com ara pèrdues, sospites d'ús indegut, recuperació de dades, etc. Aquesta comunicació es farà per les vies de Notificació d'Incidències formalment establertes, i se n'haurà d'informar immediatament al responsable de Seguretat o al seu superior jeràrquic.

- Retornar o destruir els suports i documents que continguin dades de caràcter personal un cop finalitzades les tasques que han autoritzat el seu ús, d'acord amb allò que s'especifica en la normativa interna o en la Instrucció General-Gestió de suports.
- Eliminar aquells documents amb dades personals que hagi estat necessari crear temporalment, com ara fitxers automatitzats i/o còpies paper amb informació temporal, a fi d'impedir qualsevol tractament posterior d'aquesta informació.
- Quan els documents que continguin dades de caràcter personal, tant en suport paper com digital, hagin de ser extrets de les instal·lacions municipals o dels organismes o entitats afectats per aquesta norma, a més de comptar amb l'autorització corresponent del responsable del servei o del fitxer, caldrà adoptar les mesures operatives definides en funció del nivell de protecció propi de cada fitxer. Molt especialment, quan es tracti de dades de caràcter personal que requereixin l'establiment de mesures de seguretat de nivell alt, caldrà assegurar que s'adopten les mesures i els mecanismes que siguin necessaris per impedir l'accés o la manipulació de la informació que sigui objecte de trasllat.
- En general, tot tractament de dades de caràcter personal realitzat per les persones a les que es refereix aquesta Norma, ja sigui aquell tractament automatitzat o no, haurà de complir estrictament amb les mesures de seguretat establertes en el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, aprovat pel reial Decret 1720/2007, de 21 de desembre, d'acord amb les indicacions i instruccions que, respecte a aquest compliment, faci el responsable del Servei o del fitxer corresponent.

El Comitè de Seguretat de l'IMI, en exercici de les seves competències, va aprovar en la sessió de l'11 de juny de 2009 la *Norma Tècnica de Seguretat (NTS)* com a norma complementària a la *Instrucció sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament de Barcelona*.

Barcelona, 26 de juny de 2009. La secretària del Comitè de Seguretat de l'IMI, Neus Bellavista i Arimany.

NORMA TÈCNICA DE SEGURETAT PELS USUARIS DELS SISTEMES D'INFORMACIÓ DE L'AJUNTAMENT DE BARCELONA

1. OBJECTE I ÀMBIT D'APLICACIÓ

a) Aquesta norma té per objecte establir els criteris tècnics de seguretat específics per a l'adequada utilització dels sistemes d'informació i comunicació de l'Ajuntament de Barcelona.
b) Entenent com a criteris tècnics de seguretat el conjunt de mecanismes tècnics i organitzatius que permetin garantir la confidencialitat, integritat i disponibilitat dels sistemes d'informació, així com la autenticitat, el no repudi i el compliment legal.
c) Aquesta norma s'aplicarà al personal al servei de l'Ajuntament de Barcelona, dels seus organismes autònoms i entitats públiques empresarials, així com, del personal de les societats mercantils que tinguin accés a aquests sistemes i mitjans d'informació. Per extensió també serà d'aplicació a tot aquelles persones que sense tenir la condició de personal municipal amb l'Ajuntament adquireixin la condició d'usuaris del Sistemes d'Informació en virtut d'un contracte de prestació de serveis, conveni o altra tipus d'acords.
d) Aquesta norma no s'aplica als usuaris (ciutadans, empreses, representants, professionals, etc.) de portals de tramitació electrònica per Internet que es regiran per les seves pròpies condicions d'ús i prestació del servei.

2. COMPLEMENTARIETAT D'AQUESTA NORMA

Aquesta norma ha estat aprovada pel Comitè de Seguretat de l'IMI i té caràcter complementari respecte a la Instrucció: *Sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament de Barcelona (Gaseta Municipal, núm. 7, Any XCVI, de data 28 de febrer de 2009).*

3. PRINCIPIS GENERALS

Amb independència dels sistemes d'informació seran sempre d'aplicació els següents principis generals de seguretat TIC:

Principi de propietat. Tots els recursos dels sistemes d'informació municipals, així com la informació continguda, són propietat de l'Administració municipal. No està permès utilitzar els sistemes d'informació de l'Administració municipal amb finalitats privades.

Principi del mínim privilegi. Els privilegis d'accés s'assignaran tenint en compte els mínims necessaris per desenvolupar les tasques assignades.

Principi de necessitat de conèixer. El privilegi d'accés a la informació no té caràcter general, sinó que l'habilitació per accedir a una informació en concret es troba vinculada sempre a la resolució d'un expedient, tràmit o tasca encomanada.

Principi de no revelació. En el cas que la informació no hagi estat classificada o es tinguin dubtes sobre la seva classificació, aquesta haurà d'ésser considerada com no pública.

Principi de no extracció. El privilegi d'accés a la informació no pressuposa el dret a extreure-la dels Sistemes d'Informació. L'extracció de la informació s'haurà de fer sempre de manera controlada i autoritzada pel seu responsable.

Principi de coresponsabilitat amb la seguretat. Tots els usuaris compleixen una funció essencial per a garantir la seguretat dels sistemes d'informació donat que aquesta es troba condicionada per les seves accions i pel seguiment de les instruccions, normes i recomanacions en matèria de seguretat. Per tant, els usuaris tenen l'obligació de gestionar tant la informació a la que tenen accés com els mitjans emprats per accedir-hi (contrasenyes, certificats digitals, equips informàtics, etc.) de manera diligent i a comunicar qualsevol incidència de seguretat de la que tinguin coneixement pels canals que aquesta norma estableix.

Principi de retorn dels actius d'informació. Una vegada finalitzada la relació de servei o quan per una modificació en la mateixa els actius propietat de la Corporació (informació, credencials, certificats digitals, targeta magnètiques, portàtils, pda's, etc.) ja no el hi siguin necessaris el personal té l'obligació de retornar-los. En cas de dubte sobre com fer el retorn consultarà al seu departament de Recursos Humans i en cas de no ser personal municipal al responsable del contracte, conveni o servei.

4. CONTROL D'ACCÉS ALS SISTEMES D'INFORMACIÓ I IDENTITAT DIGITAL

Per als sistemes d'informació que així ho requereixin, cada persona disposarà d'unes credencials d'usuari que, mitjançant un procés tècnic, li permetran o denegaran l'accés. Els tipus de credencials d'usuari que es fan servir en l'actualitat a l'Ajuntament de Barcelona són:

- Identificador d'usuari (p.e.: codi de matrícula) + una contrasenya secreta.
- Certificat Digital (p.e.: Certificat de CATCert i Certificat IMICAT per accés VPN) + PIN.
- Targeta Magnètica (p.e.: Targeta aplicació de control horari).

El codi identificador d'usuari i la contrasenya són la credencial utilitzada de manera generalitzada per accedir als sistemes d'informació de l'Ajuntament de Barcelona.

El certificats digitals s'utilitzen principalment per a la signatura electrònica de tràmits i documents, encara que també es poden utilitzar per a accedir als sistemes d'informació a aplicacions d'altres entitats.

La targeta magnètica de control horari té la consideració de credencial ja que permet identificar al seu titular com a membre de la Corporació municipal i l'identifica en el sistema d'informació de control horari.

Com a norma general les credencials són d'ús personal e intransferible i s'atorguen amb finalitats relacionades exclusivament amb el desenvolupament de les tasques assignades al lloc de treball. Qualsevol ús fóra d'aquestes finalitats resta prohibit.

El conjunt de credencials que disposi un usuari i els seus privilegis d'accés constitueixen la seva identitat digital dins dels sistemes d'informació de l'Ajuntament de Barcelona.

Cada persona és responsable de l'ús que es faci de les credencials que tingui, i resta obligada a:

4.1. Guardar el secret de les seves contrasenyes.
4.2. Custodiar els certificats digitats que tingui assignats.
4.3. Procurar no perdre la targeta magnètica ni els suports físics que continguin els certificats com poden ser disquets o clauers usb.
4.4. Comunicar mitjançant el procediment de comunicació d'incidències indicat en la secció 12 d'aquesta norma qualsevol problema amb les seves credencials que pugui derivar en un risc per a la seguretat dels sistemes d'informació.

Contrasenyes

La contrasenya és un dels elements fonamentals del control d'accés als sistemes:

4.5. Els usuaris han de seguir unes bones pràctiques de seguretat en la selecció i ús de contrasenyes:
   - ü No revelar mai la contrasenya sota cap motiu.
   - ü Canviar la contrasenya sempre que existeixi un possible indici d'ús incorrecte del sistema o de les contrasenyes.
   - ü Canviar les contrasenyes provisionals en el primer accés encara que el sistema no obligui a fer aquest canvi.
   - ü Canviar les contrasenyes sempre que el sistema ho sol·liciti i evitar reutilitzar o reciclar velles contrasenyes. En cas que algun sistema no tingui inclosa aquesta funcionalitat, l'usuari s'encarregarà de canviar de forma periòdica la seva contrasenya (es recomana, cada tres mesos, com a mínim).
   - ü Seleccionar contrasenyes robustes i de qualitat seguint les recomanacions contingudes en aquest document.

- ü Contestar negativament quan un formulari ofereixi la opció de recordar la contrasenya o similar.
- ü No anotar la contrasenya en llocs fàcilment accessibles que posin en perill la seu caràcter secret i confidencial.

Els criteris recomanats per a la construcció de les contrasenyes, exceptuant els casos en que degut a la tecnologia o plataforma a emprar es detalli de forma específica, són:

- ü No hauran de tenir una longitud inferior a 6 caràcters alfanumèrics, essent recomanable l'ús de 7 o més, i a ser possible, es faran servir majúscules, minúscules i números.
- ü No seleccionar com a contrasenya paraules en qualsevol idioma, no utilitzar seqüències lògiques deduïbles quan es realitzi el canvi de contrasenya, no utilitzar permutacions senzilles ni seqüències del teclat, etc.
- ü No es faran servir noms de persones o coses fàcilment identificables amb un usuari tals com: nom de la parella, fills, departament, matrícula del vehicle, dates de naixement, número d'empleat, etc.

Accés als sistemes d'informació mitjançant un codi identificador d'usuari i una contrasenya.

El codi d'usuari identifica a la persona com a membre del Sistema (procés d'identificació). La garantia que la persona és qui diu ser l'aporta la contrasenya, ja que és secreta i només l'usuari la coneix (procés d'autenticació).

Les consideracions sobre l'accés al Sistemes d'Informació es troben indicats en la secció 3 de la Instrucció sobre l'ús dels sistemes d'informació i comunicació per part del personal al Servei de l'Ajuntament de Barcelona. Addicionalment:

4.6. Una persona només pot disposar d'un identificador d'usuari, qualsevol excepció ha de ser aprovada per l'IMI

4.7. No es farà servir l'usuari i accessos d'un altre usuari, encara que es disposi de l'autorització del seu propietari.

Certificats digitals.

L'Ajuntament de Barcelona utilitza certificats digitals per realitzar tasques administratives. Els certificats digitals que disposa per al personal són:

El certificat digital de personal de l'Ajuntament, certificat d'Administració local de Catcert (EC-AL), lliurat amb suport de targeta digital, és propietat de l'Ajuntament. El seu ús està destinat únicament al personal de l'Ajuntament per a la realització de tasques administratives, signatures digitals i per identificar-se i autenticar-se, i signar en altres entitats externes a l'Ajuntament. L'emissió, lliurament i revocació d'aquests certificats seguirà el procediment establert en la Direcció de Recursos Humans.

El certificat digital per connexió remota, la seva finalitat és proveir accés des de l'exterior a la xarxa corporativa i als sistemes d'informació interns de l'Ajuntament de Barcelona (VPN). L'emissió, lliurament i revocació d'aquests certificats seguirà el procediment establert en l'IMI, mitjançant el canal de peticions establert.

4.8. L'ús de certificats digitals pel desenvolupament de tasques administratives es realitzarà de conformitat amb les polítiques i pràctiques d'ús de certificats establertes per l'IMI. En cap cas el personal utilitzarà certificats digitals que no estiguin establerts i autoritzats per l'IMI.

4.9. El personal que disposi d'un d'aquests certificats ha de custodiar el certificat de forma diligent, prenent les precaucions raonables per evitar la seva pèrdua, revelació del PIN o ús no autoritzat.

4.10. El personal és responsable de realitzar una bona utilització del certificat.

4.11. Els certificats digitals que es carreguen específicament a un navegador, s'han de protegir amb un clau o PIN. Quan excepcionalment s'hagi de fer servir un certificat digital d'aquesta forma, fora de l'estació estàndard, com per exemple al propi domicili per fer teletreball o amb ordinadors compartits, s'haurà de desinstal·lar el certificat del navegador quan ja no es necessiti.

4.12. El personal ha de sol·licitar la suspensió/ revocació del certificat quan es compleixi algun dels supòsits de suspensió/revocació de certificats o s'hagi produït un incident de seguretat intern que pugui posar en perill la seguretat de la xarxa de l'Ajuntament de Barcelona.

- Supòsits de revocació:
  - ü baixa o finalització de la prestació de servei a l'Administració municipal,
  - ü canvi de les tasques assignades,
  - ü pèrdua o robatori de les credencials d'accés.

Targetes magnètiques de control horari.

En algunes dependències municipals aquesta tarja es fa servir per transitar per portes controlades mitjançant lector de tarja magnètica.

4.13. En cas de pèrdua o robatori de la tarja ho heu de comunicar immediatament al vostre departament de Recursos Humans.

5. SEGURETAT TÈCNICA DE LES OFICINES I INFRAESTRUCTURES BÀSIQUES

5.1. Disposició de les pantalles. El personal de les oficines d'atenció al públic hauran de preservar la confidencialitat de la informació dels ciutadans. Qualsevol reconfiguració de la disposició

física dels llocs de treball haurà de respectar aquest requisit.

5.2. No està permesa la manipulació interna dels equips ni de les seves connexions tant a la xarxa de dades com a la xarxa elèctrica per personal no especialitzat. Una manipulació incorrecta pot provocar accidents amb danys per a les persones i pèrdua de dades.

5.3. No està permès treure l'etiqueta de control d'inventari dels equips ni manipular les etiquetes dels números de sèrie.

5.4. No està permesa la connexió de concentradors (*hubs*) a punts de la xarxa corporativa sense la autorització de l'IMI.

5.5. No està permesa la connexió d'equips no informàtics als endolls dels SAI (Sistema d'Alimentació Ininterrompuda, normalment són endoll de color vermell).

5.6. No està permesa la connexió d'encaminadors (*routers*) o mòdems a les estacions de treball ni a la xarxa telefònica sense l'autorització de l'IMI.

5.7. Al finalitzar la jornada laboral els equips (ordinadors, impressores, etc.) hauran de ser apagats de forma controlada. Això permet un important estalvi d'energia i minimitzar el risc d'incendi.

5.8. En les zones sense accés al públic o restringides (arxius, sales d'ordinadors, oficines internes, despatxos) es vetllarà per l'eficàcia dels controls d'accés: mantenint les portes tancades, requerint passi de visitants, complint amb les normes específiques que cada dependència desenvolupi a aquest efecte, etc.

6. SEGURETAT TÈCNICA DE L'ESTACIÓ DE TREBALL

6.1. L'usuari iniciarà sessió de manera controlada a l'estació de treball amb el seu codi identificador d'usuari i contrasenya i seguint les recomanacions que hagi establert l'IMI.

6.2. Quan l'usuari s'hagi d'absentar de manera puntual del lloc de treball utilitzarà el mecanisme de bloqueig de pantalla.

6.3. Al finalitzar la jornada laboral apagarà l'equip de manera controlada.

6.4. No es permet la realització d'activitats, utilització d'equips o aplicacions que no es trobin especificades com a part del programari o productes homologats i acceptats.

6.5. Es prohibeix intentar destruir, alterar, i en general qualsevol acció malintencionada que pugui malmetre dades, programes o documents electrònics.

6.6. No està permès l'ús de programes informàtics sense la corresponent llicència, així com l'ús, reproducció, cessió, transformació o comunicació pública de qualsevol tipus d'obra o d'invenció protegida per la propietat intel·lectual o industrial.

6.7. No es permet aturar aplicacions estàndards d'execució automàtica programada com és l'antivirus.

6.8. Quan per a la resolució d'un problema, es requereixi que es controli l'equip de forma remota aleshores l'usuari tancarà totes aquelles aplicacions que puguin contenir informació confidencial o sensible i supervisarà les accions que s'estiguin realitzant, no podent deixar desatesa la pantalla.

7. SEGURETAT TÈCNICA DE LA INFORMACIÓ

La informació junt amb les persones són els actius més valuosos per qualsevol organització. L'Ajuntament de Barcelona pren especial consciència d'aquest fet i vol desenvolupar una cultura de protecció i seguretat de la informació de la que tots els usuaris són part fonamental.

Els eixos bàsics de la seguretat de la informació són:

- Seguretat en el control d'accés, ús i tractament.
- Emmagatzemament segur.
- Prevenció enfront fuites d'informació i extraccions no controlades.

Seguretat en el accés, ús i tractament de la informació.

7.1. S'accedirà a la informació sempre mitjançant els procediments tècnics establerts. Resta absolutament prohibit manipular el programari per evitar els processos estàndard de control d'accés (identificació i autenticació).

7.2. El personal accedirà amb els permisos que li han estat atorgats i no intentarà obtenir-ne d'altres que no siguin els assignats.

7.3. En el cas de les bases de dades corporatives resta absolutament prohibit intentar accedir i accedir a les mateixes directament, és a dir, fóra dels sistemes de connexió autoritzats per les aplicacions.

7.4. La connectivitat directa entre aplicacions d'ofimàtica com Excel i Access a les bases de dades corporatives haurà d'estar motivada, validada tècnicament per l'IMI i acceptada pel responsable de la informació que serà informat dels possibles riscos de seguretat inherents a aquestes funcionalitats.

7.5. L'ús i el tractament de la informació es farà sempre de conformitat al principi de legalitat que regeix l'actuació de les administracions públiques. És a dir, aquest ús i tractament de la informació serà sempre acord a les finalitats de la mateixa i a les competències legítimes de l'Administració, tot seguint els procediments administratius que garanteixen l'eficàcia de

l'actuació administrativa i els drets dels ciutadans.

7.6. Cas que la informació no estigui classificada respecte a la seva criticitat o privacitat sempre serà considerada com a confidencial o no pública. En cas de dubte, l'usuari haurà de consultar al seu responsable jeràrquic.

7.7. El personal no intentarà desxifrar claus, sistemes o algoritmes de xifrat o qualsevol altra element de seguretat. Només està permesa la utilització de mecanismes de xifrat de la informació homologats per l'IMI.

7.8. La signatura electrònica constitueix, entre d'altres, un instrument que dona resposta a la necessitat de la administració electrònica de conferir confiança, seguretat i validesa jurídica al ciutadà i a la tramitació electrònica d'expedients, així com a qualsevol altra actuació interna de l'Administració. Els documents que requereixin signatura digital de l'Ajuntament, seguiran els estàndards de l'IMI, i no es generaran signatures electròniques fora d'aquests estàndards i polítiques de signatura establertes.

Emmagatzemament segur.

L'emmagatzemament corporatiu garanteix el compliment legal respecte a l'obligació de tenir còpies de seguretat i permet recuperar les dades en cas de pèrdua d'informació. També permet garantir la recuperació i restabliment dels serveis, en un termini de temps raonable, de cara al ciutadà (disponibilitat de la informació).

7.9. Tota la informació automatitzada estarà dipositada en els servidors oficials de la xarxa corporativa de l'Ajuntament. En cap cas, s'utilitzarà per la gestió corporativa de la informació, els discs locals de les estacions de treball (pc's), discos extraïbles, portàtils.

7.10. Revisar de forma periòdica l'organització de les carpetes i els documents, vigilant de no guardar documents sense causa justificada.

Prevenció enfront de fuites d'informació.

7.11. No està autoritzada l'extracció de la informació fora dels servidors corporatius: ni a dispositius locals (discs...), ni a mòbils (USB, portàtils, suports magnètics/òptics o altres), ni l'enviament per correu electrònic o a dispositius d'accés remot.

7.12. Ningú pot realitzar còpies, transmissions, comunicacions ni cessions de la informació municipal dipositada en els sistemes informàtics que no estiguin inclosos en els procediments establerts i en exercici de les funcions que li han estat encomanades.

7.13. En el cas que per motius directament relacionats amb el lloc de treball el treballador hagués d'extreure informació, realitzar còpies, comunicacions o cessions no incloses en els procediments, aquesta extracció haurà d'estar autoritzada pel responsable del Servei Municipal, o responsable del fitxer en cas de tractar-se de dades de caràcter personal. Es recorda que la informació enviada per correu electrònic a fora de la organització ja sigui en el propi cos del missatge o en un fitxer annex té la consideració d'extracció d'informació i pot requerir d'autorització en funció del tipus d'informació i del procediment que es tracti.

7.14. Així mateix, el personal es compromet a no divulgar, utilitzar o modificar "la informació", al marge dels procediments corresponents al seu lloc de treball o de les directrius dels seus superiors, fins i tot després de la finalització del seu contracte o nomenament.

7.15. Política de pantalla bloquejada i taula endreçada. Per evitar accessos no controlats a l'estació de treball aquesta sempre s'haurà de deixar bloquejada quan es deixi desatesa i apagada en acabar la jornada laboral. Així mateix, s'ha d'evitar deixar informació confidencial i/o sensible a sobre de les taules.

7.16. Els llistats que no es lliurin en mà, és a dir aquells que es deixen en bústies o taules comunes de repartiment de carteria s'hauran de lliurar sempre en sobres tancats.

7.17. Es recomana recollir el més aviat possible els llistats de les impressores i faxos per evitar revelacions d'informació no controlades. En especial quan s'hagi enviat a imprimir informació confidencial o sensible.

7.18. Els suports tan paper, com disquets i d'altres s'han de destruir de manera controlada. Fem servir destructores de documents o dipòsits controlats per empreses que garanteixen la seva destrucció. S'haurà de tenir especial cura amb aquells suports que continguin informació confidencial, sensible o dades de caràcter personal.

7.19. S'ha de tenir especial cura de no desar fitxers temporals en carpetes de xarxa que tinguin caràcter públic més enllà de la dependència o del grup de persones que treballen en un determinat tema.

7.20. Els fitxers temporals, com per exemple els de *office* s'han d'esborrar quan ja no siguin necessaris.

8. SEGURETAT DELS DISPOSITIUS MÒBILS I DE LA INFORMACIÓ CONTINGUDA

La proliferació de dispositius mòbils com els portàtils, pda's, telèfons mòbils, memòries usb o de qualsevol altre tipus, constitueix un important repte per a la seguretat de la informació, donat que per si mateixos tenen uns riscos majors de pèrdua o ro-

batori que els dispositius tradicionals com els ordinadors de sobretaula.

A més, aquests dispositius pel seu caràcter "nòmada", canvien de lloc constantment, no es poden beneficiar de les mesures de protecció basades en perímetres segurs.

Les mesures de seguretat bàsiques per aquests dispositius són les següents:

8.1. Els dispositius mòbils de l'Administració municipal hauran d'estar convenientment inventariats i controlats per garantir que disposen de les mesures de seguretat que a tal efecte hagi establert l'IMI.

8.2. Resta absolutament prohibit modificar, actualitzar o manipular el *software* dels dispositius mòbils de la Corporació municipal sense el consentiment de la dependència que s'hagi fet responsable de les polítiques de seguretat que s'hagin establert per aquest dispositius.

8.3. L'usuari haurà de seguir les recomanacions de seguretat que en cada moment es publiquin per a aquest tipus de dispositius. L'IMI és l'encarregat d'elaborar i publicar les guies d'utilització segura de dispositius mòbils. També serà l'encarregat per als equips estàndards que tingui al seu càrrec, de la instal·lació i el manteniment del seu *software* base, a l'igual que fa amb les estacions de treball de sobretaula.

8.4. Els usuaris són responsables de la seguretat de la informació municipal que contenen els dispositius mòbils així com de la informació municipal a la qual aquests tenen accés.

8.5. La disposició de dispositius portàtils de la Administració municipal per part de determinats empleats resta sempre condicionada al seu ús professional. Per tant, encara que es facin servir fora de les oficines municipals, incloent-hi el domicili particular per aquells que fan teletreball. No s'hauran de permetre l'ús i l'accés a personal aliè a l'Administració municipal o sense la deguda autorització.

8.6. La utilització de les unitats locals del portàtil o altres dispositius mòbils per emmagatzemar dades de l'administració municipal ha d'ésser excepcional. En cas que sigui necessari s'ha de tenir en compte que:

- ü Resta absolutament prohibit l'emmagatzemament de dades de caràcter personal als dispositius portàtils o mòbils. Excepcionalment es podrà fer sempre i quan es tingui l'autorització expressa del responsable del fitxer i s'apliquin les mesures de seguretat que estableix la LOPD i el seu Reglament (RD 1720/2007).

8.7. L'emmagatzemament d'informació corporativa a l'ordinador portàtil haurà de comptar amb l'autorització del responsable del fitxer LOPD o el responsable del servei de l'Ajuntament. Es realitzarà de forma xifrada fent servir els procediments estàndards establerts, ja que aquests procediments són els únics que poden garantir la recuperació de la informació en cas de corrupció de les claus.

8.8. L'emmagatzemament d'informació corporativa a cd's, *pendrives*, etc. haurà de comptar amb l'autorització del responsable del fitxer LOPD o el responsable del servei de l'Ajuntament. La seva finalitat serà només el transport o lliurament de la informació. Mentre no existeixin procediments formals de xifrat per aquests dispositius, l'usuari xifrarà la informació amb el programari homologat que consideri oportú, com per exemple, *winzip*, la custòdia de les claus restarà sota la responsabilitat de l'usuari.

8.9. Quan es facin servir dispositius mòbils i en especial ordinadors portàtils en llocs públics, fora de les oficines municipals o en trànsit durant un viatge, caldrà augmentar les mesures de seguretat físiques amb les recomanacions següents:

- ü No deixar desatesos els equips. L'usuari haurà de prestar especial atenció a l'ús de l'equip portàtil o dispositiu mòbil en llocs públics.
- ü No deixar l'ordinador portàtil de l'Ajuntament o dispositiu mòbil en el maleter del cotxe, en el seu interior o en consignes d'estacions o aeroports.
- ü En cas de desplaçaments aeris, els equips portàtils o dispositius mòbils hauran d'endur-se com a equipatge de mà. No està autoritzada la seva facturació com a equipatge. L'usuari sempre el tindrà sota la seva vigilància.
- ü En cas que l'ordinador portàtil o dispositiu mòbil sigui utilitzat en dependències externes a l'Administració municipal s'hauran d'aplicar mesures mínimes de seguretat com per exemple tancar amb clau la sala o fer servir dispositius de cable de seguretat per lligar l'equip si és possible; i sempre bloquejar la pantalla de l'ordinador. Si l'absència és perllongada l'equip s'haurà de deixar apagat.
- ü No posar identificacions de l'Organisme en el dispositiu, excepte els estrictament necessaris.
- ü No posar dades de contacte tècnic o claus en el dispositiu.
- ü Si pel tipus de feina l'usuari fa servir l'ordinador en llocs públics es recomana fer servir filtres de privacitat.

8.10. En el cas de dispositius que interaccionen amb els sistemes d'informació municipals: ordinadors portàtils, PDA o *blackberries* s'ha de protegir el dispositiu amb una contrasenya de bloqueig físic amb un temps que en el cas del l'ordinador portàtil no ha d'esser superior a 15 minuts i en el cas de PDA i *blackberries* no ha de ser superior a 5 minuts.

8.11. Si es compromet per qualsevol causa la informació de l'Administració municipal es comunicarà mitjançant l'obertura d'una incidència pels procediments formals establerts en la secció 12 d'aquesta norma.

9. TELETREBALL (ACCÉS MITJANÇANT XARXES PRIVADES VIRTURALS "VPN")

Té la consideració de teletreball la connexió amb els sistemes d'informació de l'Ajuntament de Barcelona des de fora de la xarxa corporativa.

La forma estàndard de connexió remota es realitza mitjançant xarxes privades virtuals (VPN) i VPN-SSL que porten, a més a més, associada la utilització de certificats digitals per identificar-se i autenticar-se.

La sol·licitud de connexió via VPN es fa mitjançant un procediment documentat que es troba publicat a la Intranet. En el moment del lliurament del certificat digital i del programari necessari per realitzar la connexió es lliuren en paper les condicions de prestació del servei i les recomanacions específiques de seguretat per aquest tipus de connexió.

A més de les consideracions definides en l'estació de treball estàndard i del dispositiu mòbil, les mesures de seguretat bàsiques pel teletreball són:

9.1. No descarregar informació municipal a les estacions remotes que accedeixen a sistemes d'informació municipals.

9.2. Quan es connecti des del domicili particular es recomana tenir el programari del sistema operatiu actualitzat i fer servir un antivirus actualitzat així com tenir activat el tallafocs.

9.3. S'ha d'evitar connectar-se des de sales de prestació d'ordinadors (locutoris, cibercafés, biblioteques, etc.).

9.4. S'ha de tenir especial cura de tancar les sessions que s'hagin obert de manera controlada.

9.5. Mai s'ha d'assenyalar la opció de recordar contrasenya en el formulari d'inici de sessió dels programes.

9.6. Resta absolutament prohibit accedir a informació confidencial o sensible des d'Internet i des d'ordinadors públics. Aquesta prohibició s'estén a la informació d'aquest tipus que pugui estar inclosa en missatges de correu electrònic o en els fitxers annexes als mateixos. El personal que hagi d'accedir a aquest tipus d'informació ho haurà de fer mitjançant connexions segures (VPN i VPN-SSL) i des d'ordinadors propietat de l'Ajuntament de Barcelona, o des de l'ordinador del seu domicili particular si ha estat expressament autoritzat i disposa del certificat digital i connexió VPN.

9.7. Així mateix, s'ha d'evitar descarregar o accedir des d'ordinadors públics a qualsevol tipus de fitxer propietat de l'Ajuntament de Barcelona encara que no siguin confidencials. Cas d'haver descarregat un fitxer s'ha de tenir especial cura d'esborrar-ho del disc dur i buidar la paperera. Cas d'haver visualitzat el fitxer s'ha de verificar que no hagi quedat desat en la carpeta de fitxers temporals. Cas d'haver carregat certificat al navegador, s'ha d'eliminar.

9.8. No fer servir simultàniament durant la connexió als sistemes d'informació municipal altres programes potencialment perillosos en quan a la seguretat de la informació com són: els programes de missatgeria instantània i els programes d'intercanvi de fitxers.

10. ÚS ACURAT DELS RECURSOS I MEDI AMBIENT

La majoria dels recursos informàtics són compartits pels usuaris (ample de banda de la xarxa corporativa i accés a Internet, espai d'emmagatzemament en disc, impressores, etc.) i per tant cal fer un ús eficient dels mateixos.

En aquest sentit cal tenir en compte les següents recomanacions:

- Revisar de forma periòdica l'organització de les carpetes i els documents, vigilant de no guardar documents sense causa justificada.
- Imprimir els documents només quan sigui realment necessari i fer servir quan sigui possible la impressió a dues cares. Els llistats constitueixen un risc de fuita d'informació que s'ha d'evitar.
- Fer servir els contenidors de paper reciclat si estan disponibles a la vostra dependència. Aquest contenidors garanteixen la confidencialitat amb una destrucció controlada i la protecció del medi ambient mitjançant el procés de reciclatge.
- Apagar els equips (ordinadors, impressores, escàners) quan no es necessitin i al finalitzar la jornada laboral.

11. MONITORITZACIÓ I REGISTRES D'ACTIVITAT

Els sistemes d'informació i les infraestructures tecnològiques que els hi donen suport disposen de mecanismes de monitorització i registres d'activitat. L'explotació d'aquests mecanismes tenen com a finalitat garantir el manteniment i la continuïtat del serveis informàtics de conformitat amb els nivells de qualitat dels serveis acordats; gestionar els riscos i problemes, així com, facilitar la resolució de problemes de rendiment i/o de seguretat.

L'ús dels mecanismes de monitorització i registre d'activitats resta subjecte en tot moment al principi de legalitat i principis tècnics resumits a la secció 3 d'aquesta norma.

Les eines de monitorització i els registres d'activitat, anomenats *logs* en general, són un element

clau per avaluar i respondre a les incidències, problemes i esdeveniments que es puguin produir dins de les xarxes i sistemes d'informació, que afectin a pèrdues de rendiment i a la seva disponibilitat, confidencialitat i integritat.

En la majoria de casos, es tracta d'informació tècnica que registren els sistemes d'informació automàticament i que es conserven al llarg del temps d'acord a les seves especificitats.

La seva explotació és duta a terme pel personal especialitzat, específicament autoritzat per l'oficina de seguretat TIC de l'IMI, que només podrà accedir i visualitzar la informació mínima necessària per realitzar les tasques encomanades amb l'objectiu de donar resposta a incidències tècniques, que posin en perill la finalitat de manteniment abans enunciada, o per a la detecció de riscos i la prevenció de futurs problemes.

Aquestes incidències, poden ser produïdes, per errors en el propi sistema, per causes externes (micro tall subministrament elèctric, etc.), per intents d'intrusió a la xarxa municipal o per accions errònies o malintencionades de qualsevol usuari de la xarxa.

Quan l'explotació del *logs* impliqui la identificació d'usuaris, aquesta serà realitzada directament per tècnics qualificats de l'Oficina de Seguretat TIC, d'acord a un procediment formal i sota la tutela de Recursos Humans de l'Ajuntament de Barcelona que garantirà en tot moment els drets dels usuaris.

12. COMUNICACIÓ D'INCIDÈNCIES DE SEGURETAT

12.1. Els usuaris dels sistemes d'informació de l'Ajuntament de Barcelona tenen l'obligació de comunicar les incidències de seguretat de les que tingui sospita o coneixement.

Qualsevol persona que pertanyi o treballi per a l'Ajuntament de Barcelona , que detecti una incidència o anomalia que posi o pugui posar en perill la seguretat dels sistemes d'informació, haurà de comunicar aquesta incidència o anomalia a través de línies de comunicació establertes amb aquest propòsit (Servei d'Atenció a l'Usuari) per al seu correcte registre i resolució.

Per comunicar les incidències de seguretat es faran servir els mecanismes estàndards de comunicació incidències establerts:

Trucant al SAU (Servei d'Atenció a Usuaris) 93 291 (7) 82 34

En funció del tipus d'incidència el SAU derivarà la incidència a l'equip especialitzat en seguretat de l'IMI o la resoldrà directament.

Alguns exemples d'incidències de seguretat són els següents:

a) Sol·licitud de restabliment de contrasenya.
b) Sospita que un tercer està accedint amb el nostre codi d'usuari i contrasenya.
c) Esborrat accidental de dades i sol·licitud de recuperació de còpies de seguretat.
d) Recepció de llistats amb el precinte de seguretat trencat.
e) Pèrdua i/o robatori de llistats.
f) Pèrdua i/o robatori de suports (disquets, cintes, etc.)
g) Pèrdua i/o robatori de dispositius (ordinadors, pda's, telèfons mòbils, etc.)
h) Pèrdua i/o robatori de targetes magnètiques, certificats digitals, etc.

13. DIFUSIÓ I CONSCIENCIACIÓ EN MATÈRIA DE SEGURETAT

L'Organització promourà el coneixement d'aquesta norma i la conscienciació en matèria de seguretat de la informació.

Aquesta norma serà publicada a la Intranet municipal per donar-li la màxima difusió.

La norma s'anirà revisant i actualitzat per garantir la seva adequació als avanços tècnics que s'implantin a l'Ajuntament de Barcelona, així com per establir les recomanacions necessàries conforme vagin apareixent noves vulnerabilitats i amenaces per als sistemes d'informació.

L'IMI comunicarà mitjançant correu electrònic (IMI: Informa) la publicació de noves versions d'aquesta norma i alhora la publicarà a la web municipal.