1 Polítiques de bones pràctiques de Seguretat de la Informació en la SMAP

A continuació es plantegen una sèrie de recomanacions que pretenen regular el bon ús, disponibilitat i nivell de servei dels recursos informàtics de **SMAP**. Aquelles persones que de forma reiterada o deliberada o per negligència les ignorin o les infringeixin, es podran veure subjectes a les actuacions tècniques (per minimitzar els efectes de la incidència) o disciplinàries que s'estimin oportunes.

1.1 Procés d'autorització de recursos per al tractament de la informació

Qualsevol persona que necessiti un nou ordinador, portàtil, software de gestió, etc. haurà de remetre la sol·licitud a l'**IMI** mitjançant el correu electrònic, indicant clarament el motiu o necessitat de la compra. Aquesta sol·licitud recaurà al responsable directe de l'usuari demandant i en cap cas es procedirà a la compra o distribució del dispositiu en qüestió sense la corresponent autorització. Finalment, el responsable de IT de l'**IMI** acceptarà, denegarà o remetrà al comitè de direcció la petició.

1.2 Ús acceptable dels actius

Internet

- L'accés a Internet està limitat a les URL's i IP's que prèviament hagin estat autoritzades pel **IMI**.
- No està permès l'ús de comunicació interactiva com a xats, BBS o ICQ entre uns altres,
- No es permet l'ús de sistemes de cerca i descarrega de música, vídeos o arxius comercials amb drets reservats com per exemple: kazaa, e-mule, napster, Imesh, etc..
- L'usuari és conscient que SMAP no pot conèixer el contingut de la informació que circula a través de la seva xarxa i, per tant, eximeix a l'organització de tota responsabilitat en relació amb el contingut dels missatges transmesos a través d'aquesta.
- Els usuaris no disposen de privilegis per a la instal·lació de software.
- No es permet accedir a pàgines d'Internet on es consumeixi ample de banda (streaming), tals com spotify o reproductors de música online.

1.3 Extracció de pertinences

Els equips y el software no es poden treure fora de las instal·lacions. Per realitzar reparacions els tècnics es desplacen a la ubicació de l'equip avariat.
No es pot extreure informació propi de la SMAP fora de les oficines o en dispositius de memoria externa sense l'autorització pertinent.

1.4 Drets de propietat intel·lectual (IPR)

- Els usuaris i administradors han de respectar les condicions de llicència i copyright del software instal·lat en els seus equips.
- Tot software adquirit de forma central per la **SMAP** haurà de tenir la corresponent llicencia d'us.
- Tot software que s'usi en **SMAP** per a finalitats administratives o comercials ha d'estar degudament llicenciat, amb un nombre de llicències que es correspongui amb el nombre d'usuaris simultanis. Per descomptat, podrà usar-se en equips de la SMAP el software

"lliure" que l'**IMI** tingui inventariat com a software autoritzat per a descarrega tals com Open source, freeware, etc.

- Tot software que s'usi que estigui protegit per Copyrights no pot ser copiat, excepte amb autorització del propietari. No es podran usar els mitjans que **SMAP** posa a la disposició de la seva comunitat per copiar software protegit o trencar les proteccions del mateix.
- A part del software, tota una altra informació que també posseeixi drets d'autor, que estigui en format electrònic i que hagi estat obtinguda d'un altre equip o xarxa, s'ha d'usar d'acord amb la legislació vigent.
- Els usuaris respondran sempre personalment del software que hagi instal·lat en els seus equips, així com de l'ús que del mateix s'efectuï, i hauran de complir amb les obligacions i requisits que es derivin de la seva instal·lació i utilització.
- En cap cas els usuaris podran permetre que cap persona dugui a terme la instal·lació en els seus equips de software que no estigui degudament llicenciat.
- L'**IMI** no es farà responsable de les peticions d'instal·lació de software que es sol·licitin per part dels treballadors.

1.5 Controls contra el codi maliciós

Està instal·lat en els servidors un software detector de codi maliciós. S'executa un control de detecció com a mínim una vegada per setmana.
El procés setmanal no es podrà aturar durant l'execució del mateix ja que es d'obligada execució.

1.6 Correu electrònic i Enviament de missatges

Qualsevol empleat que ho hagi sol·licitat al **IMI** i se li hagi aprovat disposa d'un compte de correu electrònic activa, protegida amb codi d'usuari i contrasenya la qual pot utilitzar des dels diversos equips destinats per a això.

És responsabilitat del treballador fer bon ús del seu compte, entenent per bon ús:

- L'ús del seu compte amb finalitats comercials o de producció d'interès per SMAP.
- Llegir diàriament el seu correu i esborrar aquells missatges obsolets, per alliberar espai en la seva bústia de correu.
- L'ús d'un llenguatge apropiat en les seves comunicacions.
- El respectar les regles de "Conducta Internet" per a les comunicacions.
- No permetre que segones persones facin ús del seu compte

Està estrictament prohibit:

- L'ús del compte per a finalitats personals.
- Enviar o contestar cadenes de correu.
- Obrir correu amb arxius adjunts sospitosos.
- Enviar SPAMS d'informació (correu brossa), o enviar annexos (attachments) que poguessin contenir informació nociva per a un altre usuari com a virus o pornografia.

Cada persona és responsable de recolzar els seus correus en el seu equip personal o en defecte d'això en carpetes en el seu compte en el servidor de correu.

El seu compte en els servidors té un límit de 25 megabytes d'espai per a correu. Si excedeix aquest límit, tot nou correu serà automàticament rebutjat.

1.7 Sistemes d'informació offline.

El correu ordinari solament podrà ser rebut pel personal d'administració, qui ho distribuirà sense obrir a la persona a la qual vagi indicada.

Les transmissions de fax rebudes es lliuraran immediatament al destinatari pel personal d'administració autoritzat.

1.8 Política de lloc de treball lliure i pantalla neta

Els llocs de treball estan protegits amb un bloqueig automàtic de la pantalla controlat per contrasenya.

No es permet deixar l'espai de treball sense haver bloquejat el PC prèviament.

La informació en paper quan no s'utilitza estarà guardada en armaris tancats amb clau.

Els dispositius de fax i copiadores estan controlats pel responsable de l'àrea. Els documents que s'imprimeixen o copien en ells són immediatament lliurats als seus destinataris.

1.9 Política d'ús dels serveis de xarxa

Els usuaris solament disposen d'accés a les carpetes compartides en les quals tenen permisos assignats, prèviament autoritzats pel **IMI**.
La informació que es troba en carpetes d'ús compartit es personal i intransferible.
No es permet fer un ús personal d'emmagatzematge d'informació personal.

1.10 Sistema de gestió de contrasenyes

Les contrasenyes ofereixen un mitjà de validar la identitat de cada usuari, podent així establir els drets d'accés als recursos o serveis de tractament de la informació.

Tots els usuaris es comprometen a:

- Mantenir la confidencialitat de las contrasenyes.
- Evitar l'escriptura de les contrasenyes en paper.
- Canviar les contrasenyes si es té algun indici de la seva vulnerabilitat o de la del sistema;
- Seleccionar contrasenyes de bona qualitat, amb una longitud mínima de 6 caràcters incloent nombres, que siguin:
  - Fàcils de recordar.
  - No estiguin basades en alguna cosa que qualsevol pugui endevinar o obtenir usant informació relacionada amb l' usuari, por exemple, noms, dates de naixements, números de telèfon, etc.
  - No tinguin caràcters consecutius repetits o que siguin tots nombres o totes lletres
- Canviar les contrasenyes a intervals de temps regulars o en proporció al nombre d'accessos (les contrasenyes de les comptes amb privilegis especials haurien de canviar-se amb més freqüència que les normals), evitant utilitzar contrasenyes antigues o cícliques. L'**IMI** programa periòdicament uns canvis de contrasenyes obligatoris per a tots els usuaris.

- Canviar les contrasenyes temporals assignades inicialment, la primera vegada que s'accedeixi al sistema;
- No incloure contrasenyes en cap procediment automàtic de connexió, que, per exemple, les emmagatzemi en una macro;
- No compartir contrasenyes d'usuari individuals
- No apuntar contrasenyes en dispositius mòbils, agendes, etc..

1.11 Comunicacions mòbils

Els únics dispositius mòbils són els terminals de telefonia i no contenen cap tipus d'informació crítica de l'empresa.
El seu ús es personal i no es pot emprar per accions comercials o personals aliens a la SMAP.

1.12 Teletreball

Cap treballador disposa de l'opció del teletreball.