tauletes i altres equips cedits sota la custòdia del treballador que es troben fora de les instal·lacions del CSAPG, a més de les normes generals, seran d'aplicació les següents:

- Aquests dispositius estaran en tot moment sota la custòdia de l'usuari que els utilitzi, que serà el responsable d'adoptar les mesures necessàries per evitar danys, robatoris o accessos per part de persones no autoritzades.
- La pèrdua, robatori o furt d'aquests equips s'haurà de notificar immediatament per a que el CSAPG pugui adoptar les mesures que corresponguin per protegir la informació del dispositiu digital, que podran incloure el seu esborrat remot, si escau.

- Cal sol·licitar autorització quan s'utilitzin per connectar-se remotament mitjançant xarxes que no estiguin sota el control del CSAPG o que no hagin estat autoritzades (autorització que es farà extensible també als serveis on s'accedeix).
- Quan es modifiquin les circumstàncies professionals (finalització d'una tasca, cessament al càrrec, etc.) que van originar el lliurement d'un recurs informàtic mòbil o cedit, l'usuari el retornarà i es procedirà a l'esborrat segur de la informació emmagatzemada i a restaurar l'equip al seu estat original per a que pugui assignar-se a una nova persona.

5.2. EMMAGATZEMATGE D'INFORMACIÓ I CÒPIES DE SEGURETAT

La informació s'ha d'emmagatzemar en les eines informàtiques o els serveis corporatius que el CSAPG posa a disposició dels usuaris. No està permès l'emmagatzemat d'informació privada ni de tercers als recursos indicats, en especial fitxers multimèdia (vídeos, fotografies, música, entre d'altres) i dades de caràcter personal alienes a les activitats del CSAPG.

Per garantir la disponibilitat de la informació en un incident de seguretat, es realitzen còpies de seguretat de les unitats de xarxa periòdicament. Per aquest motiu, els usuaris han d'emmagatzemar en aquestes unitats de xarxa les dades generades en el desenvolupament de les seves funcions. En aquest sentit, s'informa que no es realitzen còpies de seguretat de la informació que no es trobi en aquestes unitats.

La informació emmagatzemada a les còpies de seguretat podrà ser recuperada en cas que es produeixi un incident de seguretat o una eliminació errònia o accidental. Per recuperar aquesta informació caldrà fer una sol·licitud de restauració pels canals indicats a l'apartat 4.

5.2.1. SUPORTS D'EMMAGATZEMATGE EXTRAÏBLE

Com a norma general, l'ús de suports o mitjans d'emmagatzemat extraïbles (memòries USB, discs durs, etc.) al CSAPG no està autoritzat. Per a la seva utilització caldrà comptar amb la corresponent autorització.

En cas d'autoritzar l'ús d'aquests tipus de suports de treball a alguna persona usuària, es tindrà present les següents normes:

- Com a norma general, s'utilitzaran els suports extraïbles proporcionats pel CSAPG i seran destinats a un ús exclusivament professional, com a eina de transport puntual de fitxers, no com a eina d'emmagatzemat.
- L'ús de mitjans d'emmagatzemat extraïbles particulars, no està autoritzat, llevat que es disposi de la deguda autorització.
- El seu ús no està autoritzat per l'emmagatzemat de dades personals, tret que es disposi de la deguda autorització.

Aquests tipus de dispositius hauran d'estar en llocs segurs per prevenir robatoris o l'accés de tercers no autoritzats. Caldrà informar immediatament de la pèrdua o sostracció d'aquests dispositius, indicant llur contingut.

El transport d'aquests suports fora de las instal·lacions del CSAPG només serà realitzada per personal autoritzat, autorització que contemplarà igualment a la pròpia informació que surt. Caldrà enviar al sol·licitant assessorament sobre les mesures de seguretat que caldrà implementar.

5.2.2. ESBORRAT I ELIMINACIÓ DE SUPORTS INFORMÀTICS

Els mitjans d'emmagatzemat que per obsolescència o degradació perdin la seva utilitat (especialment aquells que continguin dades de caràcter personal), seran eliminats de forma segura per evitar accessos a aquesta informació.

5.3. GESTIÓ DE DOCUMENTS

5.3.1. IMPRESSORES EN XARXA, FOTOCOPIADORES I ESCÀNERS

En general, caldrà utilitzar les impressores en xarxa i les fotocopiadores corporatives. Excepcionalment, podran instal·lar-se 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 no hagin estat proporcionades pel CSAPG. En relació als sistemes de còpia i impressió i documentació impresa, els usuaris hauran de seguir aquestes directrius:

- En general, els documents es generaran en format electrònic, podent digitalitzar aquells que no siguin susceptibles de ser generats en aquest format.
- Quan s'imprimeixen documents en sistemes d'impressió o còpia comuns, aquests hauran de romandre el menor temps possible en 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 recordar retirar els originals.
- En cas de trobar-se documentació en una impressora, l'usuari la depositarà en el contenidor de destrucció confidencial.
- Per motius de seguretat, estalvi i sostenibilitat, abans d'imprimir documents, cal garantir que és absolutament necessari fer-ho.

5.3.2. CURA I PROTECCIÓ DE LA DOCUMENTACIÓ IMPRESA

La documentació ha de protegir-se de manera que només hi tingui accés el personal autoritzat. L'usuari tindrà en compte les següents mesures:

- Els llocs de treball romandran clars sense més material sobre la taula que el necessari per l'activitat que s'està realitzant en cada moment.
- Quan no s'utilitzi, caldrà desar-lo en armaris, calaixos, o arxivadors preferentment sota clau.
- Quan els documents no siguin necessaris, hauran de dipositar-se als contenidors de documentació confidencial. En cas de necessitar recuperar cap document llençat per error, cal trucar a la cap del servei de neteja que, prèvia petició justificativa escrita i signada per l'interessat, obrirà amb clau el contenidor.
- Abans de sortir de les sales de reunions o permetre que algú aliè hi accedeixi, s'esborraran les pissarres i es recolliran tots els documents amb cura de que no quedi cap tipus d'informació "sensible" o "interna" accessible a persones no autoritzades.

5.4. LLOC DE TREBALL CLAR

Els llocs de treball han de romandre clars, sense més material sobre la taula que el necessari per l'activitat que s'està realitzant en cada moment. En finalitzar la jornada laboral, caldrà desar suports d'informació, ja siguin dispositius digitals o documents en paper, en un lloc segur, especialment si contenen dades personals o informació confidencial.

5.5. 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 d'acord amb les polítiques del CSAPG. En l'autorització de l'accés s'establirà el perfil necessari amb el que es configurin les funcionalitats i privilegis disponibles en 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 contrasenya, dada multi factor, certificat digital i número secret (PIN), etc.) per l'accés als sistemes d'informació del CSAPG utilitzant la xarxa segura, protegida amb els serveis de seguretat destinats a aquest efecte, sent responsables de la seva custòdia i de tota activitat relacionada amb l'ús del seu accés personal, respecte els quals caldrà tenir present les següents mesures:

- El codi d'usuari és únic per cada persona, intransferible i independent de l'ordinador des d'on es realitza l'accés.
- En relació amb les credencials d'accés a la informació, el personal s'ha d'abstenir de fer les accions següents:
    - Evadir, alterar o suplantar els sistemes d'autorització i control d'accés.
    - Revelar o lliurar sota cap concepte les seves credencials d'accés a cap altra persona, ni tenir-les per escrit a la vista o a l'abast de tercers. Tampoc s'han de facilitar al personal de suport o administradors durant la resolució d'incidències.
    - Descuidar el deure de custòdia de les credencials i, en concret, fer constar en correus electrònics o qualsevol altre suport les credencials d'accés.
    - Deixar desatesos els dispositius digitals un cop superat el procés d'identificació i autenticació sense bloquejar-ne prèviament l'accés.
    - Utilitzar en l'àmbit personal les credencials corporatives en comptes de correu personals, xarxes socials i altres aplicacions.
    - Utilitzar cap accés autoritzat d'una altra persona, tot i que es disposi de l'autorització del seu titular.
- Si una persona té sospites de que les seves credencials estan sent utilitzades per una altra persona, ha de comunicar-ho immediatament.
- Els usuaris han d'utilitzar contrasenyes segures, d'acord amb la política establerta al CSAPG. No han d'estar formades només per paraules del diccionari o altres fàcilment previsibles o associables a l'usuari (noms de la seva 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 contrasenya almenys un cop l'any, previ avís amb suficients dies d'antelació. En els que no sigui possible, serà responsabilitat dels usuaris procedir al seu canvi anualment.

5.6. ACCÉS A UN COMPTE D'UN USUARI EN ABSÈNCIA O BAIXA

Quan sigui necessari accedir a la carpeta personal o compte de correu corporatiu d'un usuari, aquest s'haurà de realitzar amb l'autorització expressa de la persona titular i només podrà realitzar-se pel responsable del mateix o per la persona en qui aquest delegui.

En cas que no sigui possible aconseguir aquesta autorització (defunció, malaltia, impossibilitat de localització, etc.), l'accés podrà ser realitzat sempre i quan estigui autoritzat expressament i per escrit per la Direcció.

En ambdós casos caldrà motivar la necessitat d'accés i ser comunicat, si escau, al responsable de l'usuari, que elaborarà una acta en el que es recullin totes les accions dutes a terme.

L'accés a la informació de l'usuari es realitzarà sense comunicar la contrasenya de l'usuari en qüestió al seu responsable o a la persona en qui aquest delegui, de manera que caldrà assignar permisos d'accés o activar la delegació d'accés per a la persona designada.

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

La informació continguda al Sistema d'Informació del CSAPG és responsabilitat del CSAPG, pel que les persones usuàries han d'abstenir-se a comunicar, divulgar, distribuir o posar en coneixement o a l'abast de tercers (externs o interns no autoritzats) cap informació, excepte autorització expressa del CSAPG. Endemés, caldrà tenir present aquestes premisses:

- Amb caràcter general, es considera que la informació o la dada que el personal utilitza durant la seva activitat professional té el caràcter de confidencial, amb independència de si utilitza un dispositiu digital d'ús personal, i amb l'excepció de les dades que ja tinguin el caràcter de públiques.
- Tots els usuaris que per motiu de la seva activitat professional hagin tingut accés a informació gestionada pel CSAPG (documents, metodologies, claus, anàlisis, programes, etc.) hauran de mantenir una absoluta confidencialitat per temps indefinit.
- Els usuaris només podran accedir amb les degudes autoritzacions a aquella informació necessària per al desenvolupament de les seves tasques.
- Tota informació ha de ser utilitzada únicament per al compliment de les tasques que tenen encomanades els usuaris.
- Els drets d'accés dels usuaris a la informació i al Sistema d'Informació que la tracta hauran d'atorgar-se sempre en base als principis de "mínim privilegi", "necessitat de conèixer i responsabilitat de compartir" i "capacitat d'autoritzar".
- La informació que comprèn dades de caràcter personal quedarà afectada també per la normativa vigent en matèria de Protecció de Dades personals, estant obligats els usuaris a guardar secret sobre la mateixa, deure que es mantindrà de manera indefinida incloent més enllà de la relació laboral o professional amb el CSAPG.
- No està permès compartir, emmagatzemar o processar informació sensible, com dades personals, de salut (identificables) o qualsevol altra dada protegida, en plataformes de

serveis al núvol o d'intel·ligència artificial que no siguin corporatives. Només es poden utilitzar els entorns aprovats o proporcionats pel CSAPG.

5.8. NETEJA DE METADADES I DADES OCULTES DE DOCUMENTS ELECTRÒNICS

Les metadades contingudes als arxius poden afectar tant a la seguretat de la informació com a la imatge del CSAPG. Per això, tot arxiu que hagi de ser difós internament, remés electrònicament a un tercer o publicat a Internet (plana web, seu electrònica, etc.), haurà de ser revisat per determinar les metadades associades al mateix, procedint a la seva modificació o supressió, si procedeix, seguint el procediment de Minerva 5152. El procediment també es pot consultar a l'apartat "Consulta > Protecció de dades" de la Intranet.

5.9. CORREU ELECTRÒNIC CORPORATIU

El correu electrònic corporatiu és una eina de missatgeria electrònica centralitzada, posada a disposició dels usuaris del sistema d'informació del CSAPG per a l'enviament i recepció de correus electrònics mitjançant l'ús de comptes de correu corporatives. Al ser un recurs compartit, un ús indegut del mateix repercuteix directament al servei ofert a totes les persones.

El correu electrònic s'utilitzarà amb "sentit comú" i tenint en compte la responsabilitat i funcions desenvolupades, tractant en tot cas de no comprometre ni els sistemes ni la imatge del CSAPG.

El CSAPG queda facultat per filtrar el contingut del correu electrònic del compte de correu proporcionat per al desenvolupament de les funcions laborals, amb l'objectiu de prevenir virus o en el supòsit de que hi hagi motius fonamentats per una sospita per part del CSAPG sobre l'existència d'activitats delictives o doloses del personal.

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

Es podrà inserir contingut addicional als missatges enviats per advertir als receptors dels requisits legals i de seguretat que hauran de complir en relació als correus.

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

- Utilitzar el correu electrònic corporatiu per a l'exercici de les tasques i funcions assignades i exclusivament amb finalitats professionals.
- No es pot cedir l'ús del compte de correu a terceres persones. Tampoc enviar correus-e des de comptes de correu aliens, sense autorització expressa.
- Informar de correus amb virus, phishing, malware (programa maliciós), etc. sense reenviar-los per evitar-ne la possible propagació però no eliminar-los definitivament, deixant-los a la paperera per facilitar les accions correctives i preventives que pugui dur a terme el Departament de Sistemes d'Informació.
- No respondre missatges de Spam.
- Garantir la identitat del remitent abans d'obrir un missatge.

- No executar arxius adjunts ni enllaços sospitosos. No han d'executar-se els arxius adjunts rebuts sense analitzar-los prèviament amb l'eina corporativa contra codi maliciós.

Es consideren usos prohibits les següents actuacions:

- Falsificar, ocultar, suprimir o substituir la identitat de l'emissor en qualsevol correu electrònic o manipular el contingut de la informació d'un missatge reenviat, sempre que no s'adverteixi al receptor del tipus de tractament o alteració que se n'ha fet.
- Llegir o accedir a correus electrònics aliens, sense autorització prèvia.
- Fer constar, ni a l'assumpte ni al cos del missatge, informació de caràcter personal (inclòs números d'HC). En cas necessari, aquesta informació ha d'anar com arxiu adjunt i xifrat segons el document "Compressió i xifrat d'arxius amb 7zip" (Minerva 1152).
- Enviar sense xifrar correus electrònics a persones externes del CSAPG amb categories especials de dades (salut, afiliació sindical, etc.).
- Utilitzar el correu per a la difusió interna o externa de correu no desitjat o correu brossa, virus i codis maliciosos, així com per a l'enviament de cartes en cadena o l'enviament massiu de correus que no tinguin una relació directa amb les tasques i funcions encomanades.
- Enviar o reenviar missatges amb contingut ofensiu, poc ètic, amenaçador, discriminatori, calumniador o que pugui suposar un deteriorament de la imatge del CSAPG. En cas de rebre un contingut d'aquest tipus de qualsevol altre usuari del CSAPG, el receptor ho ha de posar en coneixement del seu superior jeràrquic.
- Enviar manualment o automàticament, mitjançant l'ús de regles de reenviament, missatges amb informació del CSAPG a bústies de correus personals, llevat que la Direcció corresponent ho autoritzi expressament.
- Utilitzar el correu electrònic corporatiu per al desenvolupament d'activitats privades no autoritzades o per a registrar-se en qualsevol servei, xarxa social, plataforma, etc. d'ús personal.

5.10. EINES DE COL·LABORACIÓ

Als efectes d'aquesta normativa, s'entén per eines de col·laboració corporatives les aplicacions i serveis que el CSAPG posa a disposició del personal i que pretenen:

a) Facilitar i millorar la comunicació, tant individualment com en grup.
b) Promoure la mobilitat interna dins d'una seu o fora d'ella.
c) Proveir de capacitats per treballar en equip ja sigui dins del seu àmbit o organisme, com transversal dins de la Generalitat i amb col·laboradors externs quan s'escaigui.
d) Facilitar la interacció en remot amb persones o entitats externes a la Generalitat.

Les directrius d'ús per a aquest tipus d'eines són les següents:

- No es poden usar eines no corporatives o no autoritzades quan existeixin solucions en l'entorn professional i quan es tracti informació confidencial.
- L'usuari haurà d'utilitzar l'entorn web de les eines de col·laboració corporatives quan hi accedeixi des d'un dispositiu personal.

- No es poden utilitzar les eines de col·laboració corporatives per al desenvolupament d'activitats privades no autoritzades.

5.11. ACCÉS A INTERNET

L'accés a Internet és un recurs centralitzat que el CSAPG posa a disposició dels usuaris, com a eina necessària per l'accés a continguts i recursos d'Internet, i com a suport al desenvolupament de l'activitat professional. El CSAPG vetllarà pel bon ús de l'accés a Internet, tant des del punt de vista de l'eficiència i productivitat del personal, com des dels riscs de seguretat associats al seu ús. Les normes d'ús són les següents:

- Les connexions que es realitzin a Internet han de tenir finalitats professionals i s'han de realitzar a través de les xarxes corporatives proporcionades pel CSAPG.
- Només es podrà accedir a Internet mitjançant els navegadors subministrats i configurats pel CSAPG. No es podrà alterar la seva 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 bloquegi l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva o pàgines potencialment insegures o que continguin codi maliciós.
- Caldrà notificar qualsevol anomalia (redirecció a pàgines no sol·licitades, avís de lloc no segur en planes web habituals, etc.) detectada en l'ús de l'accés a Internet, així com la sospita de possibles problemes o incidents de seguretat relacionats amb l'accés.

Es consideren usos prohibits les següents actuacions:

- La descàrrega de programes informàtics sense l'autorització prèvia o fitxers amb contingut nociu que suposi una font de riscs per al CSAPG. En tot cas cal garantir que el lloc web visitat és confiable.
- L'accés, la descàrrega i/o l'emmagatzemat en qualsevol suport de pàgines amb continguts il·legals, nocius, inadequats o que atemptin contra la moral i l'ètica.
- 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 qualsevol altre tipus de contingut (música, pel·lícules, videojocs, etc.) que no estigui expressament autoritzats.
- La utilització de plataformes de transmissió de continguts, o streaming.
- Connectar-se a xats, fòrums de discussió, grups de treball o qualsevol aplicació interactiva, així com participar en jocs en línia, que no tinguin relació directa amb les tasques i funcions encomanades.
- Utilitzar la connexió a Internet corporativa o qualsevol accés extern (VPN, Citrix, etc.), per al desenvolupament d'activitats privades no autoritzades.
- En el cas de portàtils i altres dispositius mòbils, connectar a Internet utilitzant xarxes WiFi públiques obertes no vinculades amb el CSAPG, com les de cibercafès, aeroports, restaurants o centres comercials, entre altres.

5.12. CERTIFICATS ELECTRÒNICS

Els certificats electrònics autoritzats per al desenvolupament de les funcions encomanades al CSAPG són els certificats en format físic o digital, emesos pel Consorci d'Administració Oberta de Catalunya (AOC) o per la Fábrica Nacional de Moneda y Timbre (FNMT), vàlids per a la signatura o el xifratge de documents i la realització de tràmits amb plenes garanties jurídiques i tècniques. Les directriu d'ús dels certificats són les següents:

- En el cas de la signatura electrònica, el certificat digital s'ha d'utilitzar quan el personal hagi d'acreditar la seva pertinença al CSAPG, sens perjudici que calgui utilitzar altres certificats reconeguts per acreditar l'adscripció a col·legis professionals o per interactuar amb altres administracions.
- El CSAPG podrà sol·licitar la revocació de certificats d'usuari associats a l'entitat sense avís previ.
- En casos excepcionals i autoritzats per la Direcció, l'ús dels certificats associats a l'entitat, i no a una persona individual, es podrà delegar en altres persones per a que puguin realitzar tasques concretes que tenen assignades.
- Els certificats digitals només poden ser utilitzat en l'àmbit personal per a aquells tràmits electrònics admesos per administracions o entitats del sector públic i en cap cas es poden fer servir per a usos comercials o mercantils privats.
- El personal ha de tenir cura del certificat, pel que fa a la conservació en bon estat en el cas de targetes físiques i a la custòdia adequada de fitxers de certificat, claus i contrasenyes en el cas de certificats en format digital.

6. PÈRDUA DE LA VINCULACIÓ DEL PERSONAL AMB EL CSAPG

Quan un usuari perdi la seva vinculació amb el CSAPG, aplicaran les següents directrius:

- El personal s'ha d'abstenir d'esborrar informació dels dispositius digitals, de la xarxa, espais o serveis corporatius, aplicacions corporatives, bústies de correu departamentals i suports externs d'informació.
- El personal haurà de lliurar al Departament d'Informàtica els dispositius digitals i els suports externs que custodiï segons el procediment establert.
- Els certificats digitals en format físic proporcionats pel CSAPG (TCAT) hauran de ser retornats a l'encarregat de la gestió dels mateixos, per a que procedeixi a la baixa segons el procediment establert.
- En casos de jubilació definitiva s'aplicarà el procediment de baixa dels recursos informàtics previstos. Només en aquells casos on s'autoritzi expressament per la Direcció corresponent es podrà acordar mantenir l'accés al correu electrònic i al portal del treballador per un període de temps limitat.
- En els casos on sigui convenient, s'establirà un missatge de resposta automàtica al compte de correu electrònic de l'usuari indicant que el compte ja no és operatiu i l'adreça on s'hauran de dirigir els missatges de correu electrònic en endavant.
- En cap cas es redireccionarà el correu electrònic cap a una adreça aliena al CSAPG.

- El Departament d'Informàtica podrà recuperar la informació dels serveis informàtics que es van posar a la disposició del personal per a l'exercici de les seves funcions mitjançant procediments i garanties previstos en la normativa vigent.

7. PERSONAL I DISPOSITIUS EXTERNS

L'ús de les TIC per part del personal d'empreses externes que presten serveis al CSAPG en virtut d'un contracte o encàrrec de prestació de serveis, sense perjudici del que estableixi l'instrument que en reguli la prestació, se subjecta a les condicions addicionals següents:

- La utilització dels recursos TIC per part del personal extern ha de ser prèviament autoritzada per la Direcció de la que depengui la prestació d'aquest servei extern.
- Les identitats del personal extern no podran ser genèriques, estaran sempre vinculades unívocament a una persona física. El personal extern només es podrà connectar a la xarxa corporativa utilitzant el seu identificador corporatiu nominal.
- Quan els equips del personal extern no són propietat del CSAPG, hauran de complir una política de seguretat d'acord amb aquestes directrius:
    - El sistema operatiu de l'equip haurà de comptar amb el suport i el manteniment del fabricant i una política d'aplicació d'actualitzacions activa.
    - Tots els programes que ho requereixin han de tenir una llicència vàlida.
    - L'equip disposarà de programari contra codi nociu amb suport de fabricant vigent i amb política d'actualització automàtica activa amb periodicitat diària com a mínim. Aquest programari s'executarà automàticament en el moment de l'arrencada de l'equip i analitzarà qualsevol binari que s'executi i els fitxers que s'obrin de tot dispositiu extern que es connecti.
- La configuració dels equips del personal extern haurà de ser modificada a instàncies del Departament d'Informàtica del CSAPG, si aquest considera que existeix un risc per a la seguretat de la informació. En el mateix supòsit, es podrà indicar la instal·lació dels programes necessaris per mantenir el nivell de seguretat desitjat en els sistemes d'informació corporatius.
- No està permès connectar els dispositius amb connexions alternatives (mòdem, *tethering* mòbil o WiFi) quan el dispositiu estigui connectat a la vegada a la xarxa del CSAPG.
- Sense l'autorització expressa del Departament d'Informàtica del CSAPG, no està permès tenir actius en els dispositius programes de tipus servidor que puguin alterar el funcionament de la xarxa corporativa, com serveis DNS o DHCP, servidors web, etc.

8. SUPERVISIÓ I APLICACIÓ D'AQUESTA NORMATIVA

Per motius legals, de seguretat i de qualitat del servei, i complint en tot moment els requisits que estableix la legislació vigent, el CSAPG:

- Revisarà periòdicament l'estat dels equips, el software instal·lat, els dispositius i xarxes de comunicacions de la seva responsabilitat.
- Podrà registrar i supervisar els accessos a la informació ubicada en els seus sistemes.

- Auditarà la seguretat de les credencials i les aplicacions.
- Supervisarà 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, d'acord amb la normativa sobre protecció de dades personals, de funció pública o laboral, i demés disposicions que resultin d'aplicació i tenint en compte aquestes directrius:

- Quan sigui necessària la connexió remota a equips client per resoldre incidències o realitzar qualsevol altra intervenció de manteniment sobre l'equip, aquesta connexió es realitzarà amb el coneixement de l'usuari que estigui utilitzant el dispositiu.
- Es registraran les activitats dels usuaris, retenint la informació necessària per supervisar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar en cada moment a la persona que actua.
- Els sistemes en els que es detecti un ús inadequat o en els que no es compleixin els requisits mínims de seguretat, podran 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, refusar, bloquejar o eliminar part del contingut dels missatges enviats o rebuts en els que es detecti algun problema de seguretat o d'incompliment d'aquesta Normativa. Es podrà inserir contingut addicional als missatges enviats per advertir als receptors sobre els requisits legals i de seguretat que caldrà 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 enregistrar i deixar traça de les pàgines a les que s'ha accedit, així com del temps d'accés, volum i mida dels arxius descarregats. El sistema permetrà l'establiment de controls que possibilitin detectar i notificar sobre usos perllongats i indeguts del servei.

Sens perjudici dels punts anteriors i a l'efecte de verificar els indicis existents sobre usos indeguts, il·lícits o abusius, l'accés a la informació necessària es podrà dur a terme prèvia autorització, amb caràcter d'informació reservada, d'un membre de la Direcció o la Gerència, i sempre tenint en compte aquests preceptes:

- L'acte d'accés a la informació es durà a terme respectant la normativa de protecció de dades de caràcter personal i la intimitat i dignitat de la persona afectada, en presència seva i, si ho sol·licita, la d'un representant del personal, dins l'horari de prestació de serveis o laboral.
- Si la persona afectada es nega a presenciar l'acte de revisió podrà designar una persona que la representi a l'efecte, i, si no la designa, es farà constar la negativa a presenciar la revisió en l'acta corresponent i continuarà el procediment.
- Els assistents als actes de revisió han de guardar reserva de totes les actuacions.
- En l'acta que s'estengui s'ha de fer constar la identificació dels assistents, les actuacions de revisió i comprovació dutes a terme, el resultat de les actuacions, les incidències que s'hagin produït i les que els assistents vulguin manifestar.

9. INCOMPLIMENT DE LA NORMATIVA

Els usuaris del sistema d'informació del CSAPG estan obligats a complir el prescrit en aquesta "Normativa d'Ús de Mitjans Electrònics". Qualsevol excepció en el seu compliment, sempre que sigui justificada en l'exercici de les funcions i tasques encomanades i no contravingui el 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 demés disposicions que resultin d'aplicació, ha de ser autoritzada prèviament per la Direcció.

En el cas que un usuari no contempli algun dels preceptes fixats en aquesta normativa, sense perjudici de les accions disciplinàries i administratives que procedeixin i, si escau, les responsabilitats legals corresponents, es podrà acordar la suspensió temporal o definitiva de l'ús dels recursos informàtics 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 les penalitats previstes al contracte de prestació de serveis i comportar les mesures de restricció o suspensió que el CSAPG consideri adients, podent arribar inclús a la resolució del contracte, seguint el procediment establert a la normativa sobre contractació administrativa.