Política d'ús de Sistemes d'Informació i Recursos Informàtics

Servei de Qualitat i Medi Ambient

HISTÒRIC DE CANVIS		
Versió	**Data**	**Descripció de la modificació**
0	26-07-2019	S'afegeix el històric de canvis i la capçalera
1	04/01/2023	S'actualitza amb la nova marca corporativa del CETT

INDEX

1. OBJECTE

Definir les polítiques sobre l'ús apropiat dels recursos informàtics corporatius.

2. ABAST

Aquesta reglamentació s'aplica a tot membre del personal de la Fundació Gaspar Espuña-CETT, Estudis d'Hoteleria i Turisme CETT SA, integral en Turisme i Hoteleria, SL, Turisvall SL i Viatges Century, SA, Associació CETT Alumni (d'ara en endavant referenciats com a Grup CETT) que tingui accés als sistemes i els recursos de l'empresa, ja sigui personal intern de caràcter permanent o eventual (pràctiques) o personal tutelat per Empreses Externes i / o de treball temporal.

3. DEFINICIONS

S'utilitzaran, per a un millor enteniment del reglament d'usos de sistemes d'informació i recursos informàtics les següents definicions:

- **Sistemes d'Informació:** qualsevol sistema o aplicació de programari que sigui administrat pel Servei de STIC com a sistemes operatius, aplicacions de servidor i aplicacions basades en Internet.
- **Recursos Informàtics**: equips informàtics (servidors, desktops, portàtils, portàtils, impressores i perifèrics), equips de suport i infraestructura de comunicacions (routers, switches, WiFi access points, cablejats), programari de base (administració de domini, administració de base de dades, seguretat de xarxa, antivirus), programari de gestió ERP i programari d'ofimàtica i / o similar (Word, Excel, PowerPoint, PDF s, Access, etc.).
- **Usuari:** Tot el personal inclòs en l'Abast. Tot usuari al qual se li assigni un recurs informàtic de Grup CETT es converteix automàticament en "Custodi" sense cap altre document de caràcter vinculant.
- **Custodio:** tota aquella persona, àrea o procés al qual se li hagi assignat un recurs informàtic mitjançant un document formal vinculant i el qual no necessàriament faci ús directe del recurs.
- **Material NO Autoritzat:** inclou la transmissió, distribució o emmagatzematge de tot material que violi qualsevol llei aplicable. S'inclou

SENSE limitació, material protegit per drets de reproducció, marca comercial, secret comercial o un altre dret sobre la propietat intel·lectual utilitzada sense la deguda autorització i material que resulti obscè, difamatori o il·legal sota les lleis nacionals.

- Xarxa: inclou qualsevol sistema de cablejat i equips físics que permetin les transaccions de dades no inclosos a l'apartat Recursos Informàtics.
- Xarxa de Dades: és el conjunt de recursos informàtics que permeten la transferència de dades i informació a través de tota la xarxa interna, externa i Internet.
- Dades: informació continguda en qualsevol sistema d'emmagatzematge, discs locals, discos d'accés compartit ubicats en servidors i tota la informació i bases de dades gestionades dels sistemes utilitzats en Grup CETT, incloent la informació de caràcter ofimàtica.
- Maquinari: tots els recursos maquinari de l'empresa que tenen com a finalitat la seguretat, captura o procés de dades i qualsevol mitjà de comunicació, tant interna com externa.
- ERP: programari de gestió de dades modular que resideix en una única "base de dades" a la qual s'incorpora tot tipus d'informació procedent de tots els Processos de l'Empresa i gestionada "a temps real", on cada usuari se li assigna un paper d'accés per tal de garantir la confidencialitat i seguretat de les dades.

4. REGLAMENT

4.1. Utilització dels recursos i sistemes d'informació

Artículo 1. Utilització de l'equip informàtic i de comunicacions

a) Grup CETT facilita als usuaris que així ho necessitin, els equips informàtics i dispositius de comunicacions, tant fixos com mòbils, necessaris per al desenvolupament de la seva activitat professional. Així doncs, les dades, dispositius, programes i serveis informàtics que Grup CETT posa a

disposició dels usuaris s'han d'utilitzar per al desenvolupament de les funcions encomanades, és a dir, per a fins professionals.

b) En general, l'ordinador personal (PC), mòbils i tablets, seran els recursos informàtics que permetran l'accés dels usuaris als sistemes d'informació i serveis informàtics de Grup CETT, constituint un element molt important en la cadena de seguretat dels sistemes d'informació, raó per la qual és necessari adoptar una sèrie de precaucions i establir normes per a la seva adequada utilització.

c) Aquest epígraf fa específicament a tots els recursos informàtics facilitats i configurats per Grup CETT per la seva utilització per part dels usuaris, incloent equips de sobretaula, portàtils i dispositius mòbils amb capacitats d'accés als sistemes d'informació de l'organització.

d) Normes generals:

1. Els equips informàtics seran assignats pel Responsable de Manteniment de STIC.
2. Hi haurà un inventari actualitzat dels equips informàtics. El Responsable de Manteniment de STIC serà l'encarregat de gestionar aquest inventari.
3. Si un nou usuari s'incorpora a l'organització i requereix un equip informàtic, el Servei de STIC s'ho facilitaria, degudament configurat i amb accés als arxius, serveis i aplicacions necessàries per a l'exercici de les seves competències professionals. Després de:

   I- L'Aprovació del cap responsable.

   II- Omplir la fitxa d'alta d'usuari (FOR06-PGG18).

   III- notificar a assistencia.sti@cett.cat sobre la nova fitxa d'alta.

4. Els ordinadors personals s'han d'utilitzar únicament per a fins professionals i com a eina de suport a les competències professionals dels usuaris autoritzats.
5. No es permet utilitzar els recursos telemàtics de Grup CETT, inclosa la xarxa Internet, per a activitats que no es troben directament relacionades amb el lloc de treball de l'usuari.
6. Únicament l'equip de Manteniment de STIC podrà distribuir, instal·lar o desinstal·lar programari i maquinari, o modificar la configuració de qualsevol dels equips. Es considera equips a:

   I- Ordinadors personals.
   II- Ordinadors mòbils.
   III- *Smartphones* o pastilles.
   IV- *Access Points*.
   V- CD, DVD, USB, etc.

7. Està prohibit alterar, sense la deguda autorització, qualsevol dels components físics o lògics dels equips informàtics i dispositius de comunicació, excepte autorització expressa del Servei de STIC. En tot cas, aquestes operacions només podran realitzar-se per l'equip de Manteniment i Servei de STIC.
8. Excepte autorització expressa del Servei de STIC, els usuaris no tindran privilegi d'administració sobre els equips.

   I- Amb fins d'eficiència dels equips portàtils podran disposar de privilegi d'administrador. No obstant això, aquest privilegi no eximeix del compliment de tots els punts d'aquesta política, amb especial menció a:

      (a) Les limitacions d'instal·lació de programari,
      (b) Ús responsable de l'equip, internet i el correu electrònic, i

(c) Mantenir actualitzat tot el programari de seguretat (antivirus, antimalware, FW personal, etc.).

9. Els usuaris han de facilitar al personal de Manteniment STIC l'accés als seus equips, que siguin propietat de Grup CETT, ja sigui de forma presencial o remota, per a tasques de reparació, instal·lació o manteniment. Aquest accés es limitarà únicament a les accions necessàries per al manteniment o la resolució de problemes que poguessin trobar-se en l'ús dels recursos informàtics i de comunicacions, i finalitzarà completat el manteniment o un cop resolts aquells.
10. Qualsevol reubicació dels sistemes d'informació, recursos informàtics, maquinari, etc., serà realitzada pel Responsable de Manteniment de STIC per tal d'evitar pèrdues d'informació o alteració de les configuracions dels perifèrics que poguessin modificar la seva configuració.
11. Les actualitzacions de sistema operatiu i antivirus es distribueixen per tots els equips de la xarxa de forma automàtica. Les actualitzacions dels aplicatius es realitzen en funció de les particularitats del propi aplicatiu, per la qual cosa l'usuari haurà d'acceptar les propostes d'actualització.
12. Els usuaris han de notificar al Servei de STIC al més aviat possible, qualsevol comportament anòmal del seu ordinador personal, especialment quan hi hagi sospites que s'hagi produït algun incident de seguretat en el mateix.
13. L'usuari haurà de participar en la cura i manteniment de l'equip que té assignat, detectant l'absència de cables i accessoris, i donant compte al Servei de STIC d'aquestes circumstàncies.
14. Només estan autoritzats com a suports d'emmagatzematge de dades els homologats per Grup CETT. L'usuari ha d'utilitzar mecanismes d'accés a la informació en el núvol per evitar l'ús de dispositius USB.

15. L'usuari ha de ser conscient de les amenaces provocades per malware. Molts virus i troians requereixen la participació dels usuaris per propagar-se, ja sigui a través de disquets, CD / DVD, memòries USB, missatges de correu electrònic o instal·lació de programes descarregats des d'Internet. És imprescindible, per tant, vigilar l'ús responsable dels equips per reduir aquest risc.
16. Usos específicament prohibits. Estan terminantment prohibits els següents comportaments:

I- Utilització de qualsevol tipus de programari nociu i la instal·lació de qualsevol programari sense previ coneixement i consentiment per part del Servei de STIC.

II- Utilització de programes que, per la seva naturalesa, facin un ús abusiu de la xarxa.

III- Utilització de connexions i mitjans sense fils amb tecnologies WiFi, Bluetooth o infrarojos que no estiguin degudament autoritzats pel Servei de STIC, especialment WiFi gratuïtes que no pertanyin al Grup CETT.

IV- Instal·lació i / o utilització de programes o continguts que vulnerin la legislació vigent en matèria de Propietat Intel·lectual.

Artículo 2. Pèrdua o robatori de recursos

a) La sostracció d'aquests equips s'ha de notificar al responsable immediat al més aviat possible i aquest a la Gerència. A partir d'aquí s'inicia el protocol establert.

Artículo 3. Normes específiques per a l'emmagatzematge d'informació

a) Amb caràcter general, la informació emmagatzemada de forma local en els ordinadors personals dels usuaris (disc dur local, per exemple) no serà

objecte de salvaguarda mitjançant cap procediment corporatiu de còpia de seguretat.

b) Si en el desenvolupament del treball es necessita emmagatzemar dades de caràcter personal en ordinadors o en qualsevol suport informàtic, l'usuari es responsabilitzarà d'adoptar les mesures de seguretat oportunes mentre aquestes dades es mantinguin.
c) Grup CETT té a disposició dels usuaris unitats de xarxa compartides per a l'emmagatzematge de tota la informació amb la que duen a terme les seves funcions laborals. Aquestes unitats són sotmeses al sistema de còpies de seguretat com es detalla en el document "PGG18 Servei de Sistemes i Tecnologies de la Informació i la Comunicació".
d) No es permet emmagatzemar informació privada, de qualsevol naturalesa, en els recursos d'emmagatzematge compartits o locals.

Artículo 4. Norma específica per a equips a la zona de Servidors,

a) L'accés a la zona de servidors i l'ús dels equips de procés de dades, programari i aplicacions que allí es troben, està restringit exclusivament a personal autoritzat a través del sistema de gestió de targetes d'accés.

Artículo 5. Normes específiques per a equips portàtils i mòbils

a) Els equips portàtils i mòbils seran assignats pel Responsable de Manteniment TIC, sota la petició prèvia del responsable de l'usuari de l'equip, prèvia aprovació per part de la Gerència.
b) Hi haurà un inventari actualitzat dels equips portàtils i mòbils. El Servei de STIC serà la unitat encarregada de gestionar aquest inventari.
c) Aquest tipus de dispositius estarà sota la custòdia de l'usuari que els utilitzi i haurà d'adoptar les mesures necessàries per evitar danys o sostracció, així com l'accés a ells per part de persones no autoritzades.

d) Els equips portàtils i mòbils s'han d'utilitzar únicament per a fins professionals, especialment quan es facin servir fora de les instal·lacions de Grup CETT.

e) Els usuaris d'aquests equips es responsabilitzaran que no seran usats per terceres persones alienes al Grup CETT o no autoritzades per a això.

f) S'ha d'evitar en la mesura possible l'ús de xarxes Wifi desconegudes o gratuïtes que no pertanyin al Grup CETT.

g) Els equips portàtils propietat de Grup CETT estan sotmesos a un procés de manteniment regular. Per tant, al moment de connectar-los a la LAN, el sistema detecta actualitzacions pendents del sistema operatiu i l'antivirus i es procedeix a l'actualització automàtica.

h) 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, el responsable de notificar, en el full de baixa, com actuar amb els recursos i després es procedeix a actualitzar l'inventari.

i) Existeix a disposició dels empleats el document FOP (Funcions i obligacions del personal), que facilita l'ús responsable d'equips portàtils i mòbils.

Artículo 6. Ús de memòries / llapis USB (pendrives)

a) Només estan autoritzats com a suports d'emmagatzematge de dades els homologats per Grup CETT L'usuari ha d'utilitzar mecanismes d'accés a informació al núvol per evitar l'ús de dispositius USB.

Artículo 7. Connexió a la Xarxa de Dades

a) Només es podran connectar equips informàtics a les xarxes de dades corporatives, sempre que aquests estiguin sota control del Servei de STIC, que el registrarà de forma adequada.

Artículo 8. Gravació de CD, DVD, Blu-ray

a) Amb caràcter general, s'han d'utilitzar les unitats de xarxa i eines en el núvol per compartir informació vinculada a l'activitat professional. Per a casos molt puntuals en què es requereixi l'enregistrament de CD, DVD, Blu-ray, s'ha de fer la petició del suport d'enregistrament en el departament de STIC.
b) Si es detecta qualsevol anomalia en el procés d'enregistrament, es fa saber a Gerència i es determina la idoneïtat o no de la gravació.

Artículo 9. Còpies de seguretat

a) Mantenir còpies de seguretat és una cautela essencial de protecció de la informació.
b) Les dades generades per l'usuari en l'exercici de les seves competències professionals s'han de mantenir en un repositori en una unitat de xarxa compartida.
c) Diàriament, es realitzaran còpies de seguretat completes de les unitats de xarxa compartides de Grup CETT, on s'emmagatzemi la informació de l'usuari. En cap cas es realitzarà còpia de seguretat de la informació emmagatzemada de forma local en el lloc de l'usuari.
d) Per part del Servei de STIC es realitzaran còpies de seguretat dels fitxers del sistema d'emmagatzematge en xarxa (carpetes del servidor) i de la resta de sistemes corporatius segons el Procediment de Servei de STIC. Si algun usuari vol recuperar algun fitxer esborrat del sistema d'emmagatzematge en xarxa, ho ha de sol·licitar al Servei de STIC a través del correuassistencia.sti@cett.cat
e) La informació emmagatzemada en les còpies de seguretat podrà ser recuperada en el cas que es produeixi algun incident. Per recuperar aquesta informació l'usuari haurà de dirigir-se al Servei de STIC.

Artículo 10. Esborrat i eliminació de suports informàtics

a) Les còpies de seguretat o els mitjans d'emmagatzematge que, per obsolescència o degradació, perdin la seva utilitat, i especialment aquells que continguin informació sensible, confidencial o protegida, hauran de ser eliminats de forma segura per evitar accessos ulteriors a aquesta informació.

   En aquest sentit, el Servei de STIC:

   1. Farà una neteja de la informació del dispositiu.
   2. Portarà el dispositiu a una empresa externa de reciclatge.

Artículo 11. Impressores en xarxa, fotocopiadores i faxos

a) Quan s'imprimeixi documentació, haurà de romandre el menor temps possible a les safates de sortida de les impressores, per evitar que terceres persones puguin accedir-hi.
b) Convé no oblidar prendre els originals de la fotocopiadora, un cop finalitzat el procés de còpia. Si es trobés documentació sensible, confidencial o protegida abandonada en una fotocopiadora o impressora, l'usuari el lliurarà a la persona que està a la Recepció, qui s'encarregarà de lliurar-los al seu amo.
c) Els documents que s'enviïn per fax hauran de retirar immediatament de l'equip, de manera que ningú tingui accés al seu contingut si no disposa de l'autorització precisa.
d) Depenent de la tipologia de la informació trobada, podrà obrir-se el corresponent incident de seguretat.

Artículo 12. Digitalització de documents

a) Amb caràcter general, quan es digitalitzin documents, l'usuari haurà de ser especialment curós amb la selecció del directori compartit on hauran d'emmagatzemar-les imatges obtingudes, especialment si contenen informació sensible, confidencial o protegida.
b) Convé no oblidar prendre els originals de l'escàner, un cop finalitzat el procés de digitalització. Si es trobés documentació sensible, confidencial o protegida abandonada en un escàner, l'usuari el lliurarà a la persona que està a la Recepció, qui s'encarregarà de lliurar-los al seu amo.

Artículo 13. Cura i protecció de la documentació impresa

a) La documentació impresa que contingui dades sensibles, confidencials o protegits, ha de ser especialment protegida, de manera que només tingui accés a ella el personal autoritzat, havent de ser recollida ràpidament de les impressores i fotocopiadores i ser custodiada en armaris amb clau.
b) Els espais que contenen informació confidencial es troben restringits a personal autoritzat segons el sistema de targetes existent.
c) Cadascun dels departaments posseeix un inventari de tipus de document i com procedir a l'acabar la seva vida útil segons el seu nivell de privacitat. Tota la informació es detalla en el procediment de gestió de documents no automatitzats.
d) La persona que es trobi al càrrec de documentació impresa amb dades sensibles, confidencials o protegits, quan aquesta no estigui arxivada per estar en procés de revisió o tramitació, és responsable de custodiar aquesta informació i d'impedir en tot moment que hi pugui accedir per persona no autoritzada.
e) Per raons ecològiques i de seguretat, abans d'imprimir documents, l'usuari ha d'assegurar que és absolutament necessari fer-ho.

Artículo 14. Instal·lacions per a reunions i de classes

a) La persona usuària de l'espai té la responsabilitat sobre els recursos, així com d'obrir i tancar l'armari que conté els recursos, a nivell físic i lògic.
b) Abans d'abandonar les sales o permetre que algú aliè entri, es netegessin adequadament les taules, les pissarres, tenint cura que no quedi cap tipus d'informació sensible o que pogués ser reutilitzada.

Artículo 15. Seguretat en el lloc de treball

a) Un cop acabada la jornada laboral tot suport físic (electrònic o paper) que hagi estat utilitzat ha de ser guardat en un lloc segur i no visible, no havent de quedar sobre de les taules de treball cap element susceptible de contenir qualsevol tipus d'informació.
b) Si la informació amb la qual es treballa és de caràcter confidencial o conté dades de caràcter personal ha de ser guardada en els espais disposats per a això i protegits mitjançant el sistema d'accés amb targeta.
c) Si s'abandona el lloc de treball durant un període de temps considerable cal bloquejar l'accés als dispositius electrònics, així com protegir els documents sensibles. Aquest fet és obligatori i responsabilitat de l'usuari, independentment de les mesures tècniques que puguin facilitar aquest bloqueig.
d) El personal de l'empresa ha de mantenir el seu entorn de treball correctament ordenat i recollit un cop acabada la jornada laboral.

Artículo 16. Protecció de la propietat intel·lectual

a) Està estrictament prohibit l'execució de programes informàtics en els equips i dispositius de Grup CETT sense la corresponent llicència d'ús.
b) Els programes informàtics propietat de Grup CETT, o llicenciats al Grup CETT, estan protegits per la vigent legislació sobre Propietat Intel·lectual i, per tant, està estrictament prohibida la seva reproducció, modificació,

cessió, transformació o comunicació, llevat que els termes de l'llicenciament ho permetin i amb l'autorització prèvia del Servei de STIC.

c) Està estrictament prohibit l'ús, reproducció, cessió, transformació o comunicació pública de qualsevol altre tipus d'obra protegida per drets de propietat intel·lectual.
d) Qualsevol requisit d'instal·lació de programari ha de ser autoritzat prèviament pel Servei de STIC, com s'especifica en el FOP.

Artículo 17. Protecció de la dignitat de les persones

a) Està terminantment prohibida tota transmissió, distribució o emmagatzematge de qualsevol material obscè, difamatori, amenaçador o que constitueixi un atemptat contra la dignitat de les persones.

Artículo 18. Ús eficient d'equips i recursos informàtics

a) Dins de les mesures adoptades per Grup CETT es promouen les següents accions per a un ús més eficient dels mitjans tecnològics posats a disposició dels usuaris.
b) Apagar el PC (i la impressora local, si s'escau), en finalitzar la jornada laboral. Aquesta mesura obeeix tant a raons de seguretat com d'eficiència energètica.
c) Imprimir únicament aquells documents que siguin estrictament necessaris. La impressió es farà, preferiblement, a doble cara i evitant, sempre que sigui possible, la impressió en color.
d) S'optarà per usar les impressores en xarxa abans que les locals.
e) Com que els recursos d'emmagatzematge en xarxa són limitats i compartits entre tots els usuaris, cal fer un ús responsable dels mateixos i emmagatzemar únicament aquella informació que sigui estrictament necessària.

Artículo 19. Instal·lació de programari

a) Únicament l'Equip de Manteniment TIC podrà instal·lar programari en els equips informàtics o de comunicacions dels usuaris.
b) No es podrà instal·lar o utilitzar programari que no disposi de la llicència corresponent o la utilització no sigui conforme amb la legislació vigent en matèria de Propietat Intel·lectual.
c) Es prohibeix terminantment la reproducció, modificació, transformació, cessió, comunicació o ús fora de l'àmbit de Grup CETT dels programes i aplicacions informàtiques instal·lades en els equips que pertanyen a l'organització.
d) En cap cas es podran eliminar o desactivar les aplicacions informàtiques instal·lades pel Servei de STIC, especialment aquelles relacionades amb la seguretat.
e) El Servei de STIC podrà realitzar, sense previ avís, la desinstal de qualsevol programari instal·lat en equips de procés que no compleixin els requisits d'acord amb el lloc de treball / paper autoritzats per la Direcció.

Artículo 20. Accés als sistemes d'informació ia les dades tractades

a) És responsabilitat de l'usuari fer bon ús del seu compte d'usuari. El compte es podrà desactivar pel Servei de STIC en cas de mala utilització.
b) Els usuaris tindran autoritzat l'accés únicament a aquella informació i recursos que necessitin per al desenvolupament de les seves funcions. L'accés a la informació serà personal i les credencials d'accés, intransferibles.
c) Quan un usuari deixi d'atendre un PC durant un cert temps, cal bloquejar la pantalla d'usuari o activar el salvapantalles, per evitar que cap persona pugui fer un mal ús de les seves credencials, i pot arribar a suplantar-lo.

1. Haurà salvaguardar qualsevol informació, document, suport informàtic, dispositiu d'emmagatzematge extraïble, etc., que pugui contenir informació confidencial o protegida davant de possibles revelacions o robatoris de tercers no autoritzats.

d) Assignació de permisos.

1. L'assignació (i / o revocació) de perfils d'autorització als usuaris quedarà degudament registrat, i en tots els casos requerirà de l'autorització del responsable immediat de l'usuari.
2. L'assignació de privilegis es realitzarà mitjançant el principi de mínim privilegi i la necessitat d'ús.

I- No s'atorgaran privilegis a cap usuari fins s'hagi completat el procés d'autorització.

II- Cada usuari -i el seu responsable directe- és responsable dels permisos d'accés que té assignats, i de les accions que es derivin de l'explotació d'aquests.

III- El responsable del departament a què pertany l'usuari és el que determina els accessos necessaris.

IV- Les excepcions al principi de mínim privilegi o la no segregació de funcions haurà de ser autoritzada pel responsable directe, assumint el risc i les possibles conseqüències.

Artículo 21. Identificació i autenticació. Ús de contrasenyes

a) Tot accés als sistemes d'informació de Grup CETT es realitzarà a través d'un procés de validació de l'usuari que determini l'autorització per accedir al propi sistema i els permisos de què disposarà un cop hagi accedit al sistema.

1. Qualsevol procés d'accés constarà, com a mínim, de les següents fases:

   I- Fase d'identificació: En aquesta fase l'usuari haurà d'introduir el seu codi personal.

   II- Fase de validació: En aquesta fase es comprovarà la propietat del codi introduït, en el qual l'usuari supera una prova d'autenticació.

2. Es consideraran vàlids tots aquells mètodes d'autenticació inequívoca que garanteixin, com a mínim, els mateixos objectius de seguretat proveïts per l'ús de la combinació "usuari-contrasenya".

b) Els usuaris no han de revelar o lliurar, sota cap concepte, els seus credencials d'accés o targeta criptogràfica a una altra persona, ni mantenir-les per escrit a la vista o l'abast de tercers.

c) Els usuaris no han d'utilitzar cap accés autoritzat d'un altre usuari, encara que disposin de l'autorització del seu titular.

d) Si un usuari té sospites que les seves credencials estan sent utilitzades per una altra persona, ha de posar en coneixement del responsable del sistema per tal que li assigni una nova clau d'accés.

e) Els usuaris han d'utilitzar contrasenyes segures:

1. Les contrasenyes han de tenir una longitud mínima de 8 caràcters i es recomana que incloguin lletres majúscules i minúscules, caràcters especials (del tipus @, #, +, etc.) i dígits numèrics.
2. Les contrasenyes no han d'estar compostes únicament per paraules del diccionari o altres fàcils de predir 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.).
3. Les contrasenyes han de canviar-se periòdicament.

4. Si un usuari entén que la contrasenya ha quedat compromesa o l'ha cedit a tercers autoritzats per motius de treball o manteniment, ha de procedir a substituir-la per una altra que no hagi estat compromesa, de manera immediata.
5. D'altra banda, l'usuari haurà de realitzar una petició de canvi de contrasenya.
6. Cap usuari està autoritzat a accedir als serveis interns de Grup CETT utilitzant usuari + contrasenya d'altres usuaris.

f) Si, en un moment donat, un usuari rebés una trucada telefònica sol·licitant-seu nom d'usuari i contrasenya, mai facilitarà aquestes dades i procedirà a comunicar aquest fet a Servei de STIC, de forma immediata.

Artículo 22. Protecció de dades de caràcter personal i deure de secret

a) La informació continguda en les bases de dades de Grup CETT que comprengui dades de caràcter personal està protegida per la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD).
b) Els fitxers o tractaments de dades de caràcter personal gestionats per Grup CETT han d'adoptar les mesures tècniques i organitzatives de seguretat per garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament, així com les exigències previstes en la normativa vigent.
c) Tot usuari (de Grup CETT o de terceres organitzacions) que, en virtut de la seva activitat professional, pogués tenir accés a dades de caràcter personal, està obligat a guardar secret sobre els mateixos, deure que es mantindrà de manera indefinida, fins i tot més enllà de la relació laboral o professional amb Grup CETT.

Artículo 23. Connexió als sistemes d'informació de forma remota

a) Grup CETT podrà posar a disposició del personal accés remot als sistemes d'informació, sota les següents consideracions:

1. Es requerirà autorització expressa per part de la Gerència.
2. Aquest accés remot es pot realitzar des de qualsevol equip. Està permesa la utilització d'equips personals per a accés remot als sistemes de gestió, però en tot cas és responsabilitat de l'usuari mantenir els seus equips en l'estat adequat per no corrompre la informació dels sistemes de Grup CETT. És d'obligat compliment que l'usuari disposi dels corresponents sistemes de protecció antivirus actualitzats, així com també les últimes actualitzacions dels sistemes operatius dels seus equips personals.
3. Aquest accés remot garanteix els mateixos accessos que té l'usuari accedint des de la LAN.

Artículo 24. Compromisos dels usuaris

a) És responsabilitat directa de l'usuari:
   1. Custodiar les credencials que se li proporcionin i seguir totes les recomanacions de seguretat que elabori el Servei de STIC per garantir que aquelles no puguin ser utilitzades per tercers. Haurà tancar el seu compte en acabar la sessió o bloquejar l'equip quan ho deixi desatès.
   2. En el cas que el seu equip contingui informació sensible, confidencial o protegida, aquesta ha de complir tots els requisits legals aplicables i les mesures de protecció que la normativa de Grup CETT estableixi al respecte.
   3. Garantir la disponibilitat de tota la informació important per a Grup CETT emmagatzemant-la en carpetes assignades en els servidors corresponents.

4. Notificar qualsevol sospita d'un incident de seguretat.

b) A més de l'anterior, no es podrà accedir als recursos informàtics i telemàtics de Grup CETT per desenvolupar activitats que persegueixin o tinguin com a conseqüència:

1. L'ús intensiu de recursos de procés, memòria, emmagatzematge o comunicacions, per a usos no professionals.
2. La degradació dels serveis.
3. La destrucció o modificació no autoritzada de la informació, de manera premeditada.
4. La violació de la intimitat, del secret de les comunicacions i del dret a la protecció de les dades personals.
5. El deteriorament intencionat del treball d'altres persones.
6. L'ús dels sistemes d'informació per a fins aliens als del Grup CETT llevat d'aquelles excepcions que preveu la present política.
7. Danyar intencionadament els recursos informàtics de Grup CETT o d'altres institucions.
8. Incórrer en qualsevol altra activitat il·lícita, del tipus que sigui.

Artículo 25. Baixa d'empleats

a) Quan el responsable dels serveis jurídics i laboral o el responsable immediat de l'usuari, notifica la baixa, des Assistència STIC es reenvia el missatge al cap del departament en qüestió per tal que doni la conformitat per a procedir a donar-lo de baixa a la xarxa.
b) El responsable de l'usuari especificar, en el full de baixa, qualsevol observació a considerar, incloent les especificitats sobre els equips, si aquests s'han de retirar o seran reaprofitats per una nova incorporació.
c) El missatge rebut es guarda en una carpeta de la bústia d'assistència, com a evidència, durant un any a partir de la data de petició de baixa.

d) Per a qualsevol baixa, el responsable de l'usuari determinarà si s'ha d'activar una resposta automàtica o tenir accés a aquest bústia de correu.
e) En cas de baixes per incapacitat temporal o accidents de treball similars, l'usuari haurà d'activar el missatge de resposta automàtica notificant que no es troba disponible, i indicant les dades del mail de la persona a la qual dirigir-se en la seva absència. Per a això disposarà d'un termini de 7 dies naturals i, en cas d'incomplir aquesta obligació, la mateixa organització podrà dur a terme l'activació d'aquesta resposta automàtica a fi a poder seguir prestant el servei als seus clients i grups d'interès.

4.2. Ús i accés a internet

Artículo 26. Generalitats de l'accés a internet

a) Amb caràcter general, els usuaris de Grup CETT disposaran d'accés a Internet com a eina de productivitat i coneixement, per a l'exercici de la seva activitat professional.
b) L'accés corporatiu a Internet és un recurs centralitzat que Grup CETT posa a disposició dels usuaris, com a eina necessària per a l'accés a continguts i recursos d'Internet i com a suport al desenvolupament de la seva activitat professional.
c) Grup CETT 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 riscos de seguretat associats al seu ús.

Artículo 27. Normes generals d'ús i accés a internet

a) Les connexions que es realitzin a Internet han d'obeir a fins professionals, tenint sempre en compte que s'estan utilitzant recursos informàtics restringits i escassos. L'accés a Internet per a fins personals no està permès.

b) Només es podrà accedir a Internet mitjançant el navegador subministrat i configurat per Grup CETT en els llocs d'usuari. No podrà alterar-se la seva configuració ni utilitzar un navegador alternatiu, sense la deguda autorització del Servei de STIC.

c) S'ha de notificar al Servei de STIC qualsevol anomalia detectada en l'ús de l'accés a Internet, així com la sospita de possibles problemes o incidents de seguretat relacionats amb aquest accés.

Artículo 28. Usos específicament prohibits l'ús d'internet

a) La descàrrega d'arxius molt voluminosos, especialment en horaris coincidents amb la jornada laboral, llevat autorització expressa.

b) La descàrrega de programes informàtics sense autorització prèvia o fitxers amb contingut nociu que suposin una font de riscos per a l'organització. En tot cas s'ha d'assegurar que el lloc web visitat és fiable.

c) L'accés a debats en temps real (Xat / IRC) per ser perillós en facilitar la instal·lació d'utilitats que poden permetre accessos no autoritzats al sistema.

d) L'accés a pàgines web (WWW), grups de notícies (*NewsGroups*) i altres fonts d'informació com FTP, etc., que no estiguin relacionades amb l'activitat de Grup CETT o amb les comeses del lloc de treball de l'usuari.

e) 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 un altre tipus de contingut (música, pel·lícules, etc.) que no estigui expressament autoritzada pel servei de STIC.

Artículo 29. Ús acceptable d'internet

a) Amb el desplegament de les TIC i, en particular, amb el desenvolupament d'Internet com a eina de comunicació global, s'han estès igualment les

amenaces que poden posar en perill els sistemes d'informació de les organitzacions.

b) Per tant, per minimitzar els riscos derivats de l'ús d'Internet, resulta necessari adoptar un conjunt mínim de mesures de seguretat dirigides a propiciar el seu correcte ús. Aquestes mesures són:

1. Utilitza Internet per a fins professionals. Internet és una eina més de les utilitzades pels usuaris de Grup CETT. Per això, s'ha d'utilitzar de manera responsable i exclusivament per a fins professionals. Amb les excepcions o precisions que s'assenyalen:

I- No visitar pàgines de contingut poc ètic, ofensiu o il·legal. No està permès l'accés a pàgines el contingut pugui resultar ofensiu o atemptar contra la dignitat humana. Anàlogament, no es permet l'accés a pàgines de contingut no adequat, il·legal o poc ètic.

II- No visitar pàgines no fiables o sospitoses. Per evitar possibles incidents de seguretat, és aconsellable no visitar pàgines que es considerin sospitoses de contenir codi maliciós.

III- Tenir cura de la informació que es publica a Internet. No s'ha de proporcionar informació sobre l'organització en fòrums, xats, etc., ja que podria ser utilitzada de forma fraudulenta. En aquest sentit, està prohibit difondre sense autorització qualsevol tipus d'informació no pública sobre el funcionament intern de Grup CETT, els seus recursos, estructura, etc.

IV- Observar les restriccions legals que siguin d'aplicació. Abans d'utilitzar una informació obtinguda d'Internet, els usuaris hauran de comprovar en quina mesura es troba subjecta als drets derivats de la propietat intel·lectual o industrial.

V- Realitzar descàrregues només si es té autorització. Les descàrregues indiscriminades o sense autorització són un dels orígens més usuals d'infecció per codi maliciós. Encara Grup CETT

decideixi no limitar tècnicament la capacitat per descarregar arxius d'àudio o vídeo, els usuaris hauran de tenir en consideració que la descàrrega d'aquests arxius pot anar en detriment del rendiment dels recursos informàtics i, per això, limitaran la seva descàrrega i reproducció a àmbit estrictament professional.

VI- No descarregar codi o programes no fiables. Cal assegurar la fiabilitat del lloc des del qual es descarreguen els programes, utilitzant sempre les pàgines oficials. A més, cal comprovar si cal l'ús de llicència per utilitzar les aplicacions descarregades. Convé que aquestes activitats siguin escomeses, de manera exclusiva, el Servei de STIC.

VII- Assegurar l'autenticitat de la pàgina visitada. Quan es vagin a realitzar intercanvis d'informació o transaccions és important assegurar que la pàgina que visita és realment la que diu ser. És recomanable accedir a les pàgines escrivint i comprovant la direcció a la barra d'adreces del navegador i no a través de vincles externs. Moltes suplantacions de pàgines web mostren una pàgina que és virtualment idèntica a la pàgina coneguda per l'usuari, fins i tot evidenciant un fals nom a la barra de direccions. Quan la pàgina web es trobi autenticada mitjançant certificat digital, l'usuari ha de verificar la seva autenticitat.

VIII- Comprovar la seguretat de la connexió. En general, la informació transmesa per Internet no circula de manera xifrada. No obstant això, en la transmissió d'informació sensible, confidencial o protegida és important assegurar la seva xifrat. Una manera d'assegurar la confidencialitat és comprovar que s'utilitza protocol HTTPS en la comunicació en comptes del protocol estàndard http (examinant la barra d'adreces). També hauria d'aparèixer una icona representant un cadenat a la barra del navegador. A través d'aquest cadenat es pot obtenir informació sobre el certificat digital d'identitat del lloc web visitat.

IX- Tancar les sessions en acabar la connexió. És molt convenient tancar les sessions en acabar la connexió o l'intercanvi d'informació, ja que en moltes ocasions la connexió roman oberta per defecte i no n'hi ha prou amb tancar el navegador. Això pot fer que altres usuaris tinguin accés als comptes dels usuaris que no haguessin tancat correctament les sessions. La majoria dels llocs web disposen d'una opció de "desconnexió", "logout" o similar que convé utilitzar.

X- Utilitzar eines contra codi perjudicial. El volum de codi nociu que circula en el ciberespai és molt elevat i presenta multitud d'aspectes diferents.

XI- Per tant, cal disposar de l'adequat ventall d'eines que permetin una adequada protecció. L'ús d'un antivirus permanentment actualitzat és la primera de protecció contra aquest tipus d'atacs. A més d'això, cal configurar i usar adequadament tallafocs, programari específic contra programes espia (*spyware*), etc.

XII- Mantenir actualitzat el navegador i les eines de seguretat. És imprescindible actualitzar les eines d'accés a Internet (navegadors) i de seguretat (antivirus, tallafocs, etc.) a les darreres versions estables, sempre de conformitat amb el que indica i aprovat pel Servei de STIC. Ja que el codi nociu es genera incessantment, és molt important actualitzar les definicions de virus amb la major freqüència possible. Els sistemes han d'estar configurats per a realitzar aquesta tasca de forma automàtica. Així mateix, és molt important informar sobre qualsevol problema que es detecti en aquest procés.

XIII- Utilitzar els nivells de seguretat del navegador. Els navegadors web permeten configuracions amb diferents nivells de seguretat. L'idoni és mantenir el nivell de seguretat "alt", i no és recomanable utilitzar nivells per sota de "mig". Això pot fer-se usant les eines disponibles en el navegador.

XIV- Desactivar les galetes. Les *cookies* són petits programes que fan servir els servidors web per a emmagatzemar i recuperar informació sobre els seus visitants. (Per exemple, qui, quan i des d'on s'ha connectat un usuari). Aquests programes s'emmagatzemen a l'ordinador de l'usuari en visitar una pàgina web, podent ser desactivats fent servir les eines disponibles en el navegador.

XV- Eliminar la informació privada. Els navegadors web emmagatzemen informació privada durant la seva utilització, tal com l'historial de navegació, galetes acceptades, contrasenyes, etc.; informació a la qual podria accedir un atacant que s'hagués introduït en el sistema. Per tant, és recomanable esborrar aquesta informació de manera periòdica, usant les eines disponibles en el navegador.

XVI- No instal·lar complements desconeguts. Quan es carreguen certes pàgines web, es mostra un missatge comunicant la necessitat d'instal·lar a l'ordinador de l'usuari un complement (*plug-in*, *add-on*, etc.) per poder accedir al contingut. És molt recomanable analitzar primer la conveniència d'instal·lar tal complement i fer-ho, en qualsevol cas, sempre des de la pàgina del distribuïdor o proveïdor oficial del mateix.

XVII- Limitar i vigilar l'execució d'*Applets* i Scripts. Els scripts són un conjunt d'instruccions que permeten l'automatització de tasques. Els *applets* són petites aplicacions (components d'aplicacions) que s'executen en el context del navegador web. Tot i que, en general, resulten útils, poden ser usats per a executar codi maliciós i, per tant, és recomanable limitar la seva execució.

Artículo 30. propietat intel·lectual

a) Queda estrictament prohibit l'ús de programes informàtics que no estiguin homologats per Grup CETT.
b) Grup CETT es reserva el dret de revisar, sense previ avís, els programaris instal·lats en tots els ordinadors de Grup CETT per tal de comprovar el compliment d'aquestes normes i prevenir activitats que puguin afectar aquest com a responsable civil subsidiària.
c) Queda prohibida la instal·lació de qualsevol programari sense previ avís al Servei de STIC, així com modificar les configuracions locals de l'equip, com ara desactivar l'antivirus, per garantir la seguretat i la continuïtat del servei.
d) El contingut d'internet pot estar subjecte a Propietat Intel·lectual.
e) Cal tenir certa consideració, especialment amb material audiovisual, fotos i vídeos.
f) No utilitzar per a presentacions corporatives, material descarregat d'internet sense conèixer els drets d'ús.
g) En cas de necessitar material visual per les presentacions, posar-se en contacte amb el Departament de Màrqueting i / o Comunicació.
h) En cas de dubte legal sobre un contingut concret, poseu-vos en contacte amb el Departament Regulatori.
i) No reenviar, ni distribuir material de què es desconegui la propietat intel·lectual del mateix.

4.3. Ús de serveis al cloud

Artículo 31. Emmagatzematge d'informació corporativa al cloud

a) L'emmagatzematge d'informació en serveis *cloud*, com ara Dropbox, Google Drive, iCloud Drive, està permès.
b) Si un usuari vol enviar, gravar o allotjar informació de grans dimensions, haurà d'intentar comprimir al màxim els arxius a enviar.

4.4. Ús del correu electrònic

Artículo 32. Generalitats d'ús del correu electrònic

a) El correu electrònic (e-mail) és un servei de xarxa per a permetre als usuaris de Grup CETT enviar i rebre missatges. Juntament amb els missatges també poden ser enviats fitxers adjunts. 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 o que aprofiten les seves vulnerabilitats.
b) El correu electrònic corporatiu és una eina de missatgeria electrònica centralitzada, posada a disposició dels usuaris de Grup CETT, per a l'enviament i recepció de correus electrònics mitjançant l'ús de comptes de correu corporatives.
c) Es tracta d'un recurs compartit per tots els usuaris de l'organització, de manera que un ús indegut del mateix repercuteix de manera directa en el servei ofert a tots.
d) Les normes d'ús del correu electrònic establertes per Grup CETT estan recollides en el FOP.

Artículo 33. Normes generals d'ús del correu electrònic.

a) Tots els usuaris que ho necessitin per a l'exercici de la seva activitat professional disposaran d'un compte de correu electrònic, per a l'enviament i recepció de missatges interns i externs a l'organització.
b) El correu haurà d'utilitzar, únicament i exclusivament, per a la realització de les funcions encomanades al personal, evitant l'ús privat d'aquest.
c) S'haurà de notificar al responsable de Seguretat qualsevol tipus d'anomalia detectada, així com els correus no desitjats (SPAM) que es rebin, seguint el protocol existent de gestió d'incidències com s'indica en el FOP, per tal de configurar adequadament les mesures de seguretat oportunes.

d) S'ha de prestar especial atenció als fitxers adjunts en els correus rebuts. No s'han d'obrir ni executar fitxers de fonts no fiables, ja que podrien contenir virus o codi maliciós. En cas de dubte sobre la fiabilitat d'aquests, s'haurà de notificar aquesta circumstància al responsable de seguretat seguint el protocol existent de gestió d'incidències com s'indica en el FOP.
e) Està terminantment prohibit suplantar la identitat d'un usuari d'internet, correu electrònic o qualsevol altra eina col·laborativa.
f) Recomanacions addicionals:

1. Assegurar que els reenviaments de missatges prèviament rebuts es transmetin únicament als destinataris apropiats.
2. Evitar, en la mesura del possible, l'ús ineficient en els enviaments de correu: agrupar els enviaments a múltiples destinataris en un sol missatge, evitar la incorporació de signatures escanejades, imatges i fons com a format habitual dels correus (ja que incrementen innecessàriament la mida i volum d'aquests), enviaments innecessaris, etc.

g) Les bústies de correu es configuren amb una mida per a emmagatzematge limitat i finit. El sistema indicarà quan es troba al límit de la seva capacitat, després del qual no es permetrà enviar i rebre correus.
h) Usos especialment prohibits del correu electrònic:

3. L'enviament de correus electrònics amb contingut inadequat, il·legal, ofensiu, difamatori, inapropiat o discriminatori per raó de sexe, raça, edat, discapacitat, que continguin programes informàtics (programari) sense llicència, que vulnerin els drets de propietat intel·lectual dels mateixos, d'alerta de virus falsos o difusió de virus reals i codi maliciós, o qualsevol altre tipus de continguts que puguin perjudicar els usuaris, identitat i imatge corporativa i als propis sistemes d'informació de l'organització.

4. Enviaments de correus de multidifusió tipus "SPAM" o comunicacions fraudulentes des dels comptes corporatives de Grup CETT (@cett.cat) que puguin originar danys d'imatge al grup.
5. L'accés a una bústia de correu electrònic diferent de la pròpia i l'enviament de correus electrònics amb usuaris diferents del propi.
6. La difusió del compte de correu de l'usuari en llistes de distribució, fòrums, serveis de notícies, etc., que no siguin conseqüència de l'activitat professional de l'usuari.
7. Respondre missatges dels que es tingui sospites sobre la seva autenticitat, fiabilitat i contingut, o missatges que continguin publicitat no desitjada.
8. La utilització del correu com a mitjà d'intercanvi de fitxers especialment voluminosos sense autorització, i l'enviament d'informació sensible, confidencial o protegida. El sistema evitarà l'intercanvi de correus de mides superiors als límits establerts pel Servei de STIC, llevat d'excepcions autoritzades.
9. La utilització del correu per recollir correu de bústies que no pertanyin al Grup CETT o el reenviament automàtic del correu a bústies aliens a l'organització.
10. Reenviar fitxers adjunts innecessaris que puguin provocar el col·lapse dels sistemes de comunicació per tràfic innecessari.
11. No està permès l'enviament d'informació "classificada" a través del correu electrònic corporatiu.

Artículo 34. Ús acceptable del correu electrònic

a) Per fer un ús adequat del correu s'inclou un conjunt de normes que tenen com a objectiu reduir el risc en el seu ús:

1. Utilitzar el correu electrònic exclusivament per a propòsits professionals. Gran part dels missatges de correu electrònic no

desitjats que arriben a les organitzacions tenen el seu origen en un ús no professional dels comptes de correu. Utilitzar el correu electrònic únicament per a fins professionals redueix la possibilitat d'atac.

2. Utilitza contrasenyes segures.
3. No cedir l'ús dels comptes de correu. Els comptes de correu són personals i intransferibles. Excepte en casos puntuals -per als que haurà de sol·licitar i obtenir la corresponent autorització-, no s'ha de cedir l'ús del compte de correu a terceres persones, el que podria provocar una suplantació d'identitat i l'accés a informació confidencial. A més d'això, és convenient controlar la difusió dels comptes de correu, facilitant la direcció professional només en els casos necessaris.
4. Revisar la barra d'adreces abans d'enviar un missatge. L'enviament d'informació a destinataris erronis pot suposar una bretxa en la confidencialitat de la informació. Quan es respon a un missatge és important revisar les adreces que apareixen en el camp Amb Còpia (CC). A més, han d'esborrar totes les adreces que poguessin aparèixer en el correu enviat amb anterioritat i que apareguin reflectides en el nou correu reenviat o respost.
5. No s'han d'enviar o reenviar correus de forma massiva. Si s'envia per necessitat un correu a un conjunt de destinataris, convé utilitzar una llista de distribució o, si no, col·locar la llista d'adreces en el camp de còpia oculta (CCO o BCC), evitant la seva visibilitat a tots els receptors del missatge.
6. No enviar missatges en cadena. Les alarmes de virus i les cadenes de missatges són, en moltes ocasions, correus simulats, que pretenen saturar els servidors i la xarxa. En cas de rebre un missatge en cadena alertant d'un virus, s'ha de notificar la incidència al Servei de STIC.
7. No respondre a missatges de SPAM. La major part dels generadors de missatges de correu brossa (correu electrònic massiu no sol·licitat) s'envien a adreces de correu electrònic aleatòriament generades,

esperant que les respostes obtingudes confirmin l'existència d'adreces de comptes reals. A més d'això, de vegades tenen l'aspecte de missatges legítims i, fins i tot, poden contenir informació relativa a Grup CETT. En qualsevol cas, mai s'ha de respondre als mateixos.

8. Assegurar la identitat del remitent abans d'obrir un missatge. Molts ciberatacs s'originen quan l'atacant es fa passar per una persona o entitat coneguda (amic, company, etc.) de l'usuari atacat. L'origen d'aquestes accions és divers: accés no autoritzat al compte, suplantació visual de la identitat, introducció de codi maliciós que utilitza el compte remitent per propagar-se, etc. En cas de rebre un correu sospitós, i depenent de la seva versemblança, cal:

   I- Ignorar-, no obrir-lo i posar el fet en coneixement del remitent, independentment de comunicar la incidència de seguretat corresponent. Igualment, l'enviament d'informació sensible, confidencial o protegida a petició d'un correu del qual no es pot assegurar la identitat del remitent ha de rebutjar-se.

   II- És important tenir en compte que resulta molt senzill enviar un correu amb un remitent fals. Mai s'ha de confiar que la persona amb la qual ens comuniquem via email sigui qui diu ser, excepte en aquells casos que s'utilitzin mecanismes de signatura electrònica dels correus (no només dels fitxers adjunts).

9. Utilitzar eines d'anàlisi contra codi perjudicial. La utilització d'eines com ara antivirus i tallafocs ajuda a detectar el codi maliciós ja mitigar-ne els efectes. Per això, s'ha de configurar l'antivirus amb l'opció d'analitzar el correu electrònic entrant.
10. No obrir correus brossa ni correus sospitosos. Tot i que un missatge no desitjat hagués traspassat el filtre contra robots de correu, no s'ha d'obrir, havent de reportar el corresponent incident de seguretat. És

convenient esborrar els correus sospitosos o, almenys, situar-los (sense obrir) en una zona de quarantena.

11. No executar arxius adjunts sospitosos. No s'han d'executar els arxius adjunts rebuts sense analitzar-prèviament amb l'eina corporativa contra codi maliciós. Això és especialment important quan es reben adjunts no sol·licitats o el correu és sospitós. Gran part del codi maliciós sol inserir-se en fitxers adjunts, ja sigui en forma d'executables (.exe, per exemple) o en forma de macros d'aplicacions (Word, Excel, etc.).
12. Informar de correus amb virus, sense reenviar. Si l'usuari detectés que un correu conté un virus o, en general, codi maliciós, cal notificar l'incident de seguretat a Manteniment STIC i no reenviar-lo, per evitar la seva possible propagació.
13. No utilitzar el correu electrònic com a espai d'emmagatzematge. La capacitat d'espai en els servidors de correu de Grup CETT és limitada. Quan un compte es satura pot ser que es restringeixin per part del servidor els privilegis d'enviament i / o recepció de missatges o que es realitzi un esborrat, més o menys selectiu, dels missatges emmagatzemats. Per tot això, es recomana conservar únicament els missatges imprescindibles i revisar periòdicament aquells que hagueren quedat obsolets.
14. En relació amb l'accés remot (via web) al correu electrònic, s'han d'adoptar les següents cauteles:

    I- Els navegadors utilitzats per accedir al correu via web han d'estar permanentment actualitzats a la seva última versió, almenys pel que fa a pegats de seguretat, així com correctament configurats.

    II- Un cop finalitzada la sessió web, és obligatòria la desconnexió amb el servidor mitjançant un procés que elimini la possibilitat de reutilització de la sessió tancada.

III- Desactivar la interpretació de continguts remots a l'hora de llegir missatges de correu via *webmail*.

IV- Desactivar les característiques de recordar contrasenyes per al navegador.

V- Activa l'opció d'esborrat automàtic al tancament del navegador, de la informació sensible registrada pel mateix: històric de navegació, descàrregues, formularis, memòria cau, galetes, contrasenyes, sessions autenticades, etc.

Artículo 35. Prevenció contra SPAM

a) El terme SPAM es defineix com l'enviament de correus no sol·licitats, de forma massiva, a adreces de correu electrònic, constituint un dels problemes de seguretat més habituals amb què s'enfronten les organitzacions. Tals missatges poden contenir codi nociu que, de penetrar en els sistemes d'informació, podrien arribar a colonitzar una institució i propagar-se a través de les xarxes de comunicacions.

b) A més de les mesures tècniques de prevenció i eliminació de SPAM ja instal·lades en Grup CETT a través del Servei de STIC, es detallen tot seguit les normes que tot usuari haurà de seguir per fer front a aquest problema:

1. Amb caràcter general, només es proporcionarà l'adreça de correu electrònic professional de Grup CETT a persones de confiança i de l'entorn professional.
2. S'ha d'evitar introduir l'adreça de correu de Grup CETT en fòrums de notícies o llistes de correu a través d'Internet o xarxes socials, excepte en els casos necessaris i amb proveïdors de confiança. Molts atacs de SPAM es serveixen d'aquestes adreces, introduïdes en llocs no segurs.
3. Amb caràcter general, si no es coneix el remitent d'un correu, i / o l'assumpte d'aquest és estrany, es recomana esborrar el missatge (o

situar-lo en quarantena fins a disposar de més dades), especialment si conté fitxers adjunts.

c) Grup CETT disposa de sistemes antiSPAM per a la detecció i esborrat de missatges identificats com a correu brossa. No obstant això, és possible que aquests sistemes no puguin eliminar la totalitat d'aquests missatges. Per aquest motiu, si l'usuari rep un missatge de SPAM, ha de:

4. Si ho reconegués com a tal per la direcció o l'assumpte que conté, la qual esborrarà immediatament (sense obrir-lo).
5. No respondrà mai.
6. No accedirà als enllaços o annexos que poguessin contenir.
7. Comunicar al Servei de STIC immediatament.

4.5. BYOD (Bring your Own Device) ús de dispositius personals

NOTA IMPORTANT: el punt 4.5 d'aquesta norma només s'aplica a dispositius personals, no propietat de Grup CETT.

Artículo 36. aspectes generals

a) Grup CETT contempla la possibilitat que es emmagatzemi o custodiï informació corporativa en dispositius personals, això inclou l'ús del correu electrònic corporatiu.
b) Està permesa la utilització d'equips personals per a accés remot als sistemes de gestió, però en tot cas és responsabilitat de l'usuari mantenir els seus equips en l'estat adequat per no corrompre la informació dels sistemes del Grup CETT.
c) Els usuaris poden disposar de sincronització de correu i agenda al mòbil prèvia autorització del responsable de seguretat.

d) És d'obligat compliment que l'usuari disposi dels corresponents sistemes de protecció antivirus actualitzats, així com també les últimes actualitzacions dels sistemes operatius dels seus equips personals.
e) No està permès entrar com a usuari a la xarxa a través de dispositius personals. L'accés als serveis compartits de la xarxa s'haurà de realitzar des de la xarxa *WiFi* Grup CETT.

Artículo 37. reemborsament

a) Grup CETT no reemborsarà ni contribuirà al cost del dispositiu personal a l'empleat, excepte en casos excepcionals determinats per Gerència del Grup i Direcció General.
b) Els dispositius utilitzats pels empleats de Grup CETT poden ser personals. Grup CETT només ofereix cobertura sobre les línies corporatives.

Artículo 38. Ús Acceptable de dispositius personals

a) En l'ús de dispositius personals, Grup CETT estableix en el seu codi ètic no dedicar més temps de l'imprescindible a temes personals durant la jornada laboral.

Artículo 39. Dispositius i Suport

a) Grup CETT proporcionarà suport tècnic als dispositius personals només de forma correctiva.

4.6. Ús de xarxes socials

Artículo 40. Declaració d'ús de xarxes socials

a) Aquesta secció de la instrucció tècnica té l'objectiu d'ajudar el personal a prendre les decisions adequades sobre l'ús de social, mitjans de comunicació com els blogs, wikis, llocs web de xarxes socials, podcasts,

fòrums, missatges, taules, o comentaris (per exemple, a Twitter, Facebook, LinkedIn, Instagram i qualsevol altra xarxa social) tant a nivell professional com personal en relació o amb referències a la seva activitat professional.

Artículo 41. Ús de les Xarxes Socials en nom de Grup CETT

a) Només Grup CETT està autoritzat a publicar material en una xarxa social en nom del Grup CETT. Qualsevol incompliment d'aquesta restricció es constituiria en una falta que serà analitzada per prendre les mesures pertinents.

Artículo 42. Ús de les Xarxes Socials en el lloc de treball

a) Grup CETT reconeix la importància d'Internet en la conformació del pensament públic sobre la pròpia organització, els seus serveis, empleats, socis i clients. També es reconeix la Direcció a través de la interacció en xarxes socials.
b) Abans d'utilitzar les xarxes socials en el lloc de treball s'ha de:

1. Llegir i entendre la present instrucció.
2. L'accés a les xarxes socials és obert ja que representen, en molts casos, una eina més de treball, de manera que estarà dins de les funcions de l'usuari, establertes pel seu responsable, qui determinarà el seu ús.

Artículo 43. Ús personal de les Xarxes Socials

a) L'ús de xarxes socials per a l'ús personal està subjecte a certes condicions que figuren a continuació:

1. Es realitzarà substancialment fora de les hores normals de treball.
2. L'ús no ha d'interferir amb els compromisos de Grup CETT.
3. L'ús ha de complir amb la resta de les polítiques corporatives.

4. S'ha de restringir la publicació de dades relacionades amb el seu lloc de treball, més enllà del que és purament descriptiu.
5. No es divulgarà cap tipus d'informació relacionada ni amb Grup CETT ni amb el seu lloc de treball. Tampoc es podrà divulgar ni a títol curricular informació classificada propietat de Grup CETT.

Artículo 44. Regles per a l'ús de xarxes socials (personal i professional)

a) Cada vegada que es faci ús de mitjans de comunicació social, d'acord amb aquesta política, s'ha de adherir a les regles generals següents:

1. Escriu sempre en primera persona, identifiqui la seva identitat i quin és el seu paper, i faci ús del següent establiment de responsabilitat "Les opinions expressades són meves i no reflecteixen el punt de vista de Grup CETT".
2. Cada persona és responsable pel contingut que publica en els mitjans socials.
3. No pujar, enviar o reenviar un enllaç a qualsevol, abusiu, obscè, discriminatori assetjador, difamatori o de contingut despectiu.
4. Qualsevol membre del personal que sent que ha estat assetjat, intimidat o ofès pel material publicat o pujat per un company en un lloc web de mitjans socials, ha d'informar el responsable de seguretat.
5. Mai reveli informació confidencial.
6. Està prohibit pujar, publicar o transmetre qualsevol contingut que pertanyi a Grup CETT oa un tercer, o subjecte a Propietat Intel·lectual llevat que tingui el seu consentiment.
7. Abans d'incloure un enllaç a un lloc web de tercers, comproveu que tots els termes i condicions del lloc web li permeten enllaçar amb ell. Tots els enllaços s'han de fer de manera que l'usuari conegui que es tracta d'un enllaç a tercers.

8. En fer ús de qualsevol plataforma de mitjans socials s'ha de llegir i complir amb les seves condicions d'ús.
9. Si se sent una mica incòmode per alguna cosa que està a punt de publicar, no ha de fer-ho. En cas de dubte, s'ha de comentar amb el responsable de seguretat.
10. No parli dels seus companys, competidors, clients o proveïdors sense la seva prèvia aprovació.
11. Tingueu sempre en compte la privacitat dels altres i eviti els temes que poden acabar en discussions ideològiques (política, religió, etc.)
12. Eviteu publicar les seves dades de contacte de manera que siguin visibles per a gent que no tenia la intenció de veure'ls.
13. No utilitzeu per al registre a xarxes socials oa pàgines web de qualsevol índole l'adreça de correu corporatiu de Grup CETT.
14. Abans de fer la primera contribució a qualsevol lloc de xarxes socials, s'ha d'observar l'activitat en el lloc durant un temps.
15. Si s'observa qualsevol contingut publicat en les xarxes socials sobre Grup CETT (ja sigui complementari o crític), s'ha d'informar d'això al responsable de seguretat.

Artículo 45. Monitorització de les Xarxes Socials

a) El personal ha de ser conscient que qualsevol ús de les xarxes socials des de les xarxes corporatives (siguin o no per motius de treball) es pot monitoritzar i, si s'evidencien infraccions d'incompliment d'aquesta política, la situació es tractarà de manera personal i en funció del context, s'analitzarà i es prendran les mesures adequades per part del responsable immediat i Direcció.
b) Grup CETT té el dret de limitar o impedir l'accés a determinats llocs web de mitjans socials.
c) En particular, la pujada o reenviament d'un enllaç a qualsevol dels següents tipus de material en un lloc web de mitjans socials, ja sigui en ús

professional o personal, ascendirà a una falta (aquesta llista no és exhaustiva):

1. Material pornogràfic.
2. Una declaració falsa i difamatòria sobre una persona o organització.
3. Material que sigui ofensiu, obscè, criminal discriminatori, despectiu per Grup CETT, els seus clients i el seu personal.
4. La informació confidencial sobre Grup CETT o qualsevol dels seus empleats o clients.
5. La informació de caràcter personal, segons el que estableix el Reial Decret 3/2018.
6. Qualsevol altra declaració que pugui crear qualsevol responsabilitat (ja sigui penal o civil).
7. Material que violi els drets d'autor o altres drets de propietat intel·lectual, o que envaeixi la privacitat de qualsevol tercer.

4.7. Auditoria i control

Artículo 46. Monitorització de sistemes d'informació

a) Per verificació i monitorització, les dades de connexió i tràfic es guardaran en un registre durant el temps que estableixi la normativa vigent en cada supòsit. En cap cas aquesta retenció de dades afectarà el secret de les comunicacions.
b) L'ús d'Internet, del correu electrònic i l'accés a la resta dels serveis i sistemes de Grup CETT estarà degudament controlat per a tots els usuaris. Si es fes un ús abusiu o inadequat d'aquests serveis, Grup CETT analitzarà cada cas de forma personal i en funció del context per part del responsable immediat i s'adoptaran les mesures pertinents en funció del cas.

c) Grup CETT 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, i així com es detalla en el FOP:

1. Ha de revisar periòdicament l'estat dels equips, el programari instal·lat, els dispositius i xarxes de comunicacions de la seva responsabilitat.
2. Monitoritzarà els accessos a la informació continguda en els seus sistemes.
3. Auditarà la seguretat de les credencials i aplicacions.
4. Monitoritzarà els serveis d'internet, correu electrònic i altres eines de col·laboració, de forma aleatòria i en el moment de realitzar manteniment preventiu.

d) La informació recollida d'aquestes monitoritzacions per part de l'equip de manteniment que pugui considerar anòmala es reporta exclusivament a Gerència, des d'on es determinen les accions a realitzar.

e) Els sistemes en què es detecti un ús inadequat o en què no es compleixin els requisits mínims de seguretat, s'ha de prendre una decisió particular en funció del cas per part del responsable immediat i Direcció.

f) 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 els quals es detecti algun problema de seguretat o d'incompliment de la present política.

g) 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 les que s'ha accedit, així com del temps d'accés, volum i grandària dels arxius descarregats.

4.8. Incompliment de la norma

Artículo 47. Ús abusiu dels sistemes d'informació.

a) Amb caràcter general, s'enumeren tot seguit un conjunt d'accions que es consideren ús abusiu dels sistemes d'informació de Grup CETT.

b) Ús abusiu de l'accés a internet:

1. Accés a altres xarxes, amb el propòsit de violar la seva integritat o seguretat.
2. Accés a continguts no relacionats amb les comeses professionals de l'usuari, com ara:

I- Accedir, recuperar o visualitzar textos o gràfics que excedeixin els límits de l'ètica.

II- Utilitzar l'accés a Internet per a l'ús de missatgeria instantània (Messenger, Skype, etc.).

III- Transferència de fitxers no relativa a les activitats professionals de l'usuari (com ara jocs, fitxers de so, fotos, vídeos o pel·lícules, etc.).

IV- Realitzar qualsevol activitat de promoció d'interessos personals.

3. Publicació o enviament d'informació no sol·licitada.
4. Publicació o enviament d'informació sensible, confidencial, protegida o propietat del Grup CETT a persones, empreses o sistemes d'informació externs no autoritzats. En aquest sentit, els usuaris es comprometen a garantir la privacitat d'aquestes dades i contrasenyes d'accés, així com a evitar la difusió d'aquests.
5. Publicació o enviament de missatges a través d'Internet que continguin amenaces, ofenses o imputació de fets que puguin lesionar la dignitat personal i, en general, la utilització del servei d'Internet de manera il·legal o infringint qualsevol norma interna que pugui ser aplicable.

6. Ús d'Internet per a propòsits que puguin influir negativament en la imatge del Grup CETT, dels seus representants o dels organismes públics o privats amb els quals es manté relació.

c) Ús abusiu del correu electrònic:

7. Utilitzar el correu electrònic per a fins diferents dels derivats de les activitats professionals de l'usuari, especialment:

   I- Intercanviar continguts (textos o gràfics) que excedeixin els límits de l'ètica.
   II- Transferència de fitxers aliena a les activitats professionals de l'usuari (per exemple: programari sense llicència, fitxers de so, fotos i vídeos, gràfics, virus, codi maliciós, etc.).
   III- Realitzar qualsevol activitat de promoció d'interessos personals.
   IV- Utilitza qualsevol compte de correu de Grup CETT per enviar missatges o cartes en cadena i / o correus brossa o SPAM (correu electrònic no sol·licitat).
   V- Utilitza qualsevol compte de correu de Grup CETT per enviar missatges que continguin amenaces, ofenses o imputació de fets que puguin lesionar la dignitat personal i, en general, la utilització del correu electrònic de manera il·legal o infringint qualsevol norma que pugui ser aplicable.

8. Revelar a tercers el contingut de qualsevol dada reservat o confidencial propietat de Grup CETT o de tercers, llevat que tal actuació fos realitzada en compliment de fins estrictament professionals amb el previ consentiment dels afectats.
9. Utilitzar-lo per propòsits que puguin influir negativament en la imatge de Grup CETT, dels seus representants o dels organismes públics o privats amb els quals es manté relació.

d) Ús abusiu d'altres serveis i sistemes de Grup CETT:

10. Accés a serveis i / o continguts de Grup CETT amb el propòsit de violar la seva integritat o seguretat.
11. De forma general, realitzar activitats no relacionades amb les tasques professionals de l'usuari, com ara:

    I- Accedir, recuperar, o visualitzar textos o gràfics que excedeixin els límits de l'ètica.
    II- Emmagatzemar arxius personals a l'estació de treball o en els servidors de Grup CETT.
    III- L'ús de missatgeria instantània (Messenger, Skype, etc.).
    IV- Transferència de fitxers entre usuaris de Grup CETT no relativa a les activitats professionals.

12. Comunicació a tercers del contingut de qualsevol dada reservat o confidencial propietat de Grup CETT o de tercers, llevat que tal actuació fos realitzada en compliment de fins estrictament professionals amb el previ consentiment dels afectats.
13. Les accions realitzades des d'un compte d'usuari o des d'un compte de correu electrònic d'usuari són responsabilitat del seu titular.

Grup CETT implantarà els sistemes de protecció d'accés als sistemes que consideri necessari, per evitar que es produeixin incidents relacionats amb l'abús d'aquests serveis.

Artículo 48. Incompliment de la política

a) Tots els usuaris de Grup CETT estan obligats a complir el que prescriu la present Política d'usos de Sistemes d'Informació i Recursos Informàtics.

b) En el cas que un usuari no observi alguna dels preceptes assenyalats en la present política, serà tractada per part del responsable immediat i es prendran les mesures oportunes depenent del cas.

4.9. Acta de Compromís

Artículo 49. Acceptació d'un recurs

a) En l'acceptació d'un recurs de tractament de la informació (PC, tableta, *Smartphone*, USB, ...) l'usuari:

1. Accepta el coneixement d'aquesta política,
2. Es responsabilitza del compliment de la política i norma establerta.

4.10. Divulgació de polítiques

Artículo 50. Comunicació i divulgació de les polítiques

a) Al moment d'incorporar-se al seu lloc de treball, tots els usuaris:

1. Rebran un manual d'acollida en què es troba recollida tota la informació relacionada amb les polítiques i normes establertes pel Grup CETT per al resguard i protecció dels seus recursos informàtics i les dades.
2. Les persones contractades, en signar el contracte, estan donant per conegudes les normes d'ús a través del manual d'acollida.

b) Per als usuaris que formen part de Grup CETT:

3. Es realitzaran, bianualment, cursos en línia de formació i conscienciació dels usuaris sobre les polítiques i normatives establertes pel Grup CETT per al resguard i protecció dels seus recursos i dades.
4. Aquests cursos seran gestionats pel responsable dels Serveis Jurídics i el responsable de seguretat.
5. Els cursos estaran dirigits als responsables de gestió de la informació.

6. A través del campus virtual es disposarà de les corresponents evidències dels cursos realitzats per cada usuari.

5. COMPLIMENT DE LA POLÍTICA

Aquesta política és d'obligatori compliment per a tots els membres del Grup CETT, així com per aquells socis de negoci als quals els sigui la mateixa d'aplicació, la qual forma part del sistema de gestió de Compliance penal de l'Organització. L'incompliment de la present política podrà ser objecte de sanció disciplinària.

6. NOTIFICACIÓ DE LA POLÍTICA

La Direcció establirà un Acta de Compromís que signaran tots els usuaris al moment de rebre la present política.