Diputació de Lleida
Noves Tecnologies

CONTRACTACIÓ PER MITJÀ D'UN PROCEDIMENT OBERT DE SUBMINISTRAMENT I AMPLIACIÓ DE LES LLICÈNCIES D'ANTIVIRUS ESET PROTECT ELITE PER A LA DIPUTACIÓ DE LLEIDA

PLEC DE PRESCRIPCIONS TÈCNIQUES

Diputació de Lleida
Noves Tecnologies

1. OBJECTE DEL CONTRACTE

És objecte del contracte actual el subministrament de 1300 llicències d'antivirus ESET PROTECT ELITE, així com les eines necessàries per a la seva administració en el Sistema Informàtic de la Diputació de Lleida i els serveis de gestió d'amenaces avançades inherents a la solució, instal·lats als ordinadors i servidors de la Diputació de Lleida

La necessitat del mateix ve determinada pels següents motius:

La Diputació de Lleida en l'actualitat disposa de 1100 llicències d'ESET Protect Enterprise, les citades llicències caduquen en el present any, per tant, és necessària la contractació de l'adquisició, manteniment de la plataforma d'antivirus per la Diputació de Lleida, tant per als llocs de treball com els servidors, així com les eines necessàries per a la seva administració al sistema informàtic.

Així mateix, davant la creixent aparició d'amenaces avançades que impliquen una major exposició a riscos abans no coneguts, es requereix la millora de la protecció instal·lada, afegint noves tecnologies que millorin la protecció de la pròpia Diputació de Lleida. Per aquest motiu és necessària la millora de l'actual protecció a l'ESET Protect Elite.

La citada adquisició és necessària i obligatòria per a tenir actualitzada la seguretat dels equips de treball i servidors de la Diputació de Lleida. La solució haurà de garantir el compliment dels principis bàsics i requisits mínims requerits per a una protecció adequada de la informació que constitueix l'Esquema Nacional de Seguretat (ENS). En concret s'haurà d'assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de dades, informacions i serveis utilitzats en mitjans electrònics, que són objecte de la present contractació.

2. REQUERIMENTS DEL SUBMINISTRAMENT

A- CARACTERÍSTIQUES DEL PRODUCTE

Se sol·licita l'adquisició, instal·lació, configuració i manteniment de 1300 llicències de software de seguretat ESET PROTECT ELITE que inclogui funcionalitats d'antivirus, sistema de protecció contra amenaces avançades i anàlisis de codi desconegut per a la protecció d'equips de treball i servidors corporatius, així com el software necessari per a la seva instal·lació, gestió i administració centralitzada.

La solució de protecció de llocs de treball ha d'estar suportada en sistemes operatius Microsoft Windows, així com Windows Server, Linux.

- Es tracta de l'adquisició d'un motor antivirus amb la màxima protecció possible. Són els següents tipus de protecció:

2.1.- Protecció EPP. ESET Endpoint Security

- Antivirus i antiespia: ha de detectar i eliminar tot tipus d'amenaces com ara virus, rootkits, cucs i software espia. Disposarà d'anàlisi potenciada per la consulta en el núvol de la base de dades d'informació sobre possibles processos sospitosos per a obtenir una major rapidesa en les anàlisis i reduir el mínim de falsos positius.

Diputació de Lleida
Noves Tecnologies

- Sistema avançat de prevenció d'intrusions (HIPS): protegirà els registres del sistema, els processos, les aplicacions i els arxius enfront de modificacions no autoritzades. El comportament d'aquesta funcionalitat permetrà ser personalitzat per a detectar fins i tot amenaces desconegudes en funció de comportaments sospitosos.
- Control web: permetrà limitar l'accés a determinades pàgines web depenent del seu contingut o categoria, sobre la base de regles per a grups d'usuaris, per a així complir amb les polítiques de la Diputació de Lleida i bloquejar pàgines que generen un alt volum de trànsit.
- Detecció de xarxes de confiança: permetrà definir xarxes de confiança i protegir totes les altres connexions a través d'una protecció restrictiva, per a fer que els portàtils de la Diputació de Lleida i bloquejar pàgines que generen un alt volum de trànsit.
- Detecció de xarxes confiança: permetrà definir xarxes de confiança i protegir totes les altres connexions a través d'una protecció restrictiva, per a fer que els portàtils de la Diputació de Lleida siguin invisibles en les xarxes Wi-Fi públiques.
- Tallafocs bidireccional: evitarà l'accés no autoritzat a la xarxa i protegirà la informació contra el robatori de dades. L'administració remota comptarà amb un assistent per a fusionar les regles del tallafocs per a permetre agregar regles als equips de la xarxa de forma molt fàcil i ràpida.
- Client antispam: filtrarà el correu no desitjat en l'equip client, mentre protegeix l'usuari de les amenaces que es transmeten a través del correu electrònic. Es podran establir llistes blanques i negres de manera separada per a cada client o grup. L'antispam podrà filtrar els protocols POP3, IMAP, MAPI i HTTP.
- Control de dispositius: evitarà el robatori d'informació, bloquejant els dispositius i mitjans extraïbles, dispositius, usuaris i grups.
- Instal·lació basada en components: permetrà instal·lar tots o només alguns dels següents components: tallafocs, antispam, control web, control de dispositius, compatibilitat amb Microsoft NAP i protecció d'accés a la web. També es podran activar/desactivar remotament els mòduls instal·lats.
- Múltiples formats de registres: permetrà guardar els registre de l'aplicació en formats comuns com són CSV i text pla, i els registres d'esdeveniments de Windows per a la seva anàlisi immediata o per a emmagatzemar-los per a la seva posterior utilització quan sigui necessari. Aquests registres podran ser llegits per eines SIEM de tercers.
- Escut contra ransomware: una capa addicional que protegeix els usuaris del ransomware. Monitora i avalua totes les aplicacions executades en funció del seu comportament i reputació. Està dissenyat per a detectar i bloquejar processos que s'assimilen al comportament del ransomware.
- Protecció contra botnets: la protecció contra botnets detecta la comunicació maliciosa utilitzada per aquestes xarxes zombi i, al mateix temps, identifica els processos ofensius. Qualsevol comunicació maliciosa detectada es bloqueja i es notifica a l'usuari.
- Baix consum de recursos: permetrà garantir un alt nivell de protecció en l'equip, deixant la majoria dels recursos del sistema per executar els programes que s'utilitzen normalment.

2.2.- Protecció de servidors. ESET Server Security

- Antivirus i antiespia: proporcionarà una anàlisi en temps real de la informació emmagatzemada al servidor.

Diputació de Lleida
Noves Tecnologies

- Protecció multiplataforma: eliminarà les amenaces dirigides a tot tipus de sistemes operatius, com ara Windows, Mac i Linux, evitant també que es propaguin d'un sistema operatiu a un altre.
- Identificarà els comptes d'usuaris utilitzades en els intents d'infecció.
- La desinstal·lació del producte estarà protegida per contrasenya.
- Exclourà automàticament els arxius crítics del servidor.
- Detectarà les funcions del servidor automàticament per a excloure arxius crítics, com a processos, bases de dades i arxius de paginació, de l'anàlisi en temps real de a reduir el consum.

2.3.- Protecció de dispositius Android. ESET Endpoint Security Android

- Bloqueig remot: cap persona sense permís podrà accedir a la informació emmagatzemada en el dispositiu. S'ha de poder bloquejar l'accés al telèfon o tauleta en cas de pèrdua o robatori només enviant un missatge de text (SMS).
- Esborrat remot de dades: es podran esborrar de manera remota els contactes, missatges, documents, etc., de la memòria interna i de les targetes de memòria perquè ningú pugui accedir a la informació. El sistema d'esborrament assegurarà que aquesta informació serà irrecuperable en el futur, assegurant la confidencialitat de la informació.
- Localització per GPS: s'haurà de poder saber la localització del dispositiu mòbil i contribuir a la seva recuperació mitjançant l'enviament d'un missatge de text, gràcies al GPS del dispositiu.
- Comprovació de la targeta SIM: si s'insereix una targeta SIM no autoritzada, el contacte d'administrador haurà de rebre informació sobre la targeta SIM inserida, incloent-hi el número de telèfon i els codis IMSI i IMEI.
- Contactes definits com a administrador: es podran establir un o més contactes d'administrador per al parc de mòbils, per tal que rebin tota la informació important en cas de pèrdua o robatori d'algun dispositiu.
- Bloqueig de trucades: permetrà bloquejar les trucades que procedeixin de números desconeguts o ocults i també les trucades de números no desitjats. Es podrà definir una llista de contactes permesos/bloquejats.
- Protecció contra la desinstal·lació: solament els usuaris autoritzats podran desinstal·lar el producte, assegurant d'aquesta manera la protecció del dispositiu.
- Filtrat de missatges SMS/MMS: permetrà filtrar tots els missatges SMS/MMS. També permetrà definir una llista negra o blanca personalitzable o simplement bloquejar tots els números desconeguts.
- Protecció en temps real: protegirà totes les aplicacions, arxius i targetes de memòria, de forma optimitzada per a dispositius mòbils.
- Auditoria de seguretat: l'auditoria de seguretat permetrà comprovar l'estat de totes les funcions importants del telèfon.
- Anàlisi d'intents d'accés: l'anàlisi avançat protegirà els telèfons intel·ligents i tauletes de les amenaces que intenten accedir al sistema per mitjà de Bluetooth o Wi-Fi.
- Anàlisi sota demanda: l'anàlisi sota demanda proporcionarà una anàlisi i neteja fiable d'amenaces en la memòria integrada i en els mitjans extraïbles. També serà compatible amb l'anàlisi de carpetes específiques.
- L'Administració remota permetrà comprovar l'estat de seguretat del parc de dispositius mòbils. Es podrà realitzar l'anàlisi sota demanda, establint polítiques de seguretat i una

Diputació de Lleida
Noves Tecnologies

contrasenya per a la desinstal·lació. Permetrà obtenir una visió general de les plataformes, romanent sempre informat de l'estat de la seguretat dels dispositius mòbils.

- Missatge de l'administrador: permetrà a l'administrador enviar un missatge al dispositiu amb text personalitzable. Es podrà establir la prioritat del missatge, en almenys tres nivells: Normal, Avís o Crític.

2.4.- Sandbox en el núvol. ESET LiveGuard Advanced.

- Protecció automàtica: l'equip o servidor decideix automàticament si una mostra és bona, dolenta o desconeguda. Si la mostra és desconeguda, s'envia la sandbox al núvol per a la seva anàlisi. Una vegada que finalitza l'anàlisi, el resultat es comparteix i els equips responen en conseqüència.
- Configuració personalitzable: permet la configuració de polítiques detallades per equip perquè l'administrador pugui controlar el que s'envia i el que hauria de succeir en funció del resultat rebut.
- Detecció de ransomware i amenaces zero-day: té la capacitat de detectar els nous tipus d'amenaces mai vists. Utilitza tres tipus de models diferents d'aprenentatge automàtica quan s'envia un arxiu. Després, executa la mostra en un sandbox, simulant el comportament dels usuaris per a confondre a les tècniques anti evasives. Posteriorment, s'utilitza una xarxa neuronal d'aprenentatge profund per a comparar el comportament observat amb les dades històriques. Finalment, s'utilitza l'última versió del motor d'anàlisi per a desarmar-lo a la recerca de qualsevol element inusual.
- Informes detallats: els administradors poden crear informes de les dades de la consola. Poden, o bé usar un dels informes predefinits o crear un totalment personalitat.
- Enviament manual: un usuari o administrador pot enviar mostres en qualsevol moment per a la seva anàlisi i obtenir resultats complets. Els administradors veuran qui ho va enviar, què va enviar i quin va ser el resultat directament des de la consola.

2.5.- Xifratge de disc complet. ESET Full Disk Encryption.

- Permet xifrar discs del sistema, particions i unitats senceres per a garantir que tot l'emmagatzemat en cada PC o portàtil romangui bloquejat i segur, protegint-te així contra el robatori o pèrdua.
- Seguretat abans de l'inici del sistema, totalment transparent, utilitzant la validació FIPS 140-2 i el xifratge AES de 256 bits.
- Permet iniciar i gestionar el xifratge de manera remota.
- Administració remota total que permet la creació i eliminació de comptes d'usuari.
- Permet la recuperació de la contrasenya del client de manera remota.

- Gestiona el xifratge en dispositius Windows i MacOS.

2.6.- Consola administració servidors Ajuntament. ESET PROTECT

- Un únic panell de gestió: tots els productes que s'executen en Windows, MacOS, Linux es poden administrar des d'una única instància. A més, és compatible amb l'administració de dispositiu mòbils (MDM) de dispositius Android i iOS.
- Instal·lació flexible: es pot instal·lar a Windows, Linux o a través d'una Virtual Appliance. Després de la instal·lació, tota l'administració es realitza a través d'una consola web, la

Diputació de Lleida
Noves Tecnologies

qual cosa permet un fàcil accés i administració des de qualsevol dispositiu o sistema operatiu.

- Control de polítiques: es podran configurar múltiples polítiques per a un mateix equip o un grup. A més, es poden configurar les polítiques per part de l'administrador, o bloquejar qualsevol configuració dels usuaris finals.
- Suport SIEM: totalment compatible amb les eines SIEM i pot generar tota la informació de registre en el format JSON o LEEF.
- Grups estàtics i dinàmics: utilitza una gestió de clients, similar a la d'Active Directory. Els clients poden ser assignats a grups estàtics o dinàmics, així com la possibilitat de crear Grups Estàtics. També és possible assignar una directiva a un grup dinàmic, i s'aplicarà als equips clients quan passin a formar part del grup i serà eliminada quan surtin d'ell. Això ocorre sense interacció de l'administrador/usuari.
- Directives. L'administrador pot definir directives per a cada producte de seguretat. L'agent s'encarrega d'aplicar la directiva, per tant, fins i tot sense connexió a la consola, aquest és capaç d'aplicar les directives assignades a un grup específic.
- Tasques. Les tasques es creen amb l'assistent i es classifiquen clarament per a diversos productes de seguretat. Això també inclou les tasques preconfigurades.
- Informes. Els administrador poden triar entre plantilles predefinides d'informes o crear les seves pròpies plantilles personalitzades, tan sols usant un conjunt preseleccionat de dades i valors. Recopila només la informació que és necessària per a generar els informes, els registres restants s'emmagatzemen en l'equip client, la qual cosa millora el rendiment de la base de dades. Cada plantilla de l'informe pot ser consultada en la consola web com un element del planell de control per a proporcionar a l'administrador una excel·lent visió general en temps real de la seguretat de la xarxa, amb opcions més detallades. A part de mostrar informes mitjançant la consola web, aquests poden ser exportats a formats PDF o enviats com a correu electrònic d'informe de notificació.
- Notificacions. Els administradors reben notificacions de totes les incidències de seguretat de la xarxa corporativa per a poder reaccionar immediatament. Les plantilles poden ser aplicades a uns certs membres de grups dinàmics o activades per indicacions específiques o esdeveniments, ja que són guardades en els registres d'esdeveniments.
- SysInspector® integrat. SysInspector és una eina de diagnòstic que ajuda a solucionar una àmplia gamma d'incidències del sistema i està integrada en la consola web. L'administrador pot accedir directament a tots els informes de SysInspector generats per a un client particular. Això permet a l'administrador realitzar un seguiment de les incidències de seguretat o dels canvis del sistema de manera cronològica.
- La instal·lació de la consola ha d'estar ubicada necessàriament en recursos dins de la Unió Europea.

2.7.- Protecció EDR. ESET Inspect.

- Threat Hunting. Permetrà l'aplicació de filtres de dades per a classificar els arxius segons la popularitat, la reputació, la signatura digital, el comportament o la informació contextual. La instal·lació de múltiples filtres permet una cerca d'amenaces fàcil i automatitzada, incloses les APT i els atacs dirigits que es poden personalitzar. En ajustar les regles de comportament, permetrà personalitzar també per a realitzar Threat Hunting d'amenaces anteriors i "tornar a analitzar" tota la base de dades d'esdeveniments.

Diputació de Lleida
Noves Tecnologies

- Detecció d'incidències i anomalies. Permetrà comprovar totes les accions realitzades per un executable i utilitza el sistema de reputació LiveGrid per a avaluar ràpidament si els processos executats són segurs o sospitosos. La supervisió dels incidents anòmals relacionats amb els usuaris és possible gràcies a regles específiques escrites per a ser activades pel comportament, no per simples deteccions de malware o signatures. L'agrupació d'equips per usuari o departament permetrà als equips de seguretat identificar si l'usuari té permís per a realitzar una acció específica o no.
- Aïllament amb un clic. Permetrà definir polítiques d'accés a la xarxa per a aturar ràpidament els moviments laterals del malware. Permetrà aïllar un dispositiu compromès de la xarxa amb un sol clic en la interfície EEI. A més, retira fàcilment els dispositius de l'estat de contenció.
- Etiquetatge. Permetrà assignar i anul·lar l'assignació d'etiquetes per a un filtrat ràpid d'objectes com equips, alarmes, exclusions, tasques, executables, processos i scripts. Permetrà compartir les etiquetes entre els usuaris i, una vegada creades, es podran assignar en qüestió de segons.
- Recerca i resolució. Permetrà utilitzar una sèrie de regles existents o crear regles pròpies per a respondre davant els incidents detectats. Cada alarma activada presenta uns passos a seguir per a solucionar-los. Aquesta funcionalitat de resposta ràpida ajuda a garantir que tots els incidents siguin detectats.
- Protecció contra la fuga de dades. Permetrà bloquejar l'execució de mòduls malintencionats en qualsevol equip de la xarxa de la seva organització. L'arquitectura ofereix la flexibilitat de detectar fuga de dades sobre l'ús de software específic com aplicacions torrent, emmagatzematge en el núvol, navegació Tor o un altre software no desitjat.
- Puntuació. Permetrà prioritzar la gravetat de les alarmes amb una funció de puntuació que atribueix un valor de gravetat als incidents i permetrà a l'administrador identificar fàcilment els equips amb una major probabilitat d'un incident potencial.
- Integració nativa amb fonts d'informació de tercers. La solució EDR estarà integrada, per defecte, amb les bases de coneixements de tercers MITRE ATT&CK™ i Virus Total i es podrà accedir a aquesta informació amb un clic i sense necessitat de configurar res.
- Sistema de gestió d'incidents. Agrupa deteccions, equips, executables o processos en unitats lògiques per a veure possibles esdeveniments maliciosos en una franja de temps, amb accions d'usuaris relacionades. ESET Inspect suggereix automàticament a l'encarregat de respondre als incidents tots els esdeveniments i objectes relacionats que poden ser de gran ajuda en les etapes de classificació, recerca i resolució d'un incident.

2.8.- Protecció d'entorns de treball cloud (Office365 i Google Workspace). ESET Cloud Office Security

- Multi-tenant. Possibilitat de protegir i administrar diversos inquilins de Microsoft 365 i Google Workspace des d'una consola. Permet establir polítiques sobre els usuaris i les aplicacions de la seva organització per a complir les polítiques de seguretat i operatives.
- Antispam. Incorpora diverses tecnologies (RBL i DNSBL, Creació d'empremtes digitals, comprovació de la reputació, anàlisi del contingut, regles, definició manual de llistes blanques i negres, protecció contra valors de tornada i validació de missatges mitjançant SPF i DKIM). ESTE Mail Security Antispam està al núvol, i la majoria de les bases de dades del núvol estan en centres de dades d'ESET. Els serveis al núvol Antispam

Diputació de Lleida
Noves Tecnologies

permeten actualitzar les dades ràpidament, cosa que significa una reacció més ràpida en cas de nou correu no desitjat.

- Anti-phishing. Impedeix als usuaris accedir a les pàgines web conegudes per activitats de phishing. Analitzador sofisticat que busca en el cos i assumpte dels missatges de correu electrònic entrants per a identificar aquests vincles (adreces URL). Els vincles es comparen amb una base de dades de phishing.
- Anti-Malware. Protecció contra atacs i eliminació de tota mena d'amenaces, inclosos virus, ransomware, rootkits, cucs i spyware amb anàlisis al núvol per aconseguir taxes de detecció encara millors. Ocupa poc espai i no requereix massa recursos dels sistema i, per tant, no redueix el seu rendiment. Utilitza un model de seguretat per capes. Cada capa, o fase, presenta un nombre de tecnologies centrals. La fase d'execució prèvia incorpora tecnologies com a anàlisis UEFI, protecció contra els atacs de xarxa, reputació i caixet, entorn de proves al producte, deteccions d'ADN. Les tecnologies de la fase d'execució són bloquejador d'exploits, protecció contra ransomware, anàlisi avançada de memòria i anàlisi d'scripts (AMSI), mentre que en la fase posterior a l'execució s'utilitzen protecció contra botnets, sistema de protecció de malware al núvol i entorn de proves.
- Polítiques. Ajustos de protecció basats en polítiques que es poden assignar als inquilins, usuaris, grups de l'equip o llocs de SharePoint seleccionats. Pot personalitzar cada política d'acord amb les seves necessitats.
- Administrador de quarantena. Inspecciona els objectes en quarantena i realitza una acció adequada (descarregar, eliminar o alliberar). Aquesta funció ofereix una administració senzilla dels missatges de correu electrònic, els arxius adjunts i els arxius d'Exchange Online/OneDrive/Grups de l'equipo/Llocs de SharePoint que ha posat en quarantena ESET Cloud Office Security. La descàrrega ofereix l'opció d'analitzar els objectes en quarantena amb eines de tercers.
- Estadístiques de detecció. Informació general sobre les activitats de seguretat de Microsoft365. El panell conté informació essencial en cadascuna de les seves pestanyes d'informació general (Exchange Online/OneDrive/Grups de l'equipo/Llocs de SharePoint). La informació general d'usuari mostra el nombre d'inquilins i l'ús de llicències, així com estadístiques de cada inquilí: nombre d'usuaris, principals destinataris d'spam/phishing/malware i principals comptes de OneDrive, grups de l'equip i llocs de SharePoint sospitosos. Pot triar un període de temps i un inquilí per als quals mostrar les estadístiques. En les pestanyes d'informació general Exchange Online, OneDrive, Grups de l'equip i llocs de SharePoint es poden veure estadístiques i gràfics de detecció addicionals. Es tracta d'estadístiques com el nombre de correus electrònics i arxius analitzats i el número d'spam/phishing/malware detectat. Els gràfics mostren el trànsit de cada tipus de detecció: spam, malware i phishing.
- Deteccions amb opcions de filtrat. Inclou registres de totes les deteccions realitzades per l'anàlisi del correu electrònic a la pestanya Exchange Online, així com les realitzades per l'anàlisi d'arxius a la pestanya OneDrive/Grup de l'equip o llocs de SharePoint. Permet filtrar i buscar de manera eficaç mitjançant informació addicional sobre la detecció específica (per exemple, el nom de l'amenaça, el hash de l'arxiu, etc.).
- Usuaris. L'entitat central que protegeix ESTE Cloud Office Security és el compte d'usuari. Permet investigar deteccions relacionades amb un usuari específic. També pot triar quins usuaris desitja protegir. Els usuaris es classifiquen en grups. Cada grup és un inquilí de Microsoft365 que conté els seus usuaris. Permet utilitzar múltiples criteris de filtrat per a facilitar la cerca d'un usuari específic dins d'un grup.

Diputació de Lleida
Noves Tecnologies

- Proteccions d'informes i aprenentatge automatitzat.
- Informes (estadístics i de quarantena). Permet rebre dades estadístiques d'Exchange Online, OneDrive, grups de l'equip i llocs de SharePoint per correu electrònic, o generar i descarregar un informe únic per a un període triat. Pot programar informes perquè es generin i distribueixin periòdicament als destinataris de correu electrònic especificats. Triar PDF o CSV com a format de sortida. Els informes contenen dades, com un nombre de correus electrònics analitzats i malware, phishing i spam detectats. També contenen estadístiques independents dels destinataris més destacats de cada categoria: malware, phishing i spam. Hi ha diverses opcions disponibles per a generar informes. A més, permet enviar als destinataris seleccionats un informe de quarantena de correu electrònic, que és una llista dels missatges de correu electrònic posats en quarantena. L'informe de quarantena de correu electrònic s'envia en la data i a l'hora especificades, però només si hi ha elements nous que notificar.
- Equips i llocs. Ofereix protecció per a grups de l'equip o llocs de SharePoint. D'aquesta manera, s'amplia la protecció de les solucions de col·laboració de Microsoft365 amb la protecció de SharePoint i grup de l'equip mitjançant l'ús compartit segur d'arxius.
- Protecció avançada a través de sandbox al núvol. Incorpora una solució d'entorn de proves basada en el núvol que analitza els arxius enviats executant el codi sospitós en un entorn aïllat per a avaluar el seu comportament. Envia a analitzar els arxius adjunts de correu electrònic i els arxius d'Exchange Online, OneDrive, grups de l'equip i llocs de SharePoint que són sospitosos a ESET LiveGuard Advanced.
- Registres d'auditoria. Permet a l'administrador comprovar les activitats realitzades en ESET Cloud Office Security. Aquesta funció pot resultar útil, especialment quan hi ha diversos usuaris de la consola d'ESET Cloud Office Security. Les entrades del registre d'auditoria mostren les activitats i la seqüència en la qual es van realitzar. Els registres d'auditoria emmagatzemen informació sobre l'operació o l'esdeveniment específic. Els registres d'auditoria es generen sempre que es crea o modifica un objecte ESET Cloud Office Security (grup de llicències, usuari, política, informe o element de quarantena com a dades adjuntes).
- Exportació de syslogs. Permet exportar els esdeveniments registrats enumerats en deteccions i enviar-los al servidor de syslog. Pot triar quins esdeveniments desitja exportar. Els esdeveniments són per a Exchange Online/Gmail, OneDrive/Google Drive, grups d'equips i SharePoint Online.

2.9.- Protecció de servidors de correu ON-PREM. ESET Mail Security

- Anti-Malware. Protecció contra atacs i eliminació de tota mena d'amenaces, inclosos virus, ransomware, rootkits, cucs i spyware amb anàlisis en el núvol per aconseguir taxes de detecció encara millors. Ocupa poc espai i no requereix massa recursos del sistema i, per tant, no redueix el seu rendiment. Utilitza un model de seguretat per capes. Cada capa, o fase, presenta un nombre de tecnologies centrals. La fase d'execució prèvia incorpora tecnologies con a anàlisis UEFI, protecció contra els atacs de xarxa, reputació i caixet, entorn de proves en el producte, detecció d'ADN. Les tecnologies de la fase d'execució són blocador d'exploits, protecció contra ransomware, anàlisi avançada de memòria i anàlisi d'scripts (AMSI), mentre que en la fase posterior a l'execució s'utilitzen protecció contra botnets, sistema de protecció de malware al núvol i entorn de proves.

Diputació de Lleida
Noves Tecnologies

- Antispam. Incorpora diverses tecnologies (RBL i DNSBL, creació d'empremtes digitals, comprovació de la reputació, anàlisi del contingut, regles, definició manual de llistes blanques i negres, protecció contra valors de tornada i validació de missatges mitjançant SPF i DKIM). ESET Mail Security Antispam està al núvol, i la major de les bases de dades del núvol estan en centres de dades d'ESET. Els serveis al núvol Antispam permeten actualitzar les dades ràpidament, cosa que significa una reacció més ràpida en cas de nou correu no desitjat.
- Anti-phishing. Impedeix als usuaris accedir a pàgines web conegudes per activitats de phishing. Analitzador sofisticat que busca en el cos i assumpte dels missatges de correu electrònic entrants per a identificar aquests vincles (adreces URL). Els vincles es comparen amb una base de dades de phishing.
- Regles. Les regles permeten als administradors filtrar correus electrònics i arxius adjunts no desitjats segons la política de l'organització. Parlem d'arxius adjunts com a executables, arxius multimèdia, arxius comprimits protegits per contrasenya, etc. És possible realitzar diferents accions amb els missatges de correu electrònic filtrats i els seus arxius adjunts, com per exemple enviar-los a la quarantena, eliminar-los, enviar notificacions o registrar l'esdeveniment.
- Exportar a servidor de syslog (Arcsight). Permet duplicar el contingut del registre de protecció del servidor de correu electrònic en format d'esdeveniment comú (CEF) per a usar-ho amb solucions de gestió de registres com, per exemple, Micro Focus ArcSight. Els successos es poden transferir a través d'SmartConnector a ArcSight o exportar-se a arxius. Això proporciona una forma còmoda de supervisar i administrar els successos de seguretat de forma centralitzada.
- Anàlisi de bústies d'Office365.
- Administrador de quarantena.
- Informes de quarantena.
- Anàlisi a petició.
- Administració de diversos servidors de correu en clúster.
- Configuració d'exclusions.
- Instal·lació basada en components: es pot personalitzar per a triar quins mòduls del producte instal·lar.

2.10.- Gestió de vulnerabilitats i pegats. ESET Vulnerability & Patch Management

- Avaluació de vulnerabilitats.
- Permet explorar el sistema a la recerca d'aplicacions instal·lades que presentin vulnerabilitats.
- Detecció automatitzada de CVE (vulnerabilitats comunament conegudes)
- Permet prioritzar i filtrar vulnerabilitats per nivell de gravetat.
- Subministra informes de vulnerabilitats de les aplicacions i els dispositius més susceptibles.
- Administració de pegats.
- Permet iniciar la instal·lació i actualització de pegats de manera immediata mitjançant tasques automatitzades o de manera manual.
- Permet prioritzar els pegats en actius crítics deixant la resta per a moments de menys càrrega de treball de la xarxa.

Diputació de Lleida
Noves Tecnologies

- Permet registrar i portar un control de les excepcions de no aplicació de pegats en aplicacions crítiques seleccionades.
- Proporciona un inventari actualitzat de pegats.
- Tots els pegats disponibles i aplicables des de consola d'administració.

2.11.- Aplicació de doble factor d'autenticació (2FA). ESET Secure Authentication

- Permet agregar l'autenticació de dos factors (2FA) als dominis de Microsoft Active Directory o a la xarxa d'àrea local, cosa que significa que es genera i es proporciona una contrasenya d'un sol ús (OTP) juntament amb el nom d'usuari i la contrasenya generalment requerits. O bé, es genera una notificació push que ha d'aprovar-se al telèfon mòbil de l'usuari amb sistema operatiu Android, iOS o Windows quan l'usuari s'hagi autenticat correctament amb les seves credencials d'accés generals.
- Ha de permetre agregar l'autenticació de doble factor a:
  - Windows Login
  - Protocol RDP (Remote Desktop)
  - RADIUS Server per a proteccions de xarxes VPN
  - Aplicacions web de Microsoft
  - Serveis de federació d'Active Directory.
- Ha de possibilitar la integració en aplicacions personalitzades a través d'API o SDK,
- Ha de posseir una consola d'administració de la solució centralitzada.
- Ha de permetre la sincronització amb Active Directory o bé la implementació en equips stand-alone.

B- SERVEIS INCLOSOS

- Detecció, monitoratge i resposta d'amenaces, 24hs. del dia, els 365 dies de l'any, duta a terme per experts, utilitzant la informació que genera l'eina ESET Inspect. Capacitat de delegar la implementació de mesures de remediació.
- Suport realitzat per tècnics especialistes del fabricant complementat amb aplicació d'IA per a una detecció i resposta ràpida i assertiva.
- Accés a la biblioteca predefinida i personalitzada de patrons de comportament de detecció perquè pugui utilitzar-se com a plantilla, com a pas previ a la personalització de la configuració específica per a les necessitats de l'entorn.
- Generació i enviament d'informes personalitzats setmanals i mensuals d'amenaces detectades. Accés a generació d'informes sobre incidents, l'estat de l'entorn i altres detalls gestionats pel servei.
- Aplicació de contra mesures de protecció a partir del monitoratge constant realitzat pels tècnics de campanyes actives de grups de malware.
- Generació de conjunts de patrons de comportament i optimització d'exclusions personalitzades i adaptades a l'entorn del client.
- Monitoratge continu que aprofita IoC, IoA, UEBA i IA, així com fonts externes i internes d'intel·ligència d'amenaces.
- Monitoratge continu 24/7 dirigida per professionals del fabricant, detecció, triatge i resposta.
- Servei facilitat en castellà i en català.
- Suport tècnic 24/7.

Diputació de Lleida
Noves Tecnologies

Requisits mínims generals:

- La solució EPP com l'EDR ha de funcionar de forma integrada i ha de ser del mateix fabricant.
- L'adjudicatari ha d'estar autoritzat i certificat per part del fabricant per a poder revendre els productes oferts.
- S'han de poder aplicar diferents polítiques de seguretat diferenciades per equips i per grups.
- El software podrà empaquetar i distribuir de manera automatitzada per tota la xarxa corporativa, ha de permetre la instal·lació silenciosa i desatesa.
- S'han de poder definir polítiques de seguretat definides per Endpoint i per grups.
- El producte Endpoint instal·lat serà actualitzable i gestionat tant des de dins com des de fora de la xarxa corporativa.
- Els productes inclosos han de proporcionar actualitzacions i millores constants que s'adaptin a l'aparició de noves amenaces. Durant la vigència del contracte es tindrà dret a aquestes actualitzacions.
- La solució ha de comptar amb mecanismes de seguretat per a evitar la reconfiguració i la desinstal·lació per part d'agents no autoritzats.
- Accés al suport proporcionat directament pel fabricant de la solució en format 24/7 i atesa en castellà, sense límit de consultes durant la vigència del contracte.

3. SERVEIS D'INSTAL·LACIÓ I TERMINI D'EXECUCIÓ

Actualment la Diputació de Lleida té 1100 llicències d'ESET Protect Enterprise, per tant, les noves funcionalitats hauran d'actualitzar-se als equips, el fabricant realitzarà les formacions necessàries perquè aquesta actualització es realitzi amb la menor quantitat possible d'incidències.

El termini màxim d'entrega de les llicències és de 10 dies naturals, a partir de la formalització del contracte.

4. CONFIDENCIALITAT

L'adjudicatari estarà obligat a tractar de forma confidencial i reservada tant la informació rebuda com la derivada de l'execució del contracte, no podent ser objecte de difusió, publicació o utilització per a fins diferents als establerts en aquest plec. Aquesta obligació continuarà vigent una vegada que el contracte hagi finalitzat o hagi estat resolt.

A.- Tractament de dades

L'adjudicatari queda expressament obligat a mantenir indefinidament absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer en ocasió del compliment del contracte, especialment els de caràcter personal, inclosos al registre d'activitats de tractament de la Diputació de Lleida, que no podrà copiar o utilitzar amb fi diferent al que figura en aquest document, ni tampoc cedir a uns altres ni tan sols a efectes de conservació.

Diputació de Lleida
Noves Tecnologies

El licitador quedarà obligat al compliment del que es disposa el Reglament General de Protecció de Dades (Reglament 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE).

L'adjudicatari, segons el paràgraf anterior, tindrà les següents obligacions:

L'encarregat del tractament i tot el seu personal s'obliga a partir de la subscripció del contracte actual a:

a. Utilitzar les dades personals objecte del tractament, o els que reculli per a la seva inclusió, només a la finalitat objecte d'aquest encàrrec. En cap cas podrà utilitzar les dades per a altres diferents a les objecte del contracte

b. Tractar les dades d'acord amb les instruccions del responsable del tractament.

Si l'encarregat del tractament considera que alguna de les instruccions infringeix el Reglament General de Protecció de Dades (Reglament (UE) 2016/679, del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE) o qualsevol altra disposició en matèria de protecció de dades de la Unió o dels Estats membres, l'encarregat informarà immediatament al responsable.

c. No comunicar les dades a terceres persones, tret que compti amb l'autorització expressa del responsable del tractament, en els supòsits legalment admissibles.

L'encarregat pot comunicar les dades a altres encarregats del tractament del mateix responsable, d'acord amb les instruccions del responsable. En aquest cas, el responsable identificarà, de manera prèvia i per escrit, l'entitat a la qual s'han de comunicar les dades, les dades a comunicar i les mesures de seguretat a aplicar per a procedir a la comunicació.

Si l'encarregat ha de transferir dades personals a un tercer país o a una organització internacional, en virtut del dret de la Unió o dels Estats membres que li sigui aplicable, informarà al responsable d'aquesta exigència legal de manera prèvia, tret que el dret ho prohibeixi per raons importants d'interès públic.

d. No subcontractar cap de les prestacions que formin part de l'objecte d'aquest contracte que comportin al tractament les dades personals, excepte els serveis auxiliars necessaris per al normal funcionament del serveis de l'encarregat.

Si fos necessari subcontractar algun tractament, aquest fet s'haurà de comunicar prèviament i per escrit al responsable, amb una antelació d'almenys un mes indicant els tractaments que es pretén subcontractar i identificant de manera clara i inequívoca l'empresa subcontractista i les seves dades de contacte. La subcontractació podrà dur-se a terme si el responsable no manifesta la seva oposició en el termini establert.

El subcontractista, que també tindrà la condició d'encarregat del tractament, està obligat igualment a complir les obligacions establertes en aquest document per a l'encarregat del tractament i les instruccions que dicti el responsable. Correspon a l'encarregat inicial regular la nova relació de forma que el nou encarregat quedi subjecte a les mateixes

Diputació de Lleida
Noves Tecnologies

condicions (instruccions, obligacions, mesures de seguretat, etc.) i amb els mateixos requisits formals que ell, referent a l'adequat tractament de les dades personals i a la garantia dels drets de les persones afectades. En el cas d'incompliment per part del subencarregat, l'encarregat inicial continuarà sent plenament responsable davant el responsable en lo referent al compliment de les obligacions.

e. Mantenir el deure de secret respecte a les dades de caràcter personal als quals hagi tingut accés en virtut del present encàrrec, fins i tot després que finalitzi el seu objecte.

f. Garantir que les persones autoritzades per a tractar dades personals es comprometin, de manera expressa i per escrit, a respectar la confidencialitat.

g. Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per a tractar dades personals.

h. Retornar al responsable del tractament les dades de caràcter personal i, si escau, els suports on constin, una vegada complerta la prestació.

La devolució ha de comportar l'esborrament total de les dades existents als equips informàtics utilitzats per l'encarregat.

No obstant això, l'encarregat pot conservar una còpia, amb les dades degudament bloquejades, mentre pugui derivar-se responsabilitats de l'execució de la prestació.

i. Portar per escrit, un registre de totes les categories d'activitats de tractament efectuades per compte del responsable, que contingui:

- El nom i les dades de contacte de l'encarregat o encarregats i de cada responsable per compte del qual actuï l'encarregat i, si és el cas, del presentant del responsable o de l'encarregat i del delegat de protecció de dades.
- Les categories de tractaments efectuats per compte de cada responsable.
- Si és el cas, les transferències de dades personals a un tercer país o organització internacional, inclosa la identificació de dita tercera país o organització internacional i, en el cas de les transferències indicades en l'article 49 apartat 1, paràgraf segon del Reglament General de Protecció de Dades, la documentació de garanties adequades.

j. En el cas de dur a terme l'encàrrec de tractament en els seus locals, realitzar una anàlisi de riscos relatius al tractament objecte per encàrrec i implantar les següents mesures tècniques i organitzatives de seguretat que resultin d'aplicació a la llum dels resultats d'aquesta anàlisi:

1. La seudonimització i el xifrat de dades personals.

2. La capacitat de garantir la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i serveis de tractament.

Diputació de Lleida
Noves Tecnologies

3. La capacitat de restaurar la disponibilitat i l'accés a les dades personals de manera ràpida, en cas d'incident físic o tècnic.

4. Un procés per verificar, avaluar i valorar regularment l'eficàcia de les mesures tècniques i organitzatives establertes per garantir la seguretat del tractament.

5. Assistir al responsable del tractament en la resposta a l'exercici dels drets de:
   a. Accés, rectificació, supressió i oposició
   b. Limitació del tractament
   c. Portabilitat de les dades

6. A no ser objecte de decisions individualitzades automatitzades (inclosa l'elaboració de perfils)

Quan les persones afectades exerceixin els drets d'accés, rectificació, supressió i oposició, limitació del tractament, portabilitat de dades i a no ser objecte de decisions individualitzades automatitzades, davant l'encarregat del tractament, aquest ho ha de comunicar per correu electrònic a l'adreça que indiqui el responsable. La comunicació ha de fer-se de manera immediata i en cap cas més enllà del dia laborable següent al de la recepció de la sol·licitud, justament, si és el cas, amb altres informacions que puguin ser rellevants per a resoldre la sol·licitud.

7. D'acord amb l'article 33 del Reglament general de protecció de dades, en cas de violació de la seguretat de les dades personals, el responsable del tractament s'ha de notificar a l'autoritat de control competent, de conformitat amb l'article 55, sense dilació indeguda i, si és possible, en un termini màxim de 72 hores després que n'hagi tingut constància, tret que sigui improbable que la dita violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones físiques. Si la notificació a l'autoritat de control no es produeix en el termini de 72 hores, s'ha d'acompanyar amb la indicació dels motius de la dilació.

8. No serà necessària la notificació quan sigui improbable que aquesta violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones físiques.

Si es disposa d'ella es facilitarà, com a mínim, la informació següent:

a) Descripció de la naturalesa de la violació de la seguretat de les dades personals, inclusivament, quan sigui possible, les categories i el nombre aproximat d'interessats afectats, i les categories i el nombre aproximat de registres de dades personals afectats.
b) El nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en el qual pugui obtenir-se més informació.
c) Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.
d) Descripció de les mesures adoptades o propostes per a posar remei a la violació de la seguretat de les dades personals, incloent, si escau, les mesures adoptades per a mitigar els possibles efectes negatius.

Si no és possible facilitar la informació simultàniament, i en la mesura en què no ho sigui, la informació es facilitarà de manera gradual sense dilació indeguda.

9. Donar suport al responsable del tractament en la realització de les avaluacions d'impacte relatives a la protecció de dades, quan escaigui.

10. Donar suport al responsable del tractament en la realització de les consultes prèvies a l'autoritat de control, quan escaigui.

11. Posar a la disposició del responsable tota la informació necessària per a demostrar el compliment de les seves obligacions, així com per a la realització de les auditories o les inspeccions que realitzin el responsable o un altre auditor autoritzat per ell.

12.Designar un delegat de protecció de dades si resultés obligatori el seu nomenament i comunicar la seva identitat i dades de contacte al responsable.

B.- Compliment de l'Esquema Nacional de Seguretat

Requisit de capacitat

D'acord amb l'article 65.2 de la LCSP i els articles 2, 40 i 41 del RD 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de seguretat, les empreses licitadores que es presentin en aquesta licitació han de disposar del nivell MIG de l'ENS. La certificació del nivell mig s'haurà d'incloure en el sobre A, aquesta acreditació podrà realitzar-se mitjançant la presentació d'un certificat vigent emès per un organisme de certificació acreditat en el marc de l'ENS o bé mitjançant qualsevol altre mitjà de prova admès en dret que permeti verificar de manera fefaent el compliment del citat requisit.

La manca de compliment d'aquesta obligació tindrà caràcter excloent i comportarà la no admissió de l'oferta.

Aquest nivell de seguretat haurà de **mantenir-se durant tota l'execució del contracte**, restant l'empresa obligada a garantir la seva vigència i adequació d'acord amb l'establert en l'article 31 del RD 311/2022, de 3 de maig i resta d'articles que siguin d'aplicació del mateix text legal.

L'adjudicatari assumirà el compliment del que s'estableix a l'Esquema Nacional de Seguretat (ENS) i a l'Esquema Nacional d'Interoperabilitat (ENI) pel que fa a l'adopció de mesures de seguretat i interoperabilitat dels serveis d'e-administració afectats pel plec.

En aquest sentit, l'adjudicatari es compromet expressament a complir i vetllar pel compliment legal establert quan a l'adopció de les mesures de seguretat indicades en els Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, i 4/2010, de 8 de gener, Esquema Nacional d'Interoperabilitat.

El nivell d'implantació de les mesures de seguretat serà, com a mínim, el nivell mitjà de l'Esquema Nacional de Seguretat, independentment de la categorització que correspongui al sistema d'informació.

Diputació de Lleida
Noves Tecnologies

L'adjudicatari garantirà els principis bàsics i requisits mínims de protecció requerits a l'Esquema Nacional de Seguretat per a una protecció adequada de la informació. És d'aplicació que l'adjudicatari garanteixi l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en aquells mitjans electrònics dels quals siguin responsables o sobre els quals realitzen la prestació de serveis.

Segons el document "obligacions dels prestadors de serveis a les entitats públiques" del CCN (Centro Criptológico Nacional), l'adjudicatari té l'obligació de documentar i oferir la següent informació a la Diputació de Lleida:

- Descripció de serveis i modalitats.
- Informació sobre l'arquitectura de seguretat.
- Ubicació de la informació.
- Mesures de seguretat implementades.
- Compliment de la normativa vigent de protecció de dades.
- Incidents de seguretat.
- Cadena de subcontractació i els seus canvis.
- Seguiment dels Acords de Nivell de Servei (SLA).

La Diputació de Lleida es reserva el dret d'auditar en qualsevol moment el nivell de compliment de les mesures de seguretat d'aquest document i de les exigides en el Reglament General de Protecció de Dades, i en el document de seguretat relatiu a secret estadístic referit a l'apartat 17.

Per això la Diputació de Lleida haurà d'avisar a l'adjudicatari amb 5 dies d'antelació de la realització d'aquesta auditoria. L'adjudicatari haurà de facilitar l'accés als recursos que sol·liciti la Diputació de Lleida per a la correcta realització de l'auditoria.

L'adjudicatari en un termini no superior a 3 mesos, ha de solucionar sense cost per a la Diputació de Lleida, aquelles deficiències detectades en aquesta auditoria quan els recursos o serveis afectats siguin de la seva competència o estiguin inclosos en la prestació dels serveis que realitza.

5. OBLIGACIONS DEL CONTRACTISTA

L'abast del present contracte afectarà els següents punts:

Adquisició llicències i renovació de les mateixes per anualitats

El contractista haurà d'assegurar el subministrament de les llicències a la Diputació de Lleida i la renovació automàtica de les mateixes de forma anual sense que es pugui produir en cap moment la manca de protecció i cobertura de la Diputació respecte de les mateixes. La renovació serà automàtica amb independència de la tramitació de la certificació de pagament corresponent.

Servei de suport i control

El contractista haurà d'assegurar la prestació del servei 24x7 de suport i control derivat del subministrament del corresponent llicenciament en català i castellà.

Diputació de Lleida
Noves Tecnologies

Acreditació de la condició de partner

Donat que l'adjudicatari només podrà ser un partner autoritzat pel fabricant, haurà d'estar certificat per complir amb les funcions de distribució de les llicències i manteniment, autoritzades i necessàries per aquest determinades, les prestacions que s'incloguin, per les indicacions del fabricant corresponent del software que s'ofereixi.

L'empresa adjudicatària haurà de mantenir durant tota la vigència del contracte la condició de partner autoritzat del fabricant d'ESET.

La pèrdua d'aquesta condició tindrà la consideració d'incompliment essencial de les obligacions contractuals, atès que impedeix garantir la prestació dels serveis de manteniment i seguretat en les condicions requerides, així com l'accés a actualitzacions, repositoris i suport oficial del fabricant, de conformitat amb l'article 211 de la LCSP.

Detectada aquesta circumstància, l'òrgan de contractació requerirà a l'empresa adjudicatària que, en un termini de **10 dies hàbils**, acrediti la recuperació de la condició de partner autoritzat o proposi una solució alternativa que garanteixi la prestació del servei en les mateixes condicions i amb cobertura oficial del fabricant.

Si no s'acredita el compliment d'aquest requisit en el termini establert, l'òrgan de contractació podrà resoldre el contracte per incompliment donat que l'adjudicatari haurà perdut la corresponent habilitació empresarial objecte del contracte d'acord amb l'establert en l'article 65 de la LCSP, amb les conseqüències previstes als articles 211 i 213 de la LCSP.

Equips professionals vinculats a les tasques de manteniment i suport tècnic

Les tasques a desenvolupar i els objectius que s'han d'obtenir requereixen personal amb els coneixements tècnics necessaris i adequats per donar resposta.

L'equip que haurà de dur a terme les tasques de manteniment haurà de ser un equip suficientment capacitat per donar resposta a les necessitats tècniques per dur a terme l'objecte del present contracte.

Acreditació per part del Centre Criptològic Nacional (CCN – CERT)

El llicenciament subministrat haurà de comptar amb l'aprovació per part del Centre Criptològic Nacional (CCN – CERT). Per tal d'acreditar l'aprovació del CCN – CERT, serà necessari presentar un certificat emès per un organisme de certificació autoritzat, en el qual es confirmi de manera expressa que el producte objecte de contractació compleix amb els requisits establerts per l'ENS i ha estat degudament validat pel CCN – CERT.

6. GARANTIA, SUPORT I MANTENIMENT

Un cop transcorregut el termini d'execució del contracte i a comptar des de la data d'acceptació total d'aquest, s'estableixen els següents períodes mínims de garantia: 3 mesos des de la finalització de l'execució i de l'acceptació total del contracte.

El manteniment de les llicències inclourà el subministrament de les noves versions dels productes, així com les actualitzacions d'aquests durant el període del contracte. Les noves

Diputació de Lleida
Noves Tecnologies

versions del producte i actualitzacions estaran accessibles a través de la web i es podran descarregar de forma manual o de forma automàtica mitjançant les utilitats d'actualització que inclogui el propi software.

Es deixarà constància de la data d'inici i fi del manteniment contractat en la corresponent acta de recepció.

El licitador ha d'especificar un telèfon de contacte, un telèfon del tècnic assignat al projecte i la disponibilitat del mateix o d'un recurs equivalent. Addicionalment les incidències han d'estar documentades i donades d'alta per compte del licitador a l'eina de seguiment i control que el licitador posi a disposició de la Diputació de Lleida.

Els requeriments mínims són els següents:

- Monitoratge continu: detecció, triatge i resposta en format 24/7.
- Creació d'informes personalitzats.
- Detecció contínua d'amenaces dirigides.
- Detecció i anàlisi de patrons de comportament.
- Millora contínua, automatització i optimització de la protecció.
- Supervisió i anàlisi, campanya de detecció activa per a implementar contramesures de protecció.
- Combinació de mesures impulsades per IA, amb l'experiència dels tècnics proveïdors del servei.
- Obligatòriament el suport tècnic ofert pel fabricant ha de ser directament des d'Espanya i en castellà i català, serà realitzat per tècnics certificats del propi fabricador.
- Possibilitat de reportar un nombre il·limitat d'incidències i consultes.
- Possibilitat de rebre avisos quan sorgeixin alertes de seguretat de nou malware.
- En cas de detectar-se una infecció massiva, el contractista, prèvia petició de la Diputació de Lleida, designarà un tècnic, bé de forma remota o presencial per a ajudar a les tasques d'eliminació de la infecció.
- L'oferta inclourà el compromís de vida útil del sistema a adquirir per un període mínim de quatre anys des del moment de publicació del present procediment de contractació.
- El manteniment de les llicències inclou el subministrament de les noves versions dels productes, així com les actualitzacions dels mateixos durant el període contractat. Aquestes versions del producte i actualitzacions estaran accessibles a través de la web del fabricant i es podran descarregar de manera manual o automàtica mitjançant les utilitzats d'actualització que inclogui el propi software.
- Accés al suport proporcionat directament pel fabricant de la solució en format 24 x 7, i atesa en castellà, sense límit de consultes durant la vigència contracte.

Lleida, a data de la signatura electrònica.