

REGLAMENT PER LA PRESTACIÓ DE SERVEIS EN MODALITAT DE TELETREBALL DE L'AJUNTAMENT D'ARGENTONA

Article 1. Objecte

El Reglament de Teletreball de l'Ajuntament d'Argentona té per objecte regular la prestació de serveis del personal en la modalitat no presencial mitjançant el teletreball, entesa com a forma d'organització del treball, en virtut de la qual la jornada laboral es desenvolupa de manera no presencial i mitjançant l'ús de les tecnologies de la informació i la comunicació, sense que sigui d'aplicació en situacions excepcionals provocades per crisis sanitàries o altres circumstàncies que aconsellin o obliguin a prestar el servei fora dels llocs de treball ordinaris.

Aquest reglament concreta el procediment per autoritzar i desenvolupar la prestació de serveis en la modalitat de teletreball, com a mesura destinada al personal d'aquest Ajuntament que desenvolupi funcions susceptibles de realitzar-se sota aquesta modalitat.

La prestació del servei mitjançant la modalitat de teletreball serà considerada com a excepcional, considerant la modalitat presencial la ordinària de treball.

Article 2. Definició

2.1 S'entén per teletreball aquella modalitat de prestació de serveis a distància, en la qual el contingut competencial del lloc de treball pot desenvolupar-se, sempre que les necessitats del servei ho permetin, fora de les dependències de l'Administració, mitjançant l'ús de tecnologies de la informació i comunicació.

2.2 La modalitat de prestació de servei per teletreball té caràcter voluntari.

Article 3. Àmbit d'aplicació

Aquest reglament serà d'aplicació al personal laboral i funcionari, inclòs a l'àmbit subjectiu de l'Acord regulador de les condicions de treball dels/de les empleats/ades públics/iques de l'Ajuntament d'Argentona vigent.

No serà d'aplicació al personal exclòs de l'àmbit subjectiu d'aplicació de l'Acord regulador de condicions de treball, ni al personal laboral amb contracte de formació, pràctiques, període de prova, plans d'ocupació en col·laboració, que es regiran, en tot cas, per les estipulacions del corresponent contracte i/o per la resolució per la qual s'atorga la subvenció.

Article 4. Requisits per prestació de serveis en la modalitat de teletreball

4.1. Les persones treballadores de l'Ajuntament d'Argentona que tenen dret a



prestar serveis sota la modalitat de teletreball hauran de complir i acreditar els següents requisits:

- Estar en situació de servei actiu a l'Ajuntament d'Argentona i amb una antiguitat mínima de 6 mesos consecutius en el lloc de treball des del que es sol·liciti el teletreball.
- Exercir un lloc de treball que es consideri susceptible de ser desenvolupat en la modalitat de teletreball. A aquest efecte, es consideren llocs de treball susceptibles de ser exercits en la modalitat de teletreball aquells en què les tasques principals es poden desenvolupar de manera autònoma, sense necessitat de supervisió presencial o guiatge continuats, ateses les seves característiques específiques i els mitjans requerits per desenvolupar-los. (Annex 3)
- Tenir els coneixements informàtics i telemàtics, teòrics i pràctics suficients que requereix el desenvolupament de les funcions del seu lloc en la modalitat de teletreball.
- Disposar de sistemes de comunicació i connectivitat suficients i segurs.
- Disposar d'un espai de treball amb les condicions mínimes d'ergonomia i seguretat.
- Disposar de l'autorització per exercir la prestació del servei en la modalitat del teletreball.
- El compliment dels requisits que estableix aquest article s'han de mantenir durant tot el període de temps en què la persona presti el seu servei en la modalitat de teletreball.

4.2 Llocs de treball exclosos de prestació de servei en la modalitat de teletreball:

- a) Llocs de treball en oficines de registre presencial i atenció i informació al ciutadà de manera presencial.
- b) Llocs de treball que impliquin necessàriament la prestació del servei de manera presencial (policies, brigada, operaris de manteniment, inspecció, serveis d'atenció personalitzada al ciutadà, ...)

A l'Annex 3 es recull el llistat de llocs de treball amb indicació de si es considera susceptible de ser desenvolupat en la modalitat de teletreball. En cas que calgui modificar l'annex per la inclusió, supressió o modificació es farà per resolució d'alcaldia.



Article 5. Règim general i excepcional de la prestació de serveis en la modalitat de teletreball

5.1 Jornada i horari

La jornada i l'horari en la modalitat de teletreball serà la mateixa que ja ve regulada a l'Acord regulador de condicions comuns del personal del servei de l'ajuntament d'Argentona, i allò que es reculli cada any al calendari laboral anual així com en les diferents fitxes de lloc de treball on consta la peculiaritat a la que es troba subjecte cada lloc de treball.

El règim de permisos i llicències vigent també inclourà les jornades planificades de teletreball.

La persona treballadora mantindrà l'obligació de registrar la jornada diària de teletreball a través dels mitjans destinats a aquesta finalitat i inclourà els fitxatges corresponents (entrada, descansos, permisos, sortida ...).

Durant la jornada de teletreball s'haurà de desviar les trucades del telèfon corporatiu (cisco) a un número de telèfon a efectes de poder rebre trucades com si prestessin serveis presencialment. Així mateix aquells que ho vulguin poden facilitar un número de telèfon en el que poder ser localitzats si no disposen de telèfon corporatiu.

L'Ajuntament estudiarà, les característiques a implementar en un futur en la modalitat de teletreball, l'anomenada política de taules calentes, si ho aconsellen les necessitats organitzatives. D'aquesta manera els treballadors que tinguin autoritzat el teletreball, passarien a compartir taula, en funció dels dies de treball presencials.

5.2 Regim general en la prestació del servei en la modalitat de teletreball

- a) Quan per raó d'un servei, formació, visites mèdiques o altres permisos fora del centre de treball habitual el desplaçament resulti ineficient, entenent per ineficient un temps de treball presencial inferior a la meitat de la jornada, a l'inici o final de la jornada. En aquest cas la jornada restant es pot completar en règim de teletreball, prèvia conformitat del cap i/o responsable per escrit.
- b) Quan per necessitats del servei es derivin encàrrecs específics i concrets que calgui executar en un breu període de temps i sigui més efectiu i adequat emprar la modalitat de teletreball, sempre i quan es tingui la conformitat del cap i/o responsable per escrit.
- c) Quan es declarin episodis ambientals de contaminació o altres situacions d'emergència derivades de plans de protecció civil, sense necessitat de sol·licitud prèvia i d'acord amb les instruccions que proporcioni el Servei de Recursos Humans per cada cas concret.



d) Quan per estats de convalescència de la persona treballadora, per la seva naturalesa, sigui recomanable mantenir repòs. El número de dies en règim de teletreball s'adaptarà a la prescripció de repòs fixada pel metge de treball mitjançant informe mèdic emès a petició de l'ajuntament.

El règim general en la prestació del servei en la modalitat teletreball serà aplicable als llocs de treball que siguin considerats susceptibles de ser desenvolupat en la modalitat de teletreball d'acord amb l'Annex 3.

5.3 Regim excepcional en la prestació del servei en la modalitat de teletreball

Les persones treballadores que per fer efectiu el seu dret de conciliació entre la vida familiar i laboral necessitin prestar serveis en la modalitat de teletreball, ho podran sol·licitar si reuneixen els següents requisits i en les següents condicions:

- Tinguin fills o filles menors a 12 anys, i no gaudeixin d'una reducció de jornada.
- Tinguin familiars de 1r grau, cònjuge o parella de fet en situació de dependència, segons l'establert a la llei 39/2006, de 14 de desembre, de Promoció de la Autonomia Personal i Atenció a las persones en situació de dependència i no gaudeixin d'una reducció de jornada ni percebin cap ajut per aquest concepte per part de l'ajuntament.
- Ocupin un lloc de treball que es consideri susceptible de ser desenvolupat en la modalitat de teletreball.
- Els llocs de teletreball són limitats als departaments, segons les necessitats del servei.
- La modalitat de teletreball es distribuirà de manera que es puguin fer fins a un màxim de dues jornades senceres, de tal manera que cada jornada duta a terme no podrà ser fraccionada en la modalitat de teletreball i la modalitat presencial.
- Es fixarà el dia de les jornades establertes en l'apartat anterior, que només podran ser modificada en casos excepcionals
- Durant les jornades de teletreball, per necessitats del servei degudament justificades i amb un preavís no inferior a vint-i-quatre hores, es podrà exigir la presència física obligatòria a reunions de treball.
- La modificació dels dies concrets assignats en la modalitat de teletreball, s'haurà d'acordar amb la persona responsable del servei, sense que en cap cas superi el nombre màxim de dos dies.



- Excepcionalment, si el dia que es té assignat la modalitat de teletreball es requereix la presència física en una franja concreta, si no es modifica el dia de teletreball, es podrà dur a terme la resta de jornada en la modalitat de teletreball.
- L'Ajuntament pot requerir en qualsevol moment que el treballador doni compte del treball realitzat durant la jornada de teletreball. Aquest requisit es considera imprescindible per un desenvolupament seriós del procés de teletreball.

5.3.1 Durada

La durada de la prestació de serveis en la modalitat excepcional de teletreball serà mentre duri la causa que l'ha motivat o com a màxim fins que el fill o filla compleixi els 12 anys d'edat, o la persona treballadora ja no tingui familiars a càrrec d'acord amb la llei de dependència que ho haurà de comunicar immediatament.

L'autorització de la prestació de serveis en la modalitat excepcional de teletreball podrà deixar-se sense efectes quan hi hagi una avaluació desfavorable per part de la persona responsable o per la renúncia de la persona interessada, mitjançant la corresponent resolució.

5.3.2. Sol·licitud, autorització i revocació

Les persones interessades en prestar serveis en la modalitat excepcional de teletreball poden presentar la sol·licitud d'autorització de teletreball mitjançant instància, a través del model específic de sol·licitud de teletreball (annex 1) a la qual s'haurà d'omplir la declaració d'autoavaluació de riscos laborals de teletreball voluntari (annex 4).

Cal que indiquin a la sol·licitud els dies concrets de la setmana i el domicili on prestaran el servei en la modalitat de teletreball.

La persona teletreballadora haurà d'incloure a la sol·licitud de teletreball el compromís (annex 2) de complir la normativa en matèria de protecció de dades, de confidencialitat, i l'aplicació de polítiques de seguretat aprovades a tal efecte.

5.3.3 Informe de la persona responsable del servei o àrea

En el termini màxim de quinze dies a comptar des de la presentació de la sol·licitud, la persona responsable del servei o àrea en el qual presti serveis la persona sol·licitant elevarà un informe al Servei de Recursos Humans.

Els responsables polítics realitzaran aquesta funció per al personal sense superior jeràrquic.



L'informe serà desfavorable a l'autorització en el cas del personal exclòs de l'àmbit subjectiu d'aplicació d'aquest reglament, quan no es compleixin els requisits per a la prestació de serveis en la modalitat de teletreball, o quan concorrin necessitats del servei degudament justificades. En aquest cas es donarà audiència a la persona sol·licitant.

L'informe favorable ratificarà la sol·licitud pel que fa al nombre de jornades a realitzar en modalitat de teletreball i als dies sol·licitats. L'informe podrà ser favorable a l'autorització però condicionat a la modificació dels dies a realitzar la prestació del servei en la modalitat de teletreball. En aquest cas, també es donarà audiència a la persona sol·licitant.

La persona responsable haurà de dur a terme el seguiment de la feina realitzada, posant atenció a l'assoliment de les següents competències en el desenvolupament del lloc de treball, entre d'altres aspectes que pugui considerar:

- Organització i planificació: capacitat per definir les accions, terminis i recursos necessaris de cada projecte, considerant la seva importància i la seva urgència. Organitzar i gestionar el temps, establir prioritats i avaluar el propi rendiment. Coneixement de la dificultat de les tasques i control del temps necessari per dur-les a terme.
- Orientació a resultats: capacitat per orientar la feina a l'assoliment dels objectius amb la màxima qualitat i la menor despesa de recursos possible. Definir un sistema d'indicadors per conèixer el grau d'assoliment dels resultats i fer-ne el seguiment. Pro activitat per plantejar-se objectius de creixement professional i millora del servei.
- Autonomia i responsabilitat: capacitat de realitzar una tasca de forma independent, executant-la de principi a fi, sense necessitat de rebre supervisió constant. Treballar amb autonomia, actuar de forma proactiva i responsabilitzar-se de la seva feina i l'assoliment dels objectius encarregats.
- Flexibilitat i capacitat d'adaptació: adaptar-se de manera àgil i positiva a demandes i situacions diferents. Acceptar i valorar noves idees, mostrar actitud positiva vers els canvis i tenir inquietud per conèixer altres àmbits.
- Comunicació: capacitat per comunicar-se de forma clara i precisa. Capacitat de dominar els canals de comunicació que ha d'utilitzar, i escollir els més adequats per a cada situació i/o persona o col·lectiu receptor.

5.3.4 Resolució d'Alcaldia



Des del servei de Recursos Humans s'emetrà un informe proposta de resolució motivada d'autorització o denegació de la sol·licitud de teletreball en un termini màxim de dos mesos, la qual serà resolta per l'Alcaldia.

La resolució desestimarà la sol·licitud en els supòsits de personal exclòs de l'àmbit subjectiu d'aplicació d'aquesta mesura, quan no es compleixin els requisits per a la prestació de serveis en la modalitat de teletreball, o quan concorrin necessitats dels serveis degudament justificades.

La resolució d'autorització fixarà la durada de la prestació de serveis en règim de teletreball, el nombre de jornades setmanals a realitzar en modalitat de teletreball, els dies de la setmana en els quals es desenvoluparà, així com la persona que exercirà la supervisió. La resolució d'autorització establirà la data de l'inici efectiu de la prestació de serveis en la modalitat de teletreball.

La persona teletreballadora haurà d'incloure a la sol·licitud de teletreball el compromís de complir la normativa en matèria de protecció de dades, de confidencialitat, i l'aplicació de polítiques de seguretat aprovades a tal efecte.

5.3.5 Supòsits de suspensió, deixar sense efectes, revocació

L'autorització de prestació de serveis en modalitat de teletreball restarà sense efectes, de manera automàtica, en cas de canvi de lloc de treball de la persona autoritzada o en cas que hi renunciï expressament.

L'autorització de prestació de serveis en la modalitat de teletreball es podrà suspendre automàticament pel funcionament deficient de l'equip informàtic, dels sistemes de comunicació i connectivitat i per la desatenció del telèfon per un període superior a un dia.

En aquest supòsit, la persona autoritzada ha de prestar serveis en règim presencial fins que aquests problemes es resolguin. No obstant, el mateix dia en que es produeixi la deficiència podrà optar per desplaçar-se al centre de treball o sol·licitar horari recuperable.

Així mateix, mitjançant una resolució, la prestació de serveis en la modalitat de teletreball es podrà suspendre temporalment en els casos següents:

- a) Per circumstàncies sobrevingudes que requereixin la presencialitat de la persona autoritzada, fins que aquestes circumstàncies desapareguin.
- b) Per necessitats dels serveis degudament justificades que requereixin la presencialitat de la persona autoritzada, fins que aquestes es resolguin.

L'autorització per teletreballar pot ser revocada per l'òrgan que l'ha autoritzada, per qualsevol de les causes següents:





- a) Incompliment dels deures de la persona teletreballadora consignats en el present reglament, el que inclou el deure d'estar localitzable durant tota la jornada laboral.
- b) Per necessitats del servei degudament justificades.
- c) Per dificultats tecnològiques degudament justificades que el facin inviable durant un període superior a dos dies, n aquest cas es podran autoritzar en quan desapareguin.
- d) Per incompliment acreditat dels objectius o dels deures i obligacions establerts.
- e) Per inobservança de les normes i recomanacions en matèria de seguretat informàtica i de protecció de dades de caràcter personal i prevenció de riscos laborals com la connexió des de llocs inadequats.

Article 6. Drets i deures de les persones que presten serveis en la modalitat de teletreball

El personal que presti serveis en la modalitat de teletreball té els drets i deures següents:

- a) Drets i deures idèntics que la resta del personal al servei de l'Ajuntament d'Argentona, sense que pugui haver cap afectació retributiva ni diferència en les oportunitats de formació, promoció professional ni cap altre dret.
- b) Dret a la desconexió digital, respectar el temps de descans i a la intimitat personal, en els termes establerts en l'article 88 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- c) Dret a renunciar, en qualsevol moment, a la prestació de serveis en modalitat de teletreball, donat que és una modalitat de caràcter voluntari.
- d) Deure de complir la normativa en matèria de protecció de dades de caràcter personal i de mantenir reserva respecte als assumptes que conegui.
- e) Deure de complir la normativa en matèria de prevenció de riscos laborals.
- f) Deure de complir amb la normativa de seguretat i interoperabilitat en relació a l'intercanvi de dades, signatura electrònica i format de documents.
- g) Deure de dur a terme la formació que es proposi per la Corporació en matèria de ciberseguretat, protecció de dades, prevenció de riscos laborals.
- h) Resta rotundament prohibit treballar fora de l'entorn "R" i el gestor d'expedients, així com imprimir qualsevol document o guardar-lo fora de l'entorn indicat.





- i) L'Ajuntament habilitarà els mecanismes de control horari a efectes de registrar la jornada realitzada en la modalitat de teletreball i, si escau, dictarà les instruccions que siguin necessàries per al compliment de la jornada i horari de treball.
- j) Deure de superar, obligatòriament i amb anterioritat a la concessió del teletreball la formació específica indicada a la Normativa Interna de l'ús de mitjans electrònics de l'ajuntament d'Argentona.
- k) Les persones teletreballadores hauran de garantir el compliment del que preveu la normativa sobre protecció de dades de caràcter personal, (lleï orgànica 3/2018 de 5 de desembre), el compliment de totes les mesures de seguretat, així com el deure a la confidencialitat de la informació i les dades facilitades per al seu treball. En particular, es prohibeix emmagatzemar o tractar dades confidencials o de caràcter personal en suports o plataformes diferents de les autoritzades de forma expressa per l'Ajuntament
- l) En la modalitat de teletreball s'estableix la teledisponibilitat.
- m) El teletreball no es permès en dies festius ni dies no laborables, excepte en aquells que sigui inherent a la naturalesa de les funcions, subjecció de terminis o prestació del servei públic amb autorització expressa en l'autorització, ni més enllà de la franja horària autoritzada.
- n) Que hagin transcorregut 1 any des de la revocació d'una autorització de teletreball, per avaluació desfavorable d'alguns dels objectius o compromisos fixat.

L'Annex 5 conté les directrius de ciberseguretat en els sistemes corporatius que ha elaborat la Diputació de Barcelona adaptada al nostre ajuntament. Aquestes directrius són de lectura imprescindible ja que les indicacions que s'hi contemplen són molt importants.

Article 7. Mitjans tecnològics i materials per a la prestació de serveis en la modalitat de teletreball

L'Ajuntament d'Argentona posarà a disposició de la persona teletreballadora l'accés remot ubicat a la xarxa Corporativa de l'Ajuntament d'Argentona.

El personal que presti serveis en modalitat teletreball haurà de comptar amb un sistema de connexió informàtica suficient i segur en el seu domicili, perquè hi pugui exercir les tasques pròpies del seu lloc de treball en idèntiques condicions a com serien executades de manera presencial. L'equip des del qual s'estableixi la connexió ha d'estar lliure de virus, disposar d'un programari d'antivirus actualitzat i



amb l'anàlisi completa de seguretat duta a terme. El sistema operatiu de l'equip físic ha d'estar suportat pel fabricant, de manera que existeixin actualitzacions de seguretat per a aquesta versió del sistema operatiu.

Amb caràcter previ el personal informàtic es podrà connectar remotament per tal de supervisar la connexió i garantir que es compleixen aquests requisits, el qual informará de la viabilitat de realitzar la jornada en teletreball.

El personal que no disposi de l'equip informàtic necessari podrà sol·licitar-lo a l'administració. La persona treballadora mantindrà aquest equip informàtic en el mateix estat i amb la mateixa configuració que tenia al lliurament. Aquest equip pot ser compartit, de manera que caldrà retornar-lo cada dia.

L'equip informàtic haurà de ser tornat a l'administració quan així es requereixi o quan finalitzi la prestació de serveis en modalitat teletreball.

En qualsevol cas, la persona treballadora posarà els mitjans que siguin necessaris per tal de garantir la confidencialitat de l'emissió i recepció de dades, i donar compliment a les normes vigents sobre protecció de dades de caràcter personal.

En el cas que es produeixi un mal funcionament en l'equip informàtic o les aplicacions instal·lades que impedeixin el treball en el domicili i que no pugui ser solucionat el mateix dia, la persona treballadora haurà de reincorporar-se al centre de treball durant el mateix dia o, si no fos possible per causa justificada, l'endemà o següent dia laborable, tot reprenent l'exercici en la modalitat de teletreball quan s'hagi solucionat l'esmentat problema de caràcter tècnic.

La persona que realitzi la modalitat de teletreball haurà de disposar d'un equip informàtic i un dispositiu telefònic i es farà càrrec dels costos, tant directes com indirectes associats a la prestació dels serveis a distància: connexió a internet, llum, calefacció, mobiliari ergonòmic, etc.

El servei de Sistemes d'Informació podrà requerir en qualsevol moment a la persona teletreballadora perquè modifiqui o adapti la configuració de l'equipament amb la finalitat de garantir la seva idoneïtat i seguretat.

Article 8. Seguretat i salut en el teletreball

El lloc on es desenvolupi el teletreball haurà de complir la normativa vigent en matèria de prevenció de riscos laborals, en especial en allò que fa referència amb la seguretat i l'ergonomia.



En el moment de la sol·licitud del teletreball, la persona teletreballadora haurà d'omplir la declaració d'autoavaluació de riscos laborals (annex 4), en la qual la persona teletreballadora es responsabilitza del compliment d'allò que ha declarat en el qüestionari, així com l'adopció de les mesures correctores que se li proposin.

Als efectes de contingències professionals serà aplicable la normativa vigent en matèria d'accidents de treball i malalties professionals.

La persona teletreballadora haurà de realitzar tota la formació que es proposi per la correcta prestació de serveis en la modalitat de teletreball impartida pel servei de Prevenció de Riscos Laborals.

Disposició addicional

Els preceptes d'aquest Reglament que per raons sistemàtiques reproduïxin aspectes de la legislació vigent i altres normes de desenvolupament, i aquells en què es facin remissions a preceptes d'aquesta, s'entendrà que són automàticament modificats i/o substituïts en el moment en què es produeixi la modificació dels preceptes legals i reglamentaris de què porten causa.

Disposició transitòria

Les persones treballadores que actualment prestin els seus serveis en la modalitat de teletreball i estiguin interessats en continuar prestant serveis en la modalitat de teletreball, hauran de presentar la sol·licitud corresponent en el termini d'un mes a partir de l'entrada en vigor del present reglament. Fins a la resolució de l'autorització, si s'escau, podran continuar prestant serveis en aquesta modalitat, tal i com es venien fent fins ara.

Disposició derogatòria

Resten sense efecte les anteriors previsions establertes envers el teletreball a partir de l'endemà de l'entrada en vigor d'aquest Reglament.

Disposició final

D'acord amb el que preveu l'article 70.2 de la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, aquest reglament entrarà en vigor una vegada s'hagi publicat el seu text complet en el Butlletí Oficial de la Província; i hagi transcorregut el termini de 15 dies hàbils previst a l'article 65.2 del mateix text legal.





ANNEX 1

SOL·LICITUD TELETREBALL

Cognoms	Nom
DNI	Lloc de treball
Horari laboral:	

SOL·LICITO ACOLLIR-ME A LA PRESTACIÓ DE SERVEIS EN MODALITAT TELETREBALL EN RÈGIM ESPECIAL pel següent motiu:

Tenir fills/es menors de 12 anys

Tenir familiar de 1r grau o cònjuge en situació de dependència

El/s dia/es de la setmana que desitjo acollir-me a la prestació de serveis en modalitat teletreball és/són:

Dilluns

Dimarts

Dimecres

Dijous

Divendres

L'adreça en la que prestaré els serveis a afectes de poder considerar un accident, en cas que es produeixi, *in itinere*:

CONFIRMO QUE:

He signat el [compromís de confidencialitat](#) (annex 2), el qual adjunto

He omplert el [qüestionari d'autoavaluació](#) del desenvolupament del teletreball (annex 4)
(accedir a l'enllaç per omplir el qüestionari)

He llegit les [directrius de ciberseguretat](#)

Signatura treballador/a

Signatura Responsable

Signatura de Recursos Humans



ANNEX 2. COMPROMÍS DE CONFIDENCIALITAT

En/Na _____, que presta els seus serveis com a _____ a l'ajuntament d'Argentona, em comprometo quan presti serveis sota la modalitat de teletreball a:

La confidencialitat i a protegir la seguretat de les dades de caràcter personal i de la informació que utilitzi i a la que pugui accedir, evitant per tots els mitjans possibles la seva alteració, la pèrdua, el tractament o l'accés no autoritzat o bé el seu ús inadequat.

S'ha de tenir cura del tractament de tota la informació, estigui en suport digital o analògic. La persona teletreballadora és la responsable de l'ús fraudulent que es pugui fer ús de les dades a les que té accés, per la qual cosa ha de vetllar per mantenir l'ordinador amb claus d'accés que no conegui ningú del seu entorn, no deixar les pantalles obertes quan deixi l'ordinador, no es pot imprimir cap tipus de documentació ni extreure documentació en suport físic de l'Ajuntament.

Les dades a les que tingui accés la persona treballadora no es podran allotjar en dispositius fora del servidor de l'Ajuntament ni en entorn local. L'equipament posat a disposició per part de l'empresa és d'ús exclusiu per al desenvolupament de la feina.

En garantia del compliment de la seguretat i la protecció de les dades corporatives, si es detecta que s'està vulnerant l'ús, l'empresa podrà eliminar totes les dades i aplicacions no corporatives.

En cas de detectar-se un robatori dels dispositius corporatius o d'ús corporatiu o un accés indegut a dades a les que es pugui tenir accés mitjançant aquests, caldrà avisar **immediatament** a l'enllaç amb el Delegat de protecció de dades (secretària municipal) i al Responsable de Seguretat (informàtic), per tal d'activar les accions necessàries per a la seguretat de les mateixes. No es permet la connexió a xarxes públiques d'Internet o no segures. Quan s'utilitzi un ordinador privat, propietat de la persona treballadora, caldrà que aquest disposi d'un programa d'antivirus actualitzat així com les versions més actualitzades de navegadors i de sistemes operatius. La persona treballadora haurà de seguir, en tot moment, les recomanacions de seguretat que es vagin publicant des del Servei de Tecnologia i Desenvolupament digital sobre la política de seguretat en el teletreball i mantenir-se actualitzada en matèria de ciberseguretat.

DATA

SIGNATURA



ANNEX 3. Llocs teletreball

DENOMINACIÓ LLOC DE TREBALL	Teletreball
ADJUNT D'INTERVENCIÓ	Si
ADMINISTRATIU/VA	Si
AGENT DE LA POLICIA LOCAL	No
AGENT DE LA POLICIA LOCAL DE PROXIMITAT	No
ARQUITECTE/A	Si
ARQUITECTE/A TÈCNIC/A	Si
ARXIVER/A	Si
ASSESSOR/A JURÍDIC	Si
AUXILIAR DE BIBLIOTECA	No
AUXILIAR DE GESTIÓ ADMINISTRATIVA	Si
AUXILIAR DE SERVEIS	No
AUXILIAR DE SERVEIS - ESCOLA	No
AUXILIAR DE SERVEIS - POLIVALENT	No
AUXILIAR DE SERVEIS INSTAL.LACIONS ESPORTIVES	No
CAP DE L'ÀREA D'ALCALDIA	Si
CAP DE L'ÀREA DE SERVEIS PERSONALS	Si
CAP DE L'ÀREA DE SERVEIS TERRITORIALS	Si
CAP DE L'OAC	Si
CAP DE NEGOCIAT DE SERVEIS GENERALS	Si
CAP DE NEGOCIAT DE SERVEIS PERSONALS	Si
CAP DE NEGOCIAT DE SERVEIS TERRITORIALS	Si
CAP D'UNITAT	Si
CAPORAL DE LA POLICIA LOCAL	No
COORDINADOR EQUIP DE PLANEJAMENT, GESTIÓ URBANÍSTICA I OBRA PÚBLICA	Si
COORDINACIÓ EQUIP TÈCNIC DE LLICÈNCIES, OBRES I GESTIÓ	Si
COORDINACIÓ EQUIP JURÍDIC I PROJECTES ESTRATÈGICS	Si
DINAMITZADOR/A DE JOVENTUT	No
DIRECTOR/A DE LA RÀDIO MUNICIPAL	Si
EDUCADOR/A SOCIAL	No
ENCARREGAT/DA D'AUXILIAR DE SERVEIS	No
ENCARREGAT/DA DE LA BRIGADA D'OBRES I SERVEIS	No
ENGINYER/A	Si
ENGINYER/A TÈCNIC/A D'URBANISME I OBRES	Si
GESTOR/A ADMINISTRATU/VA	Si
INFORMADOR/A - TRAMITADOR/A OAC	No
INSPECTOR/A DE LA POLICIA LOCAL - CAP DE POLICIA	No
INSPECTOR/A DE VIA PÚBLICA, OBRES I MEDI AMBIENT	No
INTEGRADOR/A SOCIAL	No
INTERVENTOR/A	Si
LOCUTOR/A	No
OFICIAL BRIGADA OBRES I SERVEIS	No
OFICIAL BRIGADA OBRES I SERVEIS - CEMENTIRI	No
OPERARI/A BRIGADA OBRES I SERVEIS	No
OPERARI/A BRIGADA OBRES I SERVEIS - CEMENTIRI	No
PERIODISTA	No
PSICÒLEG/A	Si
RESPONSABLE INSTAL.LACIONS I EQUIPAMENTS	Si
RESPONSABLE DE BIBLIOTECA I ARXIU	No
SECRETARI/A	Si
SECRETARI/A D'ALCALDIA	Si
SERGEANT DE LA POLICIA LOCAL	No
TÈCNIC/A AUXILIAR DE CULTURA I FESTES	Si
TÈCNIC/A AUXILIAR DE COMUNICACIÓ	Si
TÈCNIC/A AUXILIAR DE RÀDIO	Si
TÈCNIC/A DE COMUNICACIÓ, TRANSPARÈNCIA I PARTICIPACIÓ	Si
TÈCNIC/A DE CULTURA I FESTES	Si
TÈCNIC D'INSERCIÓ SOCIOLABORAL	Si
TÈCNIC SUPERIOR D'ADMINISTRACIO DIGITAL I TRANSPARENCIA	Si
TÈCNIC/A DE GESTIÓ URBANÍSTICA I CADASTRAL	Si
TÈCNIC/A DE JOVENTUT	Si
TÈCNIC/A DE MEDI AMBIENT I SANITAT	Si
TÈCNIC/A DE PLA DE COHESIÓ	No
TÈCNIC/A DE PREVENCIÓ DE RISCOS LABORALS JP	Si
TÈCNIC/A DE PROJECTES	Si
TÈCNIC/A DE PROMOCIÓ ECONÒMICA	Si
TÈCNIC/A DE RECURSOS HUMANS	Si
TÈCNIC/A DE SERVEIS ECONÒMICS	Si
TÈCNIC/A DE SERVEIS MUNICIPALS	Si
TÈCNIC/A D'EDUCACIÓ I FORMACIÓ	Si
TÈCNIC/A D'ESPORTS	Si
TÈCNIC/A INFORMÀTIC/A	Si
TREBALLADOR/A FAMILIAR - DINAMITZADOR/A	No
TREBALLADOR/A SOCIAL	Si
TRESORER/A	Si

ANNEX 4. Formulari autoavaluació del teletreball

Instruccions per a omplir el qüestionari

- Recolliu-hi únicament la informació de les condicions específiques del lloc en què teletrebal·leu (ordinador, elements auxiliars, etc.) a casa vostra o al lloc on dureu a terme el teletreball.
- Respongueu a cada ítem de la manera següent:
 - **Resposta afirmativa:** les condicions de treball són adequades. No és necessari prendre cap mesura.
 - **Resposta negativa:** es recomana que prengueu mesures per adequar el vostre lloc de treball. Si no podeu aplicar la mesura de millora, us podeu posar en contacte amb Prevenció de Riscos Laborals (prl@argentina.cat), que analitzarà el vostre cas.

* Indica que la pregunta és obligatòria

1. Nom i cognoms *

EQUIP

Pantalla

2. Els caràcters de la pantalla estan ben definits, estan configurats de manera clara i tenen una dimensió suficient. (La majoria dels programes utilitzats actualment permeten ajustar les característiques per a facilitar la lectura dels caràcters.) *

Marqueu només un oval.

☐ Sí

☐ No



3. La lluminositat i el contrast entre els caràcters i el fons de la pantalla són bons. *

Marqueu només un oval.

- ☐ Sí
☐ No

4. La imatge de la pantalla és estable. *

Marqueu només un oval.

- ☐ Sí
☐ No

5. La pantalla no té reflexos ni reverberacions. *

Marqueu només un oval.

- ☐ Sí
☐ No

6. La distància entre la vostra visió i la pantalla és superior a 40 centímetres. *

Marqueu només un oval.

- ☐ Sí
☐ No

7. La distància entre la vostra visió i la pantalla és superior a 40 centímetres. *

Marqueu només un oval.

- ☐ Sí
☐ No



8. L'angle de visió coincideix amb la part superior de la pantalla del vostre ordinador. *

Marqueu només un oval.

- ☐ Sí
- ☐ No

Teclat

9. L'espai davant del teclat és suficient perquè els braços i les mans hi estiguin recolzats. *

Marqueu només un oval.

- ☐ Sí
- ☐ No

10. La disposició del teclat afavoreix, en la mesura del possible, l'alineació entre l'avantbraç, el canell i la mà. *

Marqueu només un oval.

- ☐ Sí
- ☐ No

MOBILIARI DE TREBALL

Taula o superfície de treball



11. La taula o superfície de treball és poc reflectora, i té unes dimensions suficients per a permetre una col·locació flexible de la pantalla, del teclat, dels documents i del material accessori. *

Marqueu només un oval.

- ☐ Sí
☐ No

12. La col·locació de la taula i la cadira permet un espai suficient per a allotjar les cames amb comoditat i per a canviar de postura sense problemes. *

Marqueu només un oval.

- ☐ Sí
☐ No

13. Hi ha espai suficient per a posar els avantbraços davant del teclat. *

Marqueu només un oval.

- ☐ Sí
☐ No

14. Hi ha espai suficient per a col·locar l'equip informàtic, els documents i altres materials de suport. *

Marqueu només un oval.

- ☐ Sí
☐ No

Cadira de treball



15. L'alçada de la cadira és regulable, el respatlle és inclinable i l'alçada es pot ajustar. *

Marqueu només un oval.

- ☐ Sí
☐ No

16. El disseny de la cadira facilita la llibertat de moviments. *

Marqueu només un oval.

- ☐ Sí
☐ No

17. La cadira disposa de cinc rodes. *

Marqueu només un oval.

- ☐ Sí
☐ No

18. La posició dels braços de la cadira no impedeix acostar-se a la taula. *

Marqueu només un oval.

- ☐ Sí
☐ No

Reposapeus



19. Els peus estan ben recolzats a terra (si escau, podeu utilitzar un reposapeus o un element similar). *

Marqueu només un oval.

☐ Sí

☐ No

LLOC DE TREBALL

Espai de treball

20. L'espai de treball està ordenat i facilita la disposició correcta dels diferents materials de teletreball. *

Marqueu només un oval.

☐ Sí

☐ No

21. La superfície de treball és com a mínim de 2 m². *

Marqueu només un oval.

☐ Sí

☐ No

22. El cablejat elèctric o la instal·lació telefònica estan ordenats i no queden en zones de pas. *

Marqueu només un oval.

☐ Sí

☐ No



23. Els aparells elèctrics estan desconnectats quan no s'utilitzen. *

Marqueu només un oval.

- ☐ Sí
☐ No

II·luminació

24. En general, la il·luminació natural es pot complementar amb una d'artificial quan la natural no garanteixi les condicions de visibilitat adequades. En qualsevol cas, el lloc de treball està il·luminat correctament. *

Marqueu només un oval.

- ☐ Sí
☐ No

25. La ubicació del lloc de treball evita els enlluernaments i els reflexos molestos, tant a la pantalla de l'ordinador com directament als ulls. A més de la ubicació de la pantalla, per a evitar aquests enlluernaments i reflexos es fan servir altres elements com cortines, pantalles, persianes... *

Marqueu només un oval.

- ☐ Sí
☐ No

26. La pantalla de l'ordinador està col·locada perpendicularment a les finestres per a evitar enlluernaments i reflexos. *

Marqueu només un oval.

- ☐ Sí
☐ No



Ergonomia

27. Es fan pauses periòdiques mentre es treballa davant de la pantalla de l'ordinador (com per exemple, 10 minuts cada hora). *

Marqueu només un oval.

- ☐ Sí
☐ No

28. L'espai per teletreballar permet la concentració adequada en la tasca. *

Marqueu només un oval.

- ☐ Sí
☐ No

Riscos psicosocials

29. L'horari de treball és regular i es fan les pauses necessàries. *

Marqueu només un oval.

- ☐ Sí
☐ No

30. La distribució de la jornada laboral permet descansar i desconnectar per a fer altres activitats de caràcter personal, sense haver d'estar pendents de la feina. *

Marqueu només un oval.

- ☐ Sí
☐ No



31. Els recursos tecnològics necessaris per a teletreballar, i la informació adequada sobre com s'han d'utilitzar, són adequats. *

Marqueu només un oval.

- ☐ Sí
☐ No

32. Els canals de comunicació periòdics amb els caps i els companys estan ben definits. *

Marqueu només un oval.

- ☐ Sí
☐ No

33. Els objectius de treball, els terminis, les instruccions i els criteris per a fer i prioritzar les activitats són raonables i clars. *

Marqueu només un oval.

- ☐ Sí
☐ No

34. La retroacció de la feina és periòdica. *

Marqueu només un oval.

- ☐ Sí
☐ No



35. La informació que rebeu sobre els nous procediments de treball i sobre els aspectes que us poden afectar en un futur és suficient i adequada. *

Marqueu només un oval.

- ☐ Sí
- ☐ No

36. Pots compatibilitzar la teva feina amb la cura de persones al teu càrrec? Si utilitzes un ordinador compartit, pots combinar bé l'ús de l'ordinador amb la resta de la família? *

Marqueu només un oval.

- ☐ Sí
- ☐ No

Google no ha creat ni aprovat aquest contingut.

Google Formularis



DIRECTRIUS DE CIBERSEGURETAT EN ELS SISTEMES CORPORATIUS DE L'AJUNTAMENT D'ARGENTONA



ÍNDEX

Ciberseguretat	3
Credencials d'accés	4
Protegim les nostres contrasenyes.....	4
Com fer una contrasenya segura i recordar-la	4
Segon factor d'autenticació	5
Canvi de contrasenya a la Ajuntament d'Argentona.....	5
Correu brossa	6
Phishing	6
Detectem i combatem el <i>phishing</i>	7
Correu brossa i phishing a la Ajuntament d'Argentona	7
Programari maliciós (<i>malware</i>)	8
Punts d'entrada típics del <i>malware</i>	8
Segrest d'informació (<i>ransomware</i>)	8
Com combatem el programari maliciós?	8
Dispositius mòbils	10
Aplicacions (apps).....	10
Dispositius mòbils a la Ajuntament d'Argentona	10
Xarxes socials.....	12
Sextorsió o xantatge amb gravacions sexuals	12
Missatgeria instantània	14
Notícies falses i enganys (<i>hoax</i>)	14
Missatgeria instantània a la Ajuntament d'Argentona	14
Navegació segura	16
Com podem saber si un web és segur?	16
Altres recomanacions	16
Galletes (<i>cookies</i>).....	16
Certificats digitals a la Ajuntament d'Argentona	17
El lloc de treball	18
Estacions de treball a la Ajuntament d'Argentona	18
Estacions de treball en remot a la Ajuntament d'Argentona.....	18



Ciberseguretat

A mesura que creix l'ús de la tecnologia a la feina i en l'àmbit personal, estem sotmesos a més riscos dels entorns digitals i a ciberamenaces com ara el robatori de dades personals, la usurpació de personalitat i altres frauds.

En aquest document hi trobareu informació i consells per fer un **ús més segur dels recursos tecnològics** tant al vostre lloc de treball com en l'àmbit personal, ja que aquests dos entorns sovint poden estar connectats i tenir repercussió l'un sobre l'altre.

La Direcció de Serveis de Tecnologies i Sistemes Corporatius posa tots els **mitjans tècnics disponibles** (antivirus, tallafocs, antispam...) per protegir els usos poc segurs de les tecnologies de la informació i la comunicació (TIC). Però sabem que vosaltres, **els empleats, sou la peça clau per garantir la seguretat** a la Diputació. Perquè sou vosaltres qui gestioneu la **informació**, la modifiqueu, transmeteu, elimineu i processeu.

La **conscienciació i col·laboració de tots** és clau per avançar en la seguretat en l'ús de les eines informàtiques. Aquí us proporcionem els recursos necessaris i les recomanacions per vetllar per un **ús òptim i segur de tots els recursos TIC**.

Credencials d'accés

- En el món digital **les persones ens hem d'identificar per accedir amb seguretat als recursos** que s'hi ofereixen.
- La identificació més utilitzada és la combinació de **nom d'usuari i contrasenya**, aquesta combinació rep el nom de **credencials d'accés**.
- L'augment de recursos digitals (ordinador, correu electrònic, webs bancàries, webs de compra, blogs, aplicacions de mòbil...) fa que les persones cada cop tinguem més **credencials d'accés** diferents.
- És important tenir en compte que aquestes credencials són la **única barrera** per accedir a les nostres dades,

Protegim les nostres contrasenyes

- No utilitzis mai les mateixes credencials per a recursos diferents i no utilitzis la mateixa contrasenya en llocs diferents.
- Com més valuós sigui el recurs al qual accedeixis més cura cal tenir amb les credencials.
- La contrasenya ha de ser personal i intransferible, mai s'ha de compartir o cedir a terceres persones.
- No anotis enlloc la teva contrasenya, ni l'enviïs mai per correu electrònic.
- És molt recomanable canviar periòdicament les contrasenyes.
- És important utilitzar contrasenyes segures. Les contrasenyes s'emmagatzemen i viatgen per les xarxes de forma encriptada. Ara bé, si la contrasenya va a parar a mans inadequades, la desxifrat d'una contrasenya



poc segura pot ser cosa de segons.

- Hi ha dues normes a seguir per fer una contrasenya segura: Fer-la llarga. Com a mínim hauria de tenir 8 caràcters.
Combinar diferents tipus de caràcters: lletres (majúscules i minúscules), números i altres caràcters no alfanumèrics.

Com fer una contrasenya segura i recordar-la

- Cal descartar, per més llarg que sigui, paraules existents o combinacions únicament de números.
- La millor manera d'aconseguir recordar una contrasenya llarga que combini lletres (minúscules i majúscules), números i caràcters no alfanumèrics és si la podem associar a una frase. Per exemple, si utilitzem la frase **"Els empleats som clau per garantir la seguretat"** podem agafar les inicials i utilitzar **Eescpgls**. A partir d'aquí podem aplicar algun canvi per afegir seguretat:
 - Substituir alguna lletra per números. La l per un 1, la e per un 3 o la p per un 9. Quedaria: **33sc9g1s**
 - Posar els verbs en majúscules. Quedaria: **EeScpGls**
 - Afegir caràcters no alfanumèrics. Quedaria: **E"e"scpgls!**
- Pots utilitzar frases que ja incloguin números, majúscules i caràcters no alfanumèrics.
 - DBaMhh40q?** "De Barcelona a Mataró hi ha 40 quilòmetres?"
 - Vne1.970aM** "Vaig néixer el 1.970 a Manresa"
 - Van32dc/PC** "Visc al número 32 del c/ Pau Claris"
 - EPvne6ilMe18** "El Pau va néixer el 6 i la Marta el 18"
- Un cop tinguis una contrasenya forta la pots utilitzar per diferents recursos afegint una diferència.
 - e2Sc!pglS:Fcb** --> Per a Facebook
 - e2Sc!pglS:Ytb** --> Per a YouTube
- No es recomana fer servir els navegadors per emmagatzemar les claus d'accés a les diferents adreces internet.
- Existeixen eines conegudes com a gestors de contrasenyes que faciliten emmagatzemar i recordar la totalitat de les nostres contrasenyes . Es basen en crear i recordar una única contrasenya robusta, la del gestor de claus, aquest pot emmagatzemar o crear de noves claus robustes per tots els llocs web que emmagatzemem. Un exemple d'eina d'aquestes característiques és *Keepass*.

Segon factor d'autenticació

- Quan en l'autenticació involucrem una confirmació a través d'un canal diferent (el més habitual és una confirmació amb un sms al nostre número de mòbil) augmentem molt la seguretat. Això es coneix com segon factor d'autenticació (2FA) i progressivament la **Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC)** anirà adoptant aquets tipus de solució per la majoria dels serveis.



Canvi de contrasenya a la Ajuntament d'Argentona

- La majoria de recursos de la Ajuntament d'Argentona (correu, xarxa, menú d'aplicacions, wifi,...) utilitzen les mateixes credencials.
- Cal ser especialment curós en la protecció d'aquestes credencials, utilitzant una contrasenya segura i canviant-la periòdicament.
- Davant de la sospita de que el teu usuari o contrasenya han estat capturats per un tercer tenim l'obligació legal d'informar immediatament **al telèfon 667 182 627 o envia email a informatica@argentona.cat**

Correu brossa

- El correu brossa (*spam*, en anglès) són aquells missatges enviats **sense el consentiment del receptor** a adreces de correu obtingudes de forma fraudulenta. És a dir, missatges no desitjats.
- Per quins motius rebem missatges d'aquest tipus?
 - **Per fer-nos publicitat** - Fer un ús indegut de llistes de correus electrònics és una forma fàcil de fer arribar publicitat d'un producte a molta gent.
 - **Per obtenir dades personals** - Aquesta pràctica coneguda com a *phishing* (pesca en anglès) pretén obtenir dades del destinatari.
 - **Per transmetre algun tipus de programari maliciós** - El programari maliciós s'instal·larà al nostre ordinador si obrim un fitxer adjunt o accedim a una plana web a través d'un link que ens proposen.
- Hi ha dos tipus de remittents:
 - Algú ha creat una adreça de correu des d'on enviar correu brossa. Aquests correus són fàcils de detectar de forma automàtica pels sistemes anti-spam i normalment no arriben al destinatari.
 - Algú utilitza la bústia de correu d'una altra persona sense el seu consentiment per enviar correu brossa. Per fer-ho, o bé ha robat les seves credencials o bé ha instal·lat algun programari maliciós en el seu ordinador. **Són els més perillosos** perquè acostumen a saltar les barreres de detecció automàtica. Cal sospitar del contingut.
- No es pot considerar correu brossa el correu publicitari que rebem si hem cedit voluntàriament les nostres dades a una empresa o entitat. En aquests casos la llei obliga a facilitar la baixa d'aquests enviaments i normalment el mateix correu porta un accés per fer-ho.
- Davant del més mínim dubte, **no accedeixis a cap enllaç, no descarreguis cap fitxer adjunt i no contestis el correu.**

Phishing

- El *phishing* o suplantació d'identitat és una estafa que consisteix a suplantar la identitat d'una persona, empresa o institució de confiança per aconseguir **dades personals** com ara dades bancàries, adreça o les **credencials d'usuari** o per **transmetre algun tipus de programari maliciós**.



- La propagació del *phishing* normalment es realitza a través del **correu electrònic**, tot i que també es pot propagar per altres canals com les **xarxes socials (facebook, twitter, whatsapp,...)** o el **SMS**.
- Funciona de la següent manera: rebem un correu electrònic, SMS o missatge de xarxes socials amb aparença real i un enllaç a una web externa falsa controlada pels ciberdelinqüents. La web falsa suplanta la web o servei original esperant que "piquem" i **introduïm les nostres dades**, passant d'aquesta manera a ser "pescats". També poden enllaçar directament a la descàrrega d'un programari maliciós.
- Amb les dades obtingudes, els **ciberdelinqüents** poden suplantar la nostra identitat, realitzar estafes econòmiques directament o vendre aquestes dades a tercers.
- El *phishing* pot ser indiscriminat o dirigit.
 - El *phishing* indiscriminat fa servir l'*spam* per arribar al màxim possible de víctimes. Suplanten a bancs o serveis de missatgeria coneguts i el que busquen és obtenir dades o infectar al màxim nombre d'usuaris. La seva força és el volum.
 - El *phishing* dirigit o *spear phishing* està orientat a una organització o persona concreta. Els atacants utilitzen uns correus molt més preparats per generar confiança al destinatari. Les webs falses o el programari maliciós que distribueixen també estan personalitzats per generar confiança. La seva força està en la dificultat per identificar-ho.

Detectem i combatem el *phishing*

- Els missatges relacionats amb el *phishing* fan servir el que s'anomena l'**enginyeria social**, és a dir, **fent servir la persuasió i l'engany busquen guanyar la nostra confiança**.
- Fan servir excuses com **canvis urgents** en les condicions de serveis, premis, promocions o multes per forçar-nos a prendre **una decisió ràpidament**.
- Si el *phishing* és indiscriminat acostumen a ser generats de manera automàtica i sovint contenen **errors gramaticals, errors ortogràfics o paraules traduïdes en altres idiomes** que ens han de fer sospitar.
- Com més valor tingui el recurs al qual suposadament enllaça el *phishing*, més cura cal tenir. Compte sobretot amb els correus de bancs on demanen canvis de contrasenyes, confirmar un compte o confirmar un pagament bancari, **sempre són falsos**.
- Rebutja de forma sistemàtica qualsevol correu electrònic o comunicat per al que sigui necessari facilitar **dades confidencials**. Contrasta la informació per altres vies.

Correu brossa i phishing a l'ajuntament d'Argentona

- Gràcies a les eines d'anàlisi, **més d'un 90% del correu que arriba als correus @argentona.cat és identificat com a brossa i ja no es lliura a les bústies**. Però resulta impossible aturar-ho tot.
- A la Ajuntament d'Argentona **també patim atacs dirigits de *phishing* per**



robar les nostres credencials d'usuari i accedir als nostres recursos.

- Recorda que des de la Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC) no t'enviarem en cap cas un missatge per demanar les teves credencials.
- Quan a la DSTSC s'om conscients que algun missatge perillós ha estat distribuït a les bústies, es prenen mesures concretes per evitar els efectes.
- Davant de qualsevol sospita d'un missatge recorda que pots enviar el correu a l'adreça informatica@argentona.cat on es revisarà el contingut i es prendran les mesures tècniques adients per evitar la propagació. Aturar el phishing és cosa de tots (servei 24 hores).

Programari maliciós (*malware*)

- El **programari maliciós o *malware*** (de l'anglès, *malicious software*) és el programari que realitza funcions no desitjades o perjudicials en un sistema sense consentiment de l'usuari.
- L'objectiu del programari maliciós és: **robar informació** dels usuaris, inserir eines de **gestió remota** per controlar els ordinadors o **xifrar la informació** que contenen els dispositius.
- Des del punt de vista tècnic hi ha molts tipus de programari maliciós depenent de com es distribueix, de com actua o de quina finalitat té: **virus, cucs, troians, programari espia...**

Punts d'entrada típics del *malware*

- **Correu electrònic:** És una manera molt directa i ràpida d'arribar a una persona i fer que **obri un fitxer o accedeixi a una web**. Aquestes accions poden provocar que el programari maliciós es traspassi a l'equip utilitzat. El correu pot ser [correu brossa](#) i utilitzar tècniques d'engany ([phishing](#)) o provenir d'un destinatari infectat sense saber-ho.
- **Navegació web:** Els cibercriminals **infecten servidors web lícits** que no estan protegits per afegir el codi maliciós a les pàgines que publiquen. Si es navega per aquesta web i l'equip no està protegit, n'hi ha prou amb la navegació per a què el programari maliciós es traspassi al nostre equip.
- **Aplicacions descarregades d'internet:** Els cibercriminals ofereixen **aplicacions falses**, per a ordinador o per a mòbils, que infectaran els dispositius de les persones que les descarreguin. Generalment l'engany és oferir de forma gratuïta programari de pagament o aplicacions amb funcionalitats molt atractives.
- **Dispositius d'emmagatzematge extern (memòries USB, discs durs, targetes de memòria, espais al núvol personal, ...).** L'execució, la descàrrega o la simple connexió a espais externs d'emmagatzematge pot suposar l'entrada de programari maliciós a l'equip, per tant no es recomana el seu ús.

Segrest d'informació (*ransomware*)

- Aquest tipus de programari maliciós xifra **el màxim d'informació possible** de



l'equip utilitzat i dels que hi estiguin connectats, abans que la víctima en sigui conscient. Una vegada realitzada l'encriptació de les dades, es mostra una **nota de rescat** (*ransom*, en anglès) exigint pagament econòmic per recuperar la informació.

- Si l'usuari no disposa de còpies de seguretat perdrà totes les dades encriptades. Cal dirigir-se a les autoritats.
- Malgrat els esforços dels governs per perseguir-lo, actualment és un dels programaris maliciosos més difosos a internet.
- La seva entrada acostuma a ser a partir d'un correu enganyós ([*phishing*](#)) amb un enllaç a una web externa o directament amb un fitxer adjunt.

Com combatem el programari maliciós?

- La **Direcció de Serveis de Tecnologies i Sistemes Corporatius** (DSTSC) disposa de totes les mesures adients per reduir l'entrada i propagació de programari maliciós, però tancar algunes vies d'entrada està únicament a les mans de les accions que pugui fer una persona amb el seu equip.
- El teu equip de l'ajuntament ja utilitza un programari antivirus oficial i manté actualitzat tot el programari de l'equip. Fes el mateix amb el teu equip personal.
- No obris enllaços o fitxers adjunts de missatges de correu de persones desconegudes o que semblin sospitoses (publicitat desconeguda, notícies urgents, escrit en diversos idiomes, amb faltes d'ortografia,...)
- No descarreguis fitxers o aplicacions sospitoses. Elimina complements sospitosos del navegador.
- Sigues molt prudent amb l'ús de dispositius d'emmagatzematge extern. Assegura't que provenen d'algú que també utilitza mesures de protecció.
- Per últim, davant de la més mínima sospita, truca al **telèfon 667 182 627**.

Dispositius mòbils

- Els nostres dispositius mòbils (*smartphones*, *tablets* o portàtils) emmagatzemen molta informació personal privada i són la porta d'accés a molts serveis personals i, per tant, cal cuidar-los i protegir-los.
- Cal protegir amb més cura l'accés als dispositius mòbils perquè estan molt exposats a pèrdues o robatoris.
- Cal vigilar l'accés als dispositius mitjançant un *pin*, una contrasenya, un patró de desbloqueig o amb l'ús de dades biomètriques. Cal establir algun d'aquests mecanismes de desbloqueig del dispositiu mòbil superat un temps d'inactivitat.
- Procura no emmagatzemar informació sensible en el dispositiu mòbil. Si ho fas, xifra la informació.
- Realitza còpia de seguretat de tota aquella informació allotjada en el teu dispositiu i mantén actualitzat tant el sistema operatiu com les aplicacions instal·lades.
- No consultis informació sensible ni utilitzis les teves credencials en xarxes wifi que no et generin prou confiança.
- Existeix programari maliciós específic pels dispositius mòbils. L'ús que es fa



d'aquests dispositius facilita la propagació i la infecció.

Aplicacions (apps)

- Les aplicacions o apps mòbils que instal·lem als nostres dispositius aporten funcionalitats per facilitar gestions o activitats, ja siguin de caire personal o professional.
- Aquestes aplicacions són una porta d'entrada per al programari maliciós.
- Els cibercriminals ofereixen **aplicacions falses** que infectaran els dispositius de les persones que les descarreguin. Generalment l'engany és oferir de forma gratuïta programari de pagament o aplicacions amb funcionalitats molt atractives.

Vigila amb les aplicacions de moda que surten abans de la data anunciada pel desenvolupador.

Compte amb les versions gratuïtes d'aplicacions de pagament.

Desconfia de les ofertes massa bones.

- La prevenció és clau, sigues molt prudent al descarregar aplicacions per als teu dispositiu mòbil:

Cal optar sempre per la descàrrega a les **botigues d'aplicacions oficials**.

Si dubtes, comprova la seva popularitat pel número d'instal·lacions, qualificacions o comentaris de la resta d'usuaris.

Cal revisar i estar atents a quins **permisos i drets sol·licita una aplicació**. Si ens demana permisos que no semblen necessaris per a la seva funció, no s'hauria d'instal·lar.

Dispositius mòbils a l'ajuntament d'Argentona

- No modifiquis la configuració dels dispositius corporatius ni hi instal·lis aplicacions no autoritzades. Respecta les indicacions del de la normativa d'ús dels mitjans electrònics de l'Ajuntament d'Argentona.
- L'ús de la connexió de dades en itinerància (sortides a l'estranger) està limitat a la Diputació per raons de racionalització de la despesa.
- La **Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC)** és troba en procés de desplegament d'una eina de gestió de la seguretat en els dispositius mòbils i en mobilitat coneguda com MDM.
- Si detectes qualsevol activitat sospitosa o un funcionament anormal del teu equip, notifica-ho a l'equip d'atenció a l'usuari, **al telèfon 667 182 627 o envia email a informatica@argentona.cat**

Xarxes socials

- Les xarxes socials formen part del nostre dia a dia, ens permeten comunicar-nos amb altres persones i compartir informació. La gran quantitat de dades i usuaris que s'hi mouen ens obliga a anar molt amb compte per fer-les servir de forma segura.
- Cal tenir **cura amb la informació que es publica**. Sovint es comparteix informació personal (fotografies, opinions o gustos) de la qual, una vegada



publicada i encara que l'esborrem, en perdrem el control. Per tant, pensa-ho bé abans de publicar res.

Informació que cal evitar publicar:

- Lloc i data de naixement
 - On vius
 - Dades bancàries
 - Número de mòbil
 - Plans per a les vacances
-
- Cal ser **respectuosos** amb els comentaris que es fan i **no publicar missatges ofensius**.
 - No facilitis o publiquis dades, informació, fotografies o vídeos **d'altres persones sense que t'hagin donat el seu consentiment**.
 - Configura correctament les opcions de **privacitat del teu perfil** i dona només accés a les persones que tu vulguis, d'aquesta manera reduiràs el risc de que la teva informació sigui accessible a gent malintencionada.
 - **Desconfia de les sol·licituds d'amistat o contactes de persones que no coneixes**. Si les acceptes pots estar donant accés a la teva informació i a la dels teus contactes.
 - **Jocs en línia com la Balena blava** (joc que incita a realitzar una sèrie de tasques i que es relaciona amb el suïcidi d'adolescents a diferents països del món) **s'aprofiten de les xarxes socials i de l'accés a la informació dels contactes per fer xantatge** quan es vol abandonar el joc.
 - Tal com succeeix amb els ordinadors i els dispositius mòbils, existeixen aplicacions malicioses (*malware*) dins de les xarxes socials. Cal revisar i estar atent a quins **permisos i drets sol·licita una aplicació**.
 - **Desconfia dels enllaços**, perquè les xarxes socials s'han convertit en un mitjà molt important per a la distribució de **virus o d'estafes**.
 - **Vigila la teva identitat digital**. Amb tanta informació publicada, els cibercriminals poden intentar robar la teva identitat (s'apropien de les teves credencials d'accés i es fan passar per tu publicant informació o enviant missatges) o suplantar-la (creen un perfil nou amb les teves dades).
 - **El robatori de dades, la suplantació d'identitat i l'assetjament són els delictes més freqüents a les xarxes socials**. Si sospites que estàs patint un d'aquests delictes, **cal denunciar-ho a la mateixa xarxa social i als cossos de seguretat**.

Sextorsió o xantatge amb gravacions sexuals

- La **sextorsió** és una de les extorsions que ha crescut més darrerament a internet. Aprofita imatges o vídeos de caire sexual, **obtingudes amb consentiment o robades**, per demanar diners a canvi si no es vol que les imatges es reenviïn als contactes o es publiquin a les xarxes socials. Si l'assetjament el fa un adult a un menor és *grooming*.
- En molts casos l'estafa comença amb una **sol·licitud d'amistat a les xarxes socials** de persones atractives que després busquen mantenir converses privades a través de xats i finalment, un cop guanyada la confiança, intercanviar imatges de caire sexual (*sexting*).



- **Darrere d'aquests perfils falsos s'oculten màfies criminals** que poden estar operant des de servidors ubicats a qualsevol lloc del món.

Missatgeria instantània

- Aquestes aplicacions permeten l'enviament instantani de missatges de text o multimèdia a un o més usuaris. Amb l'arribada dels mòbils **el seu ús s'ha estès i popularitzat** i tothom les utilitza a diari: *Whatsapp, Telegram, LINE, Hangouts, Google Allo, Skype, Messenger (Facebook), SnapChat,...* La seva immediatesa i l'alt volum d'usuaris i missatges les converteix en un espai ideal per a enganys.
- **És habitual que aquest tipus d'aplicacions no demanin credencials d'accés quan les fem servir.** Cal tenir validació d'accés al dispositiu mòbil per evitar que algú pugui consultar els nostres missatges i sobretot fer-ne en nom nostre.
- Esborra regularment l'**històric de converses** per evitar el seu accés en cas de pèrdua.
- Existeix programari maliciós especialitzat en missatgeria instantània. Cal anar amb compte amb els enllaços externs o fitxers adjunts. Desconfia dels arxius multimèdia.
- **No facis difusió dels números de telèfon dels teus contactes sense consentiment previ.** Quan es creen els grups de difusió, depenent de l'aplicació, publiquem tots els números de telèfon dels participants.
- **Sospita de missatges de desconeguts o ocults.** El millor és no respondre fins poder verificar la identitat. Mai donis dades personals sense estar segurs de la identitat de la persona que ho rebrà.
- Cal ser especialment curós en el reenviament dels missatges, **podríem estar cometent delictes per fer difusió de contingut il·legal.** Si reps contingut d'aquest tipus, notifica als cossos de seguretat i esborra'l, fer-ne difusió és delictes!
- **Actualitza sempre les aplicacions a la última versió,** a banda de noves funcionalitats, aquestes actualitzacions corregeixen els forats de seguretat.

Notícies falses i enganys (*hoax*)

- Les aplicacions de missatgeria instantània moltes vegades es fan servir **per transmetre i fer difusió de notícies falses o enganys**, també conegut com a *hoax*.
- L'**objectiu d'aquests missatges és molt divers: crear alarma social**, desprestigiar alguna marca o persona, donar consells enganyosos, actuar sobre l'opinió pública, transmetre codi maliciós,...
- No et creguis tots els missatges que reps encara que vinguin d'un conegut. **Contrasta la informació per altres vies.**
- Aquests tipus de missatges solen demanar que els facis arribar a més persones. Trenca la cadena, no formis part d'aquesta difusió. No reenviis aquest tipus de missatge als teus contactes.

Missatgeria instantània a la Ajuntament d'Argenton



- L'ús de la missatgeria instantània ha d'estar directament relacionat amb el desenvolupament de les tasques pròpies del lloc de treball. Respecta les indicacions de la Normativa d'ús dels mitjans electrònics de l'Ajuntament d'Argentonà".
- Sigues molt curós amb l'ús que fas de la missatgeria instantània, ja que no es pot controlar per on viatja o en quins servidors s'emmagatzema la informació. Si l'aplicació ho permet, fes servir xats encriptats d'extrem a extrem.
- La **Direcció de Serveis de Tecnologies i Sistemes Corporatius (DSTSC)** actualment recomana el correu electrònic corporatiu per l'enviament de dades corporatives i que aquestes preferentment han de ser adjuntades xifrades.

Recordeu que en missatgeria instantània la creació de grups de treball puntuals també està subjecte a l'obtenció fefaent del consentiment dels participants per part de l'administrador del grup.

Navegació segura

Navegar per internet forma part del nostre dia a dia. Ho fem des de diferents dispositius en diversos moments del dia. Ho fem com a lleure, per cercar informació o per treballar.

Quan es fa una transacció econòmica o s'introdueixen credencials per accedir a un espai amb dades personals és un dels moments on cal tenir més cura. Et proposem que prenguis algunes precaucions.

Com podem saber si un web és segur?

El sistema més utilitzat pels ciberdelinqüents és fer servir **noms de webs** molt semblants als originals on anem redirigits des d'algun correu maliciós o per error a l'escriure el nom. Aquests webs falsos pretenen obtenir les nostres dades personals o **distribuir programari maliciós**.

- Si la URL del web comença per **HTTPS://** indica que les dades viatgen xifrades i no resulta fàcil interceptar-les i obtenir-les. Els webs bancaris, de serveis de compres o de pagaments han de començar sempre per HTTPS://, mai per HTTP://
- Si apareix un cademat al costat de la URL indica que el web fa servir certificat que garanteix la seva identitat. Podem clicar sobre el cademat per obtenir la informació del certificat web, verificant d'aquesta manera que és autèntic i que el web és legítim, és a dir, és qui diu ser. Aquests certificats els emeten les Autoritats de Certificació que funcionen com a intermediaris i ens verifiquen la autenticitat del certificat.
- Els navegadors afegeixen **colors a la barra** per indicar si s'ha pogut verificar el certificat, en color verd si ha pogut i en color vermell si no ha pogut. Pot succeir que el certificat utilitzat sigui perfectament vàlid i segur però surti de color vermell perquè no el reconeix per defecte. En aquest cas el navegador ens demanarà si volem o no confiar i caldrà verificar la autenticitat del certificat.



Altres recomanacions

- Evita fer servir l'opció de recordar contrasenyes al navegador i esborra i configura per tal de no guardar dades com l'historial de navegació o les dades introduïdes als camps dels formularis.
- Tanca les sessions correctament en comptes de tancar directament la finestra.
- En ordinadors públics fes servir l'opció de **navegació privada (incògnit)** que incorporen tots els navegadors.
- Cal mantenir els navegadors actualitzats i ser conscients de quins complements, extensions o *plugins* tenim instal·lats.

Galetes (*cookies*)

- Les galetes (*cookies* en anglès) són petits magatzems de dades que els webs creen i gestionen en l'ordinador on es navega.
- Si el web únicament utilitza galetes per facilitar-nos la navegació no ens demanarà cap autorització.
- Alguns webs utilitzen les galetes per emmagatzemar dades sobre els nostres gustos, preferències o forma de navegar que després s'utilitzaran per oferir-nos publicitat dirigida o personalitzar navegacions. Si la informació de la galeta va a parar a un altre proveïdor (**galetes de tercers**) el web sol·licita el nostre consentiment.
- Resulta molt complicat evitar l'ús de galetes de tercers perquè si no responem i continuem navegant ho interpreten com un consentiment. A través de les configuracions de privadesa dels nostres navegadors podem activar el bloqueig de les galetes de tercers.

Certificats digitals a la Ajuntament d'Argentona

- Els webs de la ajuntament d'Argentona fan servir certificats emesos per les entitats CatCert (Consordi AOC) i geo Trust.
- L'entitat CatCert no està incorporada per defecte en els navegadors més utilitzats del mercat. Els ordinadors corporatius porten el certificat CatCert instal·lat per defecte.
- Si accedeixes a una web de la Ajuntament d'Argentona des d'un dispositiu personal sense el certificat CatCert, el navegador pot posar la URL de color vermell. Si vols instal·lar el certificat de l'entitat pots fer-ho seguint les instruccions del seu web: <https://www.aoc.cat>

El lloc de treball

Les mesures de ciberseguretat han de començar abans d'utilitzar l'ordinador o el mòbil. No només perquè algunes actuacions en el nostre lloc de treball poden obrir les portes a tota la nostra informació digital sinó també perquè cal tenir la mateixa cura en la seguretat dels documents i dades que encara mantenim en paper.

Cal seguir els següents consells en el nostre lloc de treball:



- Eviteu les còpies impreses, però si us calen recordeu:
 - Quan imprimeixis un document cal mantenir el seu nivell de seguretat. Si en format digital no era públic tampoc ho pot ser en format paper.
 - Imprimir documents amb dades personals afectades per la LOPD (Llei de protecció de dades) pot constituir un delict.
 - Revisa quins papers queden accessibles a la taula quan deixis el lloc de treball encara que sigui temporalment.
 - Cal destruir de forma segura els documents no públics.
- Ordinador personal, telèfon intel·ligent o tauletes
 - Cal bloquejar l'accés als dispositius si els deixem fora de la vista i apagar-los si no els hem d'utilitzar durant un temps.
 - No donis les teves credencials a ningú per cap mitjà ni amb cap pretext.
 - No mantinguis cap còpia escrita de les teves credencials.
- Dispositius portàtils d'emmagatzematge
 - No connectis un dispositiu sense la certesa de saber a qui pertany.
 - Si hi mantens dades, guarda'ls en llocs segurs.
- Telèfon
 - Cal verificar la identitat del teu interlocutor si en la conversa surten dades personals o informacions privades.
 - No donis les teves credencials per telèfon.

Aquestes pautes valen tant per llocs de treball corporatius o en mobilitat.

Estacions de treball a la Ajuntament d'Argentona

- Utilitza les unitats de xarxa per compartir i emmagatzemar informació i evita suports locals o portàtils.
- Respecta les indicacions del Manual d'ús dels sistemes d'informació i comunicació DiBA
- Si detectes qualsevol activitat sospitosa o un funcionament anòmal del teu equip, notifica-ho a l'equip d'atenció a l'usuari, **al telèfon 667 182 627 o envia email a informatica@argentona.cat**

Estacions de treball en remot a la Ajuntament d'Argentona

El personal de la Ajuntament d'Argentona autoritzat a prestar serveis en modalitat en remot haurà de seguir les normes de ciberseguretat que es descriuen en aquest document, i seguir els requeriments tècnics i les condicions d'utilització dels mitjans tecnològics.

- En alguns casos la Direcció de Serveis de Tecnologies i Sistemes Corporatius proveeix d'equipament informàtic amb el programari informàtic homologat carregat i configurat de forma adient. Aquell personal que disposi d'equipament corporatiu, en farà ús de forma preferent d'aquests equips informàtics sense dur a terme canvis substancials en la configuració dels



mateixos.

- En cas que s'utilitzin mitjans propis, es podrà requerir modificar la seva configuració per garantir la ciberseguretat del dispositiu. Caldrà sempre:
 - El mitjà emprat haurà de tenir instal·lat i permanentment actualitzat un programari d'antivirus i un sistema operatiu degudament actualitzat
 - S'haurà de configurar l'accés al mitjà amb un mecanisme d'autenticació robust basat en un identificador i contrasenya forta.
 - Actualment el servei wifi corporatiu empra un segon factor d'autenticació però si l'usuari no disposa d'una connexió corporativa a l'abast, podrà fer ús d'una xarxa wifi de confiança, amb protocol wpa2 o superior i que requereixi de contrasenya forta per a connectar-se.

Els serveis tecnològics a disposició del personal seran accessibles des de navegador web o en el seu defecte seran proveïts a través d'una connexió VPN per oferir confidencialitat sobre les dades, conservant les evidències digitals necessàries pel compliment legal.

- No es recomana l'ús de dispositius locals d'emmagatzematge. Per assegurar la disponibilitat de les dades que es treballin des d'aquestes estacions de treball, caldrà fer ús dels espais i eines corporatives per a les funcions d'emmagatzematge de documents. La Direcció de Serveis de Tecnologies i Sistemes Corporatius disposa de procediments de còpia de seguretat i mecanismes anti-malware per mitigar els efectes que es poguessin produir a nivell de disponibilitat i d'integritat de la Informació.
- No es permès deixar informació corporativa en espais al núvol personals.
- Cal tenir cura de no deixar còpies de la informació que amb la que es treballa en l'estació de treball en remot.

