# FUNCIONS I OBLIGACIONS DEL PERSONAL

# EN MATERIA DE PROTECCIO DE DADES PERSONALS

OBJECTE.-

Amb l'objecte de donar degut compliment al que estableix l'art. 89 del Reial Decret 1720/2007, de 21 de desembre, **CENTRE INTERNACIONAL DE MÉTODES NUMÉRICS EN ENGINYERÍA,** d'ara endavant **CIMNE,** exigeix també al seu personal el compliment de les següents obligacions que hauran de ser conegudes, acceptades i respectades per tot el personal.

ABAST.-

Aquest procediment és d'aplicació a cadascuna de les persones amb accés als fitxers de **CIMNE** amb dades de caràcter personal de l'entitat i dels clients de l'entitat i els sistemes d'informació que els continguin. Les funcions i obligacions definides en el present Document són únicament les que fan referència a la **Gestió del Sistema de Seguretat dels Fitxers amb Dades de Caràcter Personal**, amb independència d'un altre tipus de funcions i obligacions establertes per **CIMNE**.

REALITZACIÓ.-

Les funcions i obligacions del personal amb accés a fitxers amb Dades de Caràcter Personal són les següents:

## FUNCIONS I OBLIGACIONS RELATIVES AL LLOC DE TREBALL.

L'usuari està obligat a utilitzar el seu ordinador i les seves dades sense incórrer en activitats que puguin ser considerades il·lícites o il·legals, que infringeixin els drets de **CIMNE** o de tercers, o que puguin atemptar contra la moral o les normes de seguretat del present procediment de seguretat de la informació de caràcter personal.

Els llocs de treball estaran sota la responsabilitat de l'usuari que ha de garantir que la informació que es mostra no pot ser visible per persones no autoritzades.
Quan el responsable d'un lloc de treball l'abandoni, haurà de deixar-lo de manera que impedeixi la visualització de les dades protegides. Per a això, en finalitzar la jornada o en pauses en el seu treball, l'usuari haurà de deixar l'ordenador de manera que sigui necessari identificar-se i autenticar-se davant del sistema.
En el cas de les impressores haurà d'assegurar-se que no quedin documents impresos que continguin dades de caràcter personal o de qualsevol altre tipus accessibles a persones no autoritzades.

Tot usuari que realitzi una còpia de qualsevol informació susceptible de contenir dades de caràcter personal o de qualsevol altre tipus que hagi estat establert com a confidencial, haurà de sol·licitar l'autorització o posar en coneixement del responsable del fitxer si així està contemplat en el seu treball diari, que s'ha realitzat tal còpia, les dades que conté i la finalitat de la mateixa.

## NOMS D'IDENTIFICACIÓ I CLAUS D'ACCÉS

Queda prohibit comunicar a una altra persona l'identificador d'usuari i la clau d'accés. Si l'usuari sospita que una altra persona coneix les seves dades d'identificació i accés haurà de posar-ho en coneixement del responsable del sistema, a fi que li assigni una nova clau. Davant d'una baixa o absència temporal de l'usuari, el responsable del departament podrà sol·licitar al responsable del sistema la cessió de clau o dades a la persona per ell designada.

ACTIVITATS QUE PODEN CAUSAR PERJUDICI A **CIMNE**

Estan expressament prohibides les següents activitats:

- Compartir o facilitar l'identificador d'usuari i la clau d'accés facilitats per **CIMNE** amb una altra persona física o jurídica, inclòs el personal de la pròpia entitat. En cas d'incompliment d'aquesta prohibició, l'usuari serà l'únic responsable dels actes realitzats per la persona física o jurídica que utilitzi de forma no autoritzada l'identificador de l'usuari.
- Intentar desxifrar les claus, sistemes, algorismes o element de seguretat que intervinguin en els processos de **CIMNE**.
- Destruir, alterar, inutilitzar o de qualsevol altra forma, danyar les dades, programes o documents electrònics de **CIMNE** o de tercers.
- Enviar missatges de correu electrònic de forma massiva o amb fins comercials o publicitaris sense el consentiment del destinatari (*spam*).
- Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres usuaris sense autorització.
- Utilitzar el sistema per intentar accedir a àrees restringides dels sistemes informàtics de **CIMNE** o de tercers.
- Introduir voluntàriament programes, virus, macros, applets, controls ActiveX o qualsevol altre dispositiu lògic o seqüencial de caràcters que causin o siguin susceptibles de causar qualsevol tipus d'alteració en els sistemes informàtics de l'entitat o de tercers. L'usuari tindrà l'obligació d'utilitzar els programes Antivirus i les seves actualitzacions per prevenir l'entrada en el sistema de qualsevol element destinat a destruir o corrompre les dades informàtics.
- Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament per **CIMNE** o qualsevol altre tipus d'obra o material els drets de propietat intel·lectual o industrial del qual pertanyin a tercers, quan no es disposi d'autorització per a això.
- Instal·lar còpies il·legals o sense llicència de qualsevol programa, inclosos els estandarditzats.
- Esborrar, desinstal·lar o modificar qualsevol dels programes instal·lats legalment sense autorització expressa del Responsable de Seguretat.
- Introduir continguts obscens, immorals o ofensius i, en general, de manca d'utilitat per als objectius de **CIMNE**, als ordinadors de la companyia.
- Realitzar proves de funcionament dels sistemes informàtics amb dades reals de caràcter personal.

CONFIDENCIALITAT DE LA INFORMACIÓ

1 L'usuari no podrà enviar, sense la deguda autorització, informació confidencial de **CIMNE** a l'exterior, mitjançant suports materials, o a través de qualsevol mitjà de comunicació. Aquesta prohibició s'estén a la simple visualització presencial o remota de la informació.

2 Els usuaris dels sistemes d'informació corporatius hauran de guardar, per temps indefinit, la màxima reserva i no divulgar ni utilitzar directament ni a través de terceres persones o empreses, les dades, documents, metodologies, claus i altres dades a les que tinguin accés durant la seva relació laboral amb **CIMNE**, tant en suport material com electrònic. Aquesta obligació de reserva continuarà vigent després de l'extinció del contracte laboral.

3 En el cas que, per motius directament relacionats amb el lloc de treball, el treballador entri en possessió d'informació confidencial en qualsevol tipus de suport, haurà d'entendre's que aquesta possessió és estrictament temporal, amb obligació de secret i sense que això l'hi atorgui cap dret de possessió, o titularitat o còpia sobre la referida informació. Així mateix, el treballador haurà de retornar aquests materials a **CIMNE**, immediatament després de la finalització de les tasques que han originat l'ús temporal dels mateixos, i en qualsevol cas, a la finalització de la relació laboral.

4 Només les persones autoritzades directament per la Gerència de **CIMNE** podran atendre a enquestadors i emplenar qüestionaris en els quals es sol·liciti qualsevol tipus d'informació relativa a **CIMNE**.

5 Queda prohibida la instal·lació de programes descarregats d'Internet o obtinguts de qualsevol altra font no fiable pel risc que pugui contenir spyware o troyanos, és a dir programes que permetin monitoritzar de forma no autoritzada l'activitat de l'usuari i enviar a l'exterior de **CIMNE** informació confidencial.

6 Per limitar al màxim el risc de pèrdua d'informació confidencial, és obligatori guardar els documents informàtics en el servidor i no conservar-la en el disc dur dels ordinadors personals. Pel mateix motiu es prohibeix l'ús de suports, pen drive, discs durs portàtils i qualsevol altre dispositiu mòbil que pugui emmagatzemar informació. Només podran utilitzar-se els dispositius mòbils expressament autoritzats i inventariats pel responsable de seguretat.

ÚS DEL CORREU ELECTRÒNIC

El sistema informàtic i la xarxa utilitzats per cada usuari són propietat de **CIMNE.**
Qualsevol fitxer introduït als ordinadors de l'usuari a través de missatges de correu electrònic que provinguin de xarxes externes haurà de complir els requisits establerts en aquestes normes i, en especial, les referides a propietat intel·lectual i industrial i a control de virus.

**CIMNE** es reserva el dret de controlar i comprovar l'ús que es realitza del correu electrònic en casos que apreciï mala fe i ús amb caràcter competencial dels mitjans electrònics que l'entitat ha posat a la seva disposició amb la finalitat de comprovar la correcció dels usos, així com de les mesures que han d'adoptar-se si escau per garantir l'efectiva utilització laboral del mitjà quan sigui necessari, sense perjudici de la possible aplicació d'altres mesures de caràcter preventiu, com l'exclusió de determinades connexions.

ACCÉS A INTERNET

L'ús del sistema informàtic de **CIMNE** per accedir a xarxes públiques com a Internet, es limitarà als temes directament relacionats amb l'activitat de **CIMNE** i les tasques del lloc de treball de l'usuari.

L'accés a debats en temps real (Xat) és especialment perillós, ja que facilita la instal·lació d'utilitats que permeten accessos no autoritzats al sistema, per la qual cosa el seu ús queda estrictament prohibit.

L'accés a pàgines web (www), grups de notícies i altres fonts d'informació com FTP, Xats, etc. es limita a aquells que continguin informació relacionada amb l'activitat de **CIMNE** o amb les tasques del lloc de treball de l'usuari.

**CIMNE** es reserva el dret de monitoritzar i comprovar, de forma aleatòria i sense previ avís, qualsevol sessió d'accés a Internet iniciada per un usuari de la xarxa corporativa.

Qualsevol fitxer introduït als ordinadors de la xarxa des d'Internet, haurà de complir els requisits establerts en aquestes normes i, en especial, les referides a propietat intel·lectual i industrial i a control de virus.

PROPIETAT INTEL·LECTUAL I INDUSTRIAL

Queda estrictament prohibit l'ús, reproducció, cessió, transformació o comunicació pública de qualsevol tipus d'obra o invenció protegida per la propietat intel·lectual o industrial.

INCIDÈNCIES

És obligació de tot el personal de **CIMNE** comunicar al responsable del sistema qualsevol incidència que es produeixi en els sistemes d'informació a què tinguin accés. S'entén per incidència qualsevol anomalia que afecti o pugui afectar a la seguretat de les dades. L'esmentada comunicació haurà de realitzar-se immediatament, i, en qualsevol cas, en un termini de temps no superior a una jornada laboral des del moment en què es conegui l'esmentada incidència. En el cas que la incidència tingui lloc fora d'horari d'oficina, es reportarà al següent dia hàbil a primera hora dins l'horari d'oficina. El coneixement i la no-notificació d'una incidència per part de l'usuari seran considerades com una falta contra la seguretat del fitxer de dades de caràcter personal i es podrà actuar en conseqüència.

GESTIÓ DE SUPORTS

Els suports que continguin dades de caràcter personal, be com a conseqüència d'operacions intermèdies pròpies o com a conseqüència de processos d'execució de còpia de respaldo o qualsevol altra operació esporàdica, hauran d'estar degudament identificats conforme a allò que s'indica en el Document de Seguretat.

Quan la sortida de dades es realitzi per mitjà de correu electrònic, les trameses es realitzaran sempre i exclusivament des de comptes que puguin ser controlades pel Responsable de Seguretat, deixant constància d'aquestes trameses en l'històric d'aquest compte de correu o en algun registre de sortides que permeti conèixer en qualsevol moment les trameses realitzades, a qui anaven dirigides i la informació enviada, sempre d'acord al que s'especifica en els registres de sortida de suports.

PROTECCIÓ DE DADES

1 És obligació de tot el personal que accedeixi a dades personals en suport informàtic, en paper o en qualsevol altre suport, respectar la normativa aplicable en aquesta matèria, mantenint la màxima confidencialitat sobre aquestes dades i aplicant les mesures de seguretat establertes en aquest document, en el Document de Seguretat de **CIMNE** i en la llei i el reglament actualment vigent.

2 No podran crear-se fitxers de dades personals sense l'autorització del responsable de protecció de dades.

3 No es podrà creuar informació relativa a dades de diferents fitxers o serveis amb la finalitat d'establir perfils de personalitat, hàbits de consum o qualsevol altre tipus de preferències, sense l'autorització expressa del responsable de protecció de dades.

4 No podrà realitzar-se qualsevol altra activitat expressament prohibida en aquest document o en les normes sobre protecció de dades i Instruccions de l'Agència espanyola i/ o catalana de protecció de Dades.

5 Hauran de complir-se les mesures de seguretat establertes per al tractament i la conservació de dades personals de forma automatitzada o no automatitzada, en suport informàtic o en paper.

6 El treballador dóna el seu consentiment per:

a. Tractar les dades de caràcter personal que quedin registrades en els recursos TI de **CIMNE** amb les finalitats establertes en aquestes normes, incloent l'elaboració de patrons estadístics.
b. Tractar les dades de desenvolupament professional, carrera, avaluació, coaching, proves psicotécniques, i restants dades relacionades amb la gestió del capital humà.
c. Tractar les dades de salut relatives a baixes laborals i control d'absentisme que la legislació vigent permeti gestionar als serveis mèdics corporatius i al departament de recursos humans.
d. Transferir les dades de l'usuari a la xarxa nacional i internacional, si escau, amb la finalitat d'afavorir el networking, permetre l'enviament de correu electrònic entre oficines i entre professionals de la companyia, rebre informació corporativa d'altres països, intercanviar coneixements tècnics i sobre el mercat, les empreses i els sectors, afavorir els contactes comercials, realitzar còpies de seguretat, realitzar estadístiques globals i prestar serveis d'emmagatzematge d'informació.

RESPONSABILITATS.

**CIMNE** adoptarà les mesures necessàries per tal que el personal conegui les normes de seguretat que afectin el desenvolupament de les seves funcions, així com les conseqüències que es poguessin derivar en cas d'incompliment.

Cadascuna de les persones que tingui accés a les dades de caràcter personal i als sistemes d'informació de **CIMNE** hauran de tenir clarament definides i documentades les seves funcions i obligacions, segons s'estableix en l'art. 89 i següents del Reial Decret 1720/2007, de 21 de desembre, que aprova el Reglament de desenvolupament de la vigent Llei 15/1999, de protecció de dades personals.

**CONSENTIMENT INFORMAT DE LA NORMATIVA DE PROTECCIO DE DADES CONTINGUDA EN EL DOCUMENT DE SEGURETAT**

**En/Na……..,** amb DNI núm. ……., es compromet al compliment de les funcions i obligacions especificades en aquest document.

A ....., a …….de ……. de 2013.

Signat. ……