

Condicions del servei de comunicacions i notificacions electròniques

L'acceptació comportarà el consentiment de la persona interessada per rebre per mitjans electrònics qualsevol notificació amb efectes jurídics que es pugui derivar d'aquest procediment.

Les notificacions i les comunicacions electròniques es dipositaran a la seu electrònica de l'ajuntament de Montornès del Vallès https://www.montornes.cat/seu_electronica/informacio-municipal. El sistema de notificacions i comunicacions electròniques enviarà a la persona interessada, a títol merament informatiu, un SMS i/o correu electrònic informant-la del dipòsit de la notificació/comunicació.

Per a l'acreditació de l'accés de la persona interessada al contingut de les notificacions caldrà la identificació i autenticació de la mateixa amb algun dels dos mecanismes següents:

- a) Mitjançant certificat digital (DNI electrònic, certificat IdCat,...)
- b) Mitjançant una contrasenya d'un sol ús, que s'enviarà al número de telèfon mòbil o adreça de correu electrònic indicats en aquesta sol·licitud. Aquesta opció només estarà disponible quan la notificació o la comunicació permeti aquest tipus d'identificació. En la utilització d'aquest sistema es recomanable aplicar les consideracions de seguretat esmentades al final d'aquest formulari.

Per l'accés al contingut de les comunicacions únicament cal la identificació de la persona interessada.

Pel que fa a les notificacions electròniques de conformitat amb l'establert en l'article 43 de la Llei 39/2015, d'1 d'octubre, de procediment administratiu comú de les administracions públiques la notificació per mitjans electrònics s'entén rebutjada a tots els efectes i l'acte en donarà per notificat, si, un cop s'ha acreditat la posada a disposició a la persona interessada o a la persona representant, i han transcorregut deu dies naturals sense accedir-ne al contingut, o bé cinc dies en els expedients de contractació.

Consideracions de seguretat per a l'ús del mecanisme d'identificació basat en l'enviament de contrasenyes d'un sol ús al telèfon mòbil o a una adreça de correu electrònic

1. Les paraules de pas d'un sol ús:

- Només es poden fer servir per accedir al sistema que l'està sol·licitant
- Tenen una vigència temporal limitada (en general de 30 minuts)
- Només es poden fer servir en una transacció
- Són d'ús personal i intransferible

2. Donat que la paraula de pas s'envia a través del mitjà electrònic seleccionat per l'usuari, part de la seguretat global del sistema passa per la seguretat que s'apliqui en aquest mitjà.

En general, es aconsellable tenir en compte les recomanacions següents:

a) Correu electrònic

- Fer servir contrasenyes d'accés a la bústia de correu prou robustes (combinacions de lletres, números i caràcters especials amb una llargària no inferior a 8 caràcters) i canviar-les amb una periodicitat no inferior a un any.
- Fer servir un compte de correu electrònic d'ús exclusiu i mai comptes de correu d'ús col·lectiu.
- si es té alguna sospita que el mitjà ha estat compromès des del punt de vista de la seguretat (intents d'accés, evidències d'accés d'origen desconegut, etc.) cal canviar immediatament la contrasenya d'accés al correu electrònic.
- Mantenir els equips amb els que s'accedeix al correu electrònic lliure de programari malintencionat. Es recomana fer servir antivirus fiables amb regularitat.
- Mantenir actualitzat el sistema operatiu i navegadors amb els que s'accedeix al correu electrònic.
- En cas d'accedir al servei que requereix la paraula de pas des d'un equip d'ús públic, tancar la sessió i el navegador un cop finalitzat l'ús d'aquest.

b) Telèfon mòbil

- Cal protegir amb una contrasenya l'accés al dispositiu (preferiblement numèrica, no de patró) i cal configurar que el bloqueig es dispari automàticament en tancar o transcorregut un període de temps.
- Cal protegir amb una contrasenya el desbloqueig de la targeta SIM.
- En cas de pèrdua o robatori de l'aparell, cal donar-lo de baixa immediatament seguint el procediment que l'operador hagi indicat. En general, cal tenir apuntat el codi IMEI que identifica el dispositiu.
- Mantenir el telèfon lliure de programari malintencionat. Es recomana fer servir antivirus fiables amb regularitat.
- Mantenir actualitzat el sistema operatiu del telèfon