

Codi de verificació	 2J2H6B4B6G2S6E4H0HCA
Procediment: N488 Contractació de serveis	
Expedient: 6365/2025	Document: 63893/2025

PLEC DE PRESCRIPCIONS TÈCNIQUES DE CONTRACTACIÓ DE SERVEIS

Primer. Objecte del contracte

Servei d'assessorament i adaptació al Esquema Nacional de Seguretat ara en davant ASC ENS per l'obtenció de la certificació ENS i suport tècnic avançat en Ciberseguretat. Concretament:

- Anàlisi previ ENS
- Acompanyament de tot el procediment que deriva la certificació de l'ENS segons el RD 311/2022
- Assessoria jurídica ENS
- Suport tècnic presencial en tecnologies de ciberseguretat

Segon. Característiques tècniques dels serveis o prestacions

En la determinació de les prescripcions, s'han tingut en compte els arts. 124 a 128 de la LCSP sobre definicions i regles per a l'establiment de prescripcions tècniques.

El present plec té com objectiu la contractació d'un servei per l'adequació a l'ENS i suport a les principals tecnologies de seguretat gestionades per l'Ajuntament de Sant Cugat del Vallès de ara en davant ASC.

En general l'abast del projecte comprèn totes les activitats de consultoria i suport tècnic, així com la realització dels treballs d'adequació necessaris perquè els sistemes d'informació, en sentit ampli, de l'Ajuntament de Sant Cugat del Vallès compleixin amb els requisits exigits en l'ENS RS 311/2022 i, en el cas de tractament de dades personals, amb els requisits de l'RGPD i la Llei Orgànica 3/2018 de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

Al inici de la licitació es constituirà una oficina de seguiment formada amb Responsable de Seguretat designat per ASC on es realitzarà el seguiment del objecte del contracte i la presentació de l'equip de treball proporcionat pel licitador.

Suport tècnic presencial en tecnologies de ciberseguretat

Es sol·licita un servei de suport tècnic en tecnologies de Ciberseguretat, aquest servei presencial a de donar suport a les principals tecnologies següents:

- Microsoft Exchange Online
- Microsoft Defender
- Microsoft Intune
- Microsoft Entra ID (anteriorment Azure AD)

Aquest suport en ciberseguretat ha de tenir un alt coneixement en l'ecosistema Microsoft 365, enfocat específicament en la gestió de serveis crítics de comunicació, protecció, gestió de

dispositius. Aquest servei combina competències tècniques com avançades en aquestes plataformes fonamentals, proporcionant una visió integrada i holística de la seguretat i administració dins de l'ecosistema Microsoft Cloud.

Aquest suport realitzar les següents accions:

1. Identitat

La gestió de la identitat dins de l'organització es basa en una arquitectura d'hibridació que consisteix en dos active directories onpremise i el servei de Microsoft EntraID (anteriorment AzureAD).

La gestió a nivell de seguretat seria la següent:

- Implementació de cicles de revisió d'accés i certificacions
- Desplegament de mètodes d'autenticació multifactor adaptativa
- Implementació d'autenticació sense contrasenya (FIDO2, Windows Hello)
- Configuració de polítiques de protecció d'identitat i detecció de riscos
- Implementació de polítiques d'accés condicional basades en riscos
- Configuració de restriccions d'accés segons ubicació, dispositiu i aplicació
- Integració amb Intune per a avaluació de postura de seguretat de dispositius
- Implantació i gestió Identity Protection
- Configuració Privileged Identity Management (PIM)
- Gestió de la securització de la identitat

2. Correu

Actualment l'organització disposa d'una arquitectura d'hibridació distribuïda en servidors de correu onpremise i el servei contractat de Exchange online. Per aquest motiu es necessari la realització de les següents tasques mínimes:

- Implementació de polítiques anti-phishing i anti-spoofing
- Configuració de regles de transport per a prevenció de fuites d'informació
- Establiment de signatures digitals, xifrat de missatges i comunicacions segures
- Gestió de drets i permisos granulars mitjançant RBAC (Control d'Accés Basat en Rols)
- Configuració de retenció legal, auditoria i compliment normatiu
- Implementació de polítiques d'arxivat i gestió del cicle de vida de la informació
- Disseny d'estratègies d'alta disponibilitat i recuperació davant desastres
- Monitorització proactiva mitjançant eines avançades de diagnòstic
- Resolució de problemes complexos de lliurament, rendiment i connectivitat

3. Microsoft Defender

L'Ajuntament de Sant Cugat utilitza com a plataforma de seguretat integral Microsoft Defender proporcionant una protecció avançada contra amenaces en múltiples capes de l'entorn digital, aquesta solució proporciona detecció, prevenció, investigació i resposta automatitzada davant amenaces sofisticades a través de diferents vectors d'atac, incloent endpoints, identitats, aplicacions, correu electrònic, dades i entorns cloud.

Per aquesta raó es important que el servei realitzi les següents tasques:

- Configuració i gestió de Safe Attachments, Safe Links
- Implementació de polítiques anti-malware i anti-phishing avançades

- Anàlisi forense d'atacs i remediació post-compromís
- Desplegament i administració d'agents
- Configuració de detecció avançada i resposta automatitzada a incidents (EDR)
- Anàlisi de comportament i detecció d'amenaques basada en aprenentatge automàtic
- Monitoratge d'activitats sospitoses vinculades a identitats
- Detecció d'atacs de reconeixement, moviment lateral i escalat de privilegis
- Integració amb SIEM i sistemes d'orquestració de seguretat (SOAR)
- Implementació de polítiques de Cloud Access Security Broker (CASB)
- Control i visibilitat d'aplicacions SaaS no administrades (Shadow IT)
- Protecció d'informació sensible en aplicacions cloud autoritzades i no autoritzades

4. Intune

L'Ajuntament de Sant Cugat disposa de Microsoft Intune com a solució de gestió de dispositius i aplicacions mòbils per a organitzacions. Aquest servei al núvol de Microsoft permet una administració centralitzada de tots els dispositius, implementa polítiques de seguretat consistents, facilita les estratègies BYOD separant dades personals i corporatives, simplifica el desplegament d'aplicacions, assegura el compliment normatiu, s'integra perfectament amb altres productes Microsoft, implementa polítiques d'accés condicional, proporciona eines efectives per respondre a incidents de seguretat.

Per aquesta raó es important que el servei realitzi les següents tasques:

- Implementació d'estratègies d'inscripció automatitzada i massiva
- Configuració de polítiques de compliment i accés condicional específiques per dispositiu
- Gestió del cicle de vida complet de dispositius corporatius i BYOD
- Gestió d'Aplicacions Mòbils (MAM)
- Desplegament i configuració d'aplicacions
- Creació i desplegament de perfils de configuració per a múltiples plataformes (Windows, iOS, Android, macOS)
- Implementació de certificats, VPN i configuracions Wi-Fi
- Gestió d'actualitzacions i pegats de seguretat
- Implementació de polítiques de protecció amb Microsoft Defender
- Gestió de Firewall, BitLocker i altres tecnologies de seguretat natives
- Detecció i resposta a dispositius compromesos o no conformes

Aquest servei també donarà suport altres tecnologies en cas que fos necessari a nivell de seguretat.

A banda de les tecnologies definides i el seu abast l'Ajuntament de Sant Cugat disposa d'un servei de SOC i una seguretat perimetral basa en tecnologia Checkpoint aquest dos serveis no son objecte de gestió per part del servei de suport però si que podria donar assessoria o recomanacions si fos necessari.

Aquest servei de suport tècnic en tecnologies de Ciberseguretat serà l'encarregat de gestionar les incidències a nivell de seguretat derivades de les accions detallades amb anterioritat i objecte de la licitació.

El servei presencial es donarà en jornades de quatre hores i quatre dies a la setmana. Aquest horari pot variar previ acord de les dues parts.

Compliment normatiu Esquema Nacional Seguretat (ENS)

Al inici del contracte es realitzarà un anàlisi previ per poder valorar si es pot certificar el Sistema d'Informació (SI), en cas de que no fos possible es valorarà quins son els serveis que son susceptibles de certificar.

Aquesta línia base establirà el nivell de maduresa inicial, el qual serà un indicador per a avaluar els serveis a certificar.

Tota la documentació generada objecte de aquesta licitació haurà de ser redactada en català, aquella documentació que es requereixi per la certificació també es tindrà que escriure en castellà.

Així doncs, es definirà una fase inicial de posta en marxa del servei en la que es desenvoluparan les següents tasques:

- Presentació de l'equip fix de treball i de les capacitats de l'equip.
- Definició d'interlocutors per ambdues parts
- Anàlisi de l'entorn
- Anàlisi de documentació existent
- Valoració del actius i nivells de seguretat
- Enteniment de les funcions del Servei de Tecnologia i Desenvolupament Digital
- Avaluació inicial dels serveis
- Elaboració d'un informe de propostes de serveis a certificar.

En l'avaluació inicial es farà una anàlisi diferencial del serveis de l'Ajuntament per a fer una primera revisió del nivell de maduresa per poder valorar els serveis en el conjunt de controls de l'ENS

Aquesta anàlisi inicial té un doble objectiu:

- Establir el "punt de partida" que permetrà, gràcies a avaluacions posteriors, llistat els serveis que han de ser objecte de control al ENS.
- Fer una proposta d'actuacions i serveis que podria assessorar l'equip de treball per obtenir la certificació de l'ENS.

La proposta resultant serà presentada per la contractista com a document de "Recomanacions". No obstant, serà decisió de l'ASC la selecció dels serveis a executar.

Si prèviament acordat amb la contractista s'estableix que no és viable la certificació del sistema d'Informació (SI) per una falta de maduresa prèvia, s'establirà un mínim de dos serveis que seran objecte a certificar.

Per desenvolupar les tasques s'atendrà en tot moment a les guies publicades pel Centre Criptològic Nacional al respecte i a la GUIA ESTRATÈGICA EN SEGURETAT PER A ENTITATS LOCALS, publicada per la Federació Espanyola de Municipis i Províncies en col·laboració amb el Centre Criptològic Nacional ara en davant CCN. Es prestarà especial atenció al definit en aquesta última guia pel que fa a:

- "Fase I - Elaboració de el Pla d'Adequació":
 - Planificació.
 - Política de Seguretat.
 - Determinació de la Categoria de el Sistema.



- Anàlisi de Riscos.
- Declaració d'aplicabilitat (SOA).
- Informe d'insuficiències (Gap Analysis)
- Pla de Millora.
- "Fase II - Implementació de el Pla d'Adequació":
 - Revisió de el Pla d'Adequació.
 - Mesures de Seguretat - Marc Organitzatiu.
 - Mesures de Seguretat - Marc Operacional.
 - Mesures de Protecció.
- "Fase III – Conformitat amb el ENS":
 - Preparació conformitat
 - Assolir conformitat
 - Sistemes de categoria bàsica
 - Sistemes de categoria mitja o alta
- "Fase IV – Sistema de millora continua":
 - Tasques de seguiment.
 - Tasques de millora.
 - Cicle Deming.
- "Fase V - Formació":
 - Elaboració d'un pla de formació
 - Elaboració d'un pla de conscienciació.
 - Mesures de Seguretat - Marc Organitzatiu.
 - Mesures de Seguretat - Marc Operacional.
 - Mesures de Protecció.

Es fomentarà la execució en paral·lel de les fases que així ho permetin.

L'ajuntament de Sant Cugat actualment disposa de documentació de responsabilitat pro-activa en mesures del ENS; la contractista haurà de revisar el grau de compliment d'acord amb la situació normativa actual proposant quantes accions cregui necessàries per a resoldre els possibles incompliments; a més es pretén obtenir la certificació de conformitat de l'ENS emesa pel CCN en algun dels seus serveis

- S'actualitzarà i completarà la Declaració d'aplicabilitat, mitjançant l'elaboració de un quadre de comandament amb tots els controls que proposa l'ENS indicant el seu nivell de aplicabilitat i les activitats realitzades per cada un.
Es realitzarà el lliurable: **Document de declaració d'aplicabilitat.**
- Es realitzarà una anàlisi de riscos, que consideri els actius necessaris per a prestar els serveis de l'abast. Es realitzarà utilitzant l'eina PILAR. A partir dels resultats de l'anàlisi es decidiran els riscos a tractar i s'establirà un pla de tractament que implicarà la implantació o millora de controls de seguretat. El lliurable associat a aquesta activitat és l'Inventari d'actius i anàlisi de riscos en l'eina PILAR i el pla de tractament de riscos.
- Configuració i manteniment de l'eina INÉS de l'CCN.
- Pla d'accessió. Aquest pla comprendrà el de tractament de riscos i tots aquells requisits obligatoris de l'ENS que s'ha detectat que no compleix a el 100%.

Es realitzarà la definició i desenvolupament dels procediments de controls de seguretat relacionats amb tots els àmbits considerats en l'ENS:

- Control d'accés lògic a les aplicacions i informació de ASC
- Explotació de sistemes d'informació
- Gestió de serveis externs
- Gestió de la monitorització dels sistemes d'informació
- Protecció d'instal·lacions i infraestructures físiques
- Gestió de personal pel que fa a rols, funcions, formació i capacitats
- Protecció d'equips
- Protecció de les comunicacions
- Gestió de suports
- Gestió d'aplicacions
- Protecció de la informació
- Protecció de serveis específics com email, web, etc.

Les accions planificades per tractar els riscos que s'hagin considerat com no acceptables per part de ASC podran ser diferents i addicionals a les exigides per requeriment de l'ENS. Lliurable: **Pla d'acció global**.

Per a això s'hauran de realitzar les activitats que s'enumeren a continuació:

Revisió de la política de seguretat

Haurà d'atendre principalment als següents aspectes:

- L'organització del procés de seguretat.
- Els procediments per l'anàlisi i gestió dels riscos.
- Els processos, normes i procediments d'autorització d'accés als sistemes d'informació.
- Les normes i procediments per a la protecció d'instal·lacions.
- Els procediments per a l'actualització dels sistemes d'informació.
- Els procediments per a la conservació i emmagatzematge de la informació.
- Les normes i procediments per al registre de l'activitat i dels incidents de seguretat.

Revisió de la normativa de seguretat

La contractista haurà d'efectuar un diagnòstic del grau de compliment de la legislació vigent de la normativa de seguretat de sistemes d'informació interna.

Definició i posada en marxa de les mesures del marc organitzatiu

- Desenvolupant els procediments de seguretat.
- Definint el procés d'autorització.

Definició i posada en marxa de mesures operacionals

Les mesures per protegir l'operació de sistema com a conjunt integral de components per a un fi, constituït per les següents mesures:

- Planificació
- Control d'accés
- Explotació
- Serveis externs
- Continuitat del servei

- Monitorització del sistema

Definició i posada en marxa de mesures de protecció

Centrat en actius concrets, segons la seva naturalesa, amb el nivell requerit en cada dimensió de seguretat, les mesures següents:

- Instal·lacions i infraestructures
- Gestió de personal
- Protecció dels equips
- Protecció de les comunicacions
- Protecció de suports de la informació
- Protecció aplicacions informàtiques
- Protecció de la informació
- Protecció dels serveis

Revisió de la política de seguretat

Haurà d'atendre principalment als següents aspectes:

- L'organització del procés de seguretat.
- Els procediments per l'anàlisi i gestió dels riscos.
- Els processos, normes i procediments d'autorització d'accés als sistemes d'informació.
- Les normes i procediments per a la protecció d'instal·lacions.
- Els procediments per a l'actualització dels sistemes d'informació.
- Els procediments per a la conservació i emmagatzematge de la informació.
- Les normes i procediments per al registre de l'activitat i dels incidents de seguretat.

Revisió de la normativa de seguretat

La contractista haurà d'efectuar un diagnòstic del grau de compliment de la legislació vigent de la normativa de seguretat de sistemes d'informació interna.

Definició i posada en marxa de les mesures del marc organitzatiu

- Desenvolupant els procediments de seguretat.
- Definint el procés d'autorització.

Definició i posada en marxa de mesures operacionals

Les mesures per protegir l'operació de sistema com a conjunt integral de components per a un fi, constituït per les següents mesures:

- Planificació
- Control d'accés
- Explotació
- Serveis externs
- Continuitat del servei
- Monitorització del sistema

Definició i posada en marxa de mesures de protecció

Centrat en actius concrets, segons la seva naturalesa, amb el nivell requerit en cada dimensió de seguretat, les mesures següents:

- Instal·lacions i infraestructures

- Gestió de personal
- Protecció dels equips
- Protecció de les comunicacions
- Protecció de suports de la informació
- Protecció aplicacions informàtiques
- Protecció de la informació
- Protecció dels serveis

En el cas que fos necessari implantar alguna eina de control o gestió s'ha de procurar emprar les eines proporcionades pel CCN.

Peticions sota demanda

L'Ajuntament de Sant Cugat estima una bossa de 200h per cobrir necessitats de seguretat imprevistes que puguin sorgir inclouen el desplaçament a les dependències en cas estrictament necessari i sol·licitat pel responsable de l'Ajuntament de Sant Cugat. Aquestes jornades s'utilitzaran segons les necessitats específiques de seguretat de l'Ajuntament. Si durant l'any natural no s'utilitzen totes les jornades disponibles, aquestes no es perdran, sinó que s'acumularan i podran ser utilitzades durant el següent període del contracte, incloent tant el període inicial com possibles pròrroques futures.

Acords de compliment

L'empresa haurà de proporcionar els acords de nivell de servei (ANS) per l'atenció i resolució d'incidents i peticions en els diferents nivells de severitat:

- CRITIC: Incidències greus per tall del servei.
- ALT: Incidències en les que hi ha degradació del servei.
- MIG-BAIX: Incidències amb algun impacte al servei.

Aquests terminis mai podran superar els temps establerts en la següent taula.

	Resposta	Resolució	Consultes
CRITIC	30 min	4h	2d
ALT	30 min	8h	3d
MIG-BAIX	30 min	48h	3d

En el cas de les peticions sota demanda mai es podran superar els següents temps:

	Temps de resposta		
	Criticitat Alta	Criticitat Mitja	Criticitat baix
PETICIÓ SOTA DEMANDA	24h	48h	72h

Requisits de l'equip de treball

L'equip haurà de reunir, entre els seus membres, les següents titulacions i certificacions:

- Enginyeria de Telecomunicacions o Enginyeria Informàtica
- Llicenciatura en dret
- Certified Information Systems Auditor (CISA)
- Microsoft 365 Certified: Endpoint Administrator Associate
- Microsoft 365 Certified: Security Administrator Associate
- Microsoft Certified: Azure Security Engineer Associate

Hi haurà d'haver una figura que realitzarà reunions periòdiques 1 cop a la setmana amb el responsable municipal del contracte i que tindrà com a principals funcions les següents:

- Garantir la qualitat del servei prestat i la idoneïtat de l'equip de treball proposat
- Gestionar l'àmbit administratiu del servei
- Gestionar l'abast del servei
- Seguiment de les tasques desenvolupades (present, passat, futur)

En el cas d'haver de substituir algun dels membres, s'haurà de notificar al responsable del contracte amb un mínim de 15 dies d'antelació i haurà de complir el requeriments del plec en experiència i coneixements requerits.

Tercer. Acta d'inici de prestació del servei

Una vegada formalitzat el contracte en document administratiu, s'haurà d'estendre l'acta d'inici de prestació del servei, que serà signada pel legal representant de l'empresa i el responsable del contracte. Aquest haurà de remetre un dels exemplars a la Secció de Contractació i Compres per a la seva incorporació a l'expedient.

Quart. Entrega dels treballs i/o realització dels serveis durant la prestació

El contractista haurà d'entregar els treballs realitzats dins del termini estipulat en el contracte; el responsable del contracte efectuarà l'examen de la documentació presentada i, si estimés complides les prescripcions tècniques i restants condicions contractuals, proposarà que es porti a terme la seva recepció.

En el cas que estimés incomplides les prescripcions tècniques del contracte, donarà per escrit al contractista les instruccions precises i detallades amb la finalitat d'esmenar les faltes o defectes observats, fent constar en l'esmentat escrit el termini per efectuar les esmenes i les observacions que estimi oportunes.

En cas de reclamació per part del contractista respecte de les observacions formulades, el responsable del contracte l'eleva, amb el seu informe, a l'òrgan de contractació per a la seva resolució.

Si el contractista no reclamés per escrit respecte a les observacions del responsable del contracte, s'entendrà la seva conformitat quedant obligat a corregir o esmenar els defectes detectats.

En serveis de prestació continuada, el plec de clàusules administratives podrà establir altres formes de constatar la correcta execució dels serveis prestats..

Cinquè. Recepció dels treballs i serveis a la finalització

Quan la prestació s'ajusti a les condicions del contracte procedirà la seva recepció i s'estendrà l'acta corresponent que serà signada pel responsable del contracte i el representant legal del contractista.

Si la prestació no fos ajustada a les condicions necessàries per procedir a la seva recepció es donaran per escrit les instruccions oportunes al contractista a fi que esmeni els defectes observats i compleixi les seves obligacions en el termini que per això es fixi; no procedirà la recepció fins que les instruccions hagin estat complimentades, estenent-se llavors l'acta corresponent.

En serveis de prestació continuada, el plec de clàusules administratives podrà preveure altres formes de recepció.

L'acta de recepció serà estesa per triplicat exemplar, un dels quals serà incorporat a l'expedient de contractació.

Sisè. Obligacions en matèria de prevenció de riscos laborals

1. El contractista està obligat al compliment de la Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals i restant legislació general i sectorial aplicable en aquesta matèria respecte dels treballadors adscrits a la contracta.
2. En el supòsit de concurrència de treballadors del contractista amb altres treballadors en un centre de treball municipal, l'Ajuntament vetllarà pel compliment de la normativa de prevenció de riscos laborals per part de les empreses que presten serveis corresponents a la pròpia activitat en els termes establerts pel RD 171/2004, de 30 de gener, pel qual es desenvolupa l'art. 24 de Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals, en matèria de coordinació d'activitats empresarials.

L'Ajuntament facilitarà a l'empresa que resulti adjudicatària del contracte els documents i informació a que es refereix l'art. 7 del Reial Decret 171/2004, de 30 de gener, relatiu a: Avaluació de riscos del centre de treball, mesures de prevenció, pla d'emergència i qualsevol altre que correspongui.

El contractista resta obligat a presentar, abans de formalitzar-se l'acta d'inici de prestació del servei, els documents que seguidament s'indiquen en compliment del que disposa l'art. 10.2 del Reial Decret 171/2004:

- a) Avaluació de riscos i planificació de l'activitat preventiva.
 - b) Compliment de les obligacions en matèria d'informació i formació respecte dels treballadors que vagin a prestar serveis al centre de treball.
 - c) Qualsevol altre que l'Ajuntament consideri convenient o necessari.
3. El contractista tindrà accés a la documentació municipal a través de la plataforma informàtica autoritzada per l'Ajuntament en la forma que li serà indicada pel responsable del contracte i haurà de presentar el documents a través de la mateixa plataforma.

Setè. Control de qualitat

Quan la prestació s'ajusti a les condicions del contracte procedirà la seva recepció i s'estendrà l'acta corresponent que serà signada pel responsable del contracte i el representant legal del contractista.

Si la prestació no fos ajustada a les condicions necessàries per procedir a la seva recepció es donaran per escrit les instruccions oportunes al contractista a fi que esmeni els defectes observats i compleixi les seves obligacions en el termini que per això es fixi; no procedirà la recepció fins que les instruccions hagin estat complimentades, estenent-se llavors l'acta corresponent.

En serveis de prestació continuada, el plec de clàusules administratives podrà preveure altres formes de recepció.

L'acta de recepció serà estesa per triplicat exemplar, un dels quals serà incorporat a l'expedient de contractació.

Vuitè. Normativa sectorial aplicable

El contractista està obligat al compliment de la Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals i restant legislació general i sectorial aplicable en aquesta matèria respecte dels treballadors adscrits a la contracta.

En el supòsit de concurrència de treballadors del contractista amb altres treballadors en un centre de treball municipal, l'Ajuntament vetllarà pel compliment de la normativa de prevenció de riscos laborals per part de les empreses que presten serveis corresponents a la pròpia activitat en els termes establerts pel RD 171/2004, de 30 de gener, pel qual es desenvolupa l'art. 24 de Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals, en matèria de coordinació d'activitats empresarials.

L'Ajuntament facilitarà a l'empresa que resulti adjudicatària del contracte els documents i informació a que es refereix l'art. 7 del Reial Decret 171/2004, de 30 de gener, relatius a: Avaluació de riscos del centre de treball, mesures de prevenció, pla d'emergència i qualsevol altre que correspongui.

El contractista resta obligat a presentar, abans de formalitzar-se l'acta d'inici de prestació del servei, els documents que seguidament s'indiquen en compliment del que disposa l'art. 10.2 del Reial Decret 171/2004:

- Avaluació de riscos i planificació de l'activitat preventiva.
- Compliment de les obligacions en matèria d'informació i formació respecte dels treballadors que vagin a prestar serveis al centre de treball.
- Qualsevol altre que l'Ajuntament consideri convenient o necessari.

El contractista tindrà accés a la documentació municipal a través de la plataforma informàtica autoritzada per l'Ajuntament en la forma que li serà indicada pel responsable del contracte i haurà de presentar el documents a través de la mateixa plataforma.

Novè. Documentació que facilita l'Ajuntament

L'ajuntament disposa de documentació pro-activa en normativa de l'ENS que serà proporcionada al licitador.

L'Ajuntament facilitarà tota la informació de què disposi per realitzar l'objecte del contracte.