CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

Plec de Prescripcions Tècniques pel Subministrament, instal·lació i integració de les eines que formaran part del Centre d'Operacions de Ciberseguretat de l'Ajuntament de Sabadell

Ajuntament de Sabadell

Sabadell, juny de 2022

Finançat per la Unió Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Pla de Recuperació, Transformació i Resiliència

Ajuntament de Sabadell

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

1 INTRODUCCIÓ

L'Ajuntament de Sabadell disposa d'una infraestructura informàtica i de telecomunicacions sobre la que es dona servei tant a la organització interna com a la ciutadania, donant compliment als requeriments normatius establerts per les Lleis 39/2015 i 40/2015 i el Reial Decret 203/2021.

Sobre aquesta infraestructura, hi ha implantades diferents solucions tecnològiques per garantir la gestió electrònica integral dels diferents processos i procediments administratius. Avui en dia, s'han implantat eines per, entre altres, possibilitar la relació telemàtica amb els ciutadans, per garantir la interconnexió de dades i documents amb altres administracions, per garantir una gestió basada en el document i l'arxiu electrònic, etc.

Donat el canvi normatiu expressat en aquestes lleis, s'ha generat un augment de la criticitat d'aquests sistemes d'informació, exposant-los a possibles atacs que poden comprometre la disponibilitat, la integritat i la confidencialitat de les dades tractades.

Tot i que l'Ajuntament de Sabadell disposa de diversos sistemes de seguretat implantats actualment per protegir-se d'aquests atacs, es considera necessari evolucionar aquests sistemes a les actuals i futures necessitats.

La normativa actual requereix la disponibilitat dels sistemes en tot moment. Un dels requeriments per garantir-ho és la supervisió constant d'aquestes eines de seguretat. L'ús d'eines integrades entre elles facilita aquesta supervisió.

Davant aquests fets, es considera imprescindible que l'Ajuntament de Sabadell disposi d'un **Centre d'Operacions de Ciberseguretat,** que faciliti un major control sobre la informació i augmentar considerablement la capacitat de respondre a possibles atacs cibernètics, que poden comprometre de forma important els actius municipals.

2 OBJECTE

L'objectiu general del projecte és la contractació d'un conjunt d'eines i serveis per tal de que l'Ajuntament disposi d'un Centre d'Operacions de Seguretat (SOC).

Per tant, a partir de la implantació de les eines necessàries definides en aquests plecs, així com la seva configuració, la integració de les diferents fonts d'informació que recullen informació que pot ser important per a la determinació de problemes de seguretat i la formació en aquestes eines al personal tècnic de l'Ajuntament i alhora la sensibilització de tot el personal de l'Ajuntament en aquests aspectes, aconseguir un major nivell de seguretat de l'Ajuntament i de les persones i col·lectius que s'hi relacionen.

Les funcions de primer nivell del Centre d'Operacions de Ciberseguretat seran exercides per l'Agencia de Ciberseguretat de Catalunya per la qual cosa, cal que les eines objecte del present plec puguin estar en comunicació amb altres Centres d'Operacions de Seguretat,

en concret amb el Centre d'Operacions de Ciberseguretat de la Generalitat de Catalunya, gestionat per l'Agència de Ciberseguretat de Catalunya, amb qui l'Ajuntament està en procés d'adhesió i en la mesura del possible amb el de l'Administració General de l'Estat, dirigit per la Divisió de Planificació i Coordinació de Ciberseguretat, dependent de la Secretaria General d'Administració Digital (SGAD) adscrita al Ministeri de Política Territorial i Funció Pública. Aquestes connexions permetran reportar incidents de seguretat que s'hagin pogut detectar al Centre d'Operacions de Seguretat de l'Ajuntament de Sabadell i alhora rebre aquest mateix tipus d'informació dels centres d'operacions esmentats anteriorment.

També s'utilitzaran les eines proporcionades pel Centro Criptológico Nacional, depenent del CNI.

En concret aquestes eines han de permetre a l'Ajuntament:

- Ajudar a la prevenció i detecció d'incidents de Ciberseguretat i donar-hi resposta, posant en marxa les actuacions de protecció pertinents davant les ciberamenaces i els riscos inherents sobre les infraestructures tecnològiques, els sistemes d'informació, els serveis de les tecnologies de la informació i la comunicació, i la informació que aquests tracten.
- Permetre planificar, gestionar, coordinar i supervisar la Ciberseguretat a l'àmbit de l'Ajuntament i el seu sector públic.
- Ajudar a minimitzar els danys i el temps de recuperació en cas de ciberatac.
- Donar informació per tal de poder investigar i analitzar tecnològicament els ciberincidents i els ciberatacs sobre infraestructures tecnològiques, sistemes d'informació, serveis de tecnologies de la informació i la comunicació de l'Ajuntament i el seu sector públic.
- Recollir i emmagatzemar les dades pertinents de les entitats que gestionen serveis públics o essencials a l'Ajuntament de Sabadell (Smatsa, TUS, Radio Sabadell, Vimusa, PES …) per conèixer l'estat de la seguretat de la informació, informar Alcaldia i proposar les mesures adequades duent a terme la gestió de riscos en matèria de Ciberseguretat,
- Donar suport als responsables de la continuïtat dels serveis i les infraestructures de les tecnologies de la informació i la comunicació de l'Ajuntament de Sabadell i del sector públic.

3 SITUACIÓ ACTUAL

L'Ajuntament de Sabadell disposa de diferents eines informàtiques per garantir el compliment normatiu referent a la seguretat de la informació i dels actius essencials de la organització.

El disseny i la operació d'aquestes eines recau en el Programa de Tecnologia i Sistema del Servei de Tecnologia i Sistemes d'informació de l'Ajuntament de Sabadell.

L'Ajuntament disposa, entre d'altres, de:

- Mcafee Endpoint protection amb la corresponent ePO, fent les funcions de EDR.
- Firewall perimetral Paloalto networks
- Symantec messaging Gateway.

Les eines de seguretat requerides hauran de donar cobertura a:

- Directori Actiu corporatiu de Microsoft
- Microsoft Exchange

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

- Servidors publicats a internet que presten servei a la ciutadania. (Seu electrònica, portal web municipal,...)
- Servidors publicats a internet amb els serveis d'infraestructura. (Correu, DNS,...)
- Servidors crítics de la xarxa corporativa.

L'Ajuntament disposa d'infraestructura de servidors virtuals amb VMWare.

4 ABAST

El contracte inclourà el subministrament, instal·lació i configuració de les eines específiques de seguretat per la posada en marxa del Centre d'Operacions de Ciberseguretat de l'Ajuntament de Sabadell. Ha de contemplar també la integració amb els elements ja existents, sense cost afegit. També inclourà la formació al personal tècnic municipal en la configuració de les eines i la sensibilització del personal municipal en aspectes lligats a ciberseguretat.

Tot aquest projecte es farà de forma coordinada amb el Servei de Tecnologies i Sistemes d'Informació.

4.1 Subministrament de les eines requerides per permetre a l'Ajuntament dotar-se d'un Centre de Ciberseguretat.

L'abast del projecte contempla l'**adquisició de les llicències** d'ús de les diferents eines que composen un Centre d'Operacions de Ciberseguretat i que en aquests moments l'Ajuntament no té. Aquestes eines seran proposades per les empreses licitadores. Es valorarà de forma positiva que aquestes eines estiguin homologades pel *Centro Criptológico Nacional*, i formin part de les incloses a la guia CCN-STIC 105, la qual es pot trobar al següent enllaç (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html).

El subministrador haurà de proporcionar els següents components:

- Una **eina SIEM (Security Information and Event Management)**. Aquesta eina haurà de permetre:
  - Recopilació centralitzada i en temps real de logs i evidències de cadascuna de les aplicacions que composen el Centre d'Operacions.
  - Classificació de logs i evidències per temàtica.
  - Anàlisi ràpid i àgil dels diferents logs i evidències recollits.
- Una **eina Web Application Firewall (WAF)**, que permeti protegir a l'Ajuntament de possibles múltiples atacs als servidors d'aplicacions web de la xarxa interna.

- Una **eina Network Access Control (NAC)**, que permeti controlar i restringir l'accés a la xarxa corporativa interna.
- L'eina **Kaspersky Automated Security Awareness Platform**, per promoure la sensibilització entre els treballadors de l'Ajuntament i la formació en seguretat.

4.1.1 Security Information and Event Management (SIEM)

És objecte del contracte el subministrament de llicències SIEM (*Security Information And Event Management*), eines orientades a recopilar informació en temps real sobre els esdeveniments de seguretat generats per la xarxa d'una organització, per processar-la posteriorment per generar informes i /o alertes que puguin ajudar a l'organització en la presa de decisions en matèria de seguretat.

Les funcions bàsiques de seguretat que ha de proporcionar el SIEM són les següents:

- Gestió de múltiples fonts de dades. Ha de permetre administrar dades d'esdeveniments provinents de diverses fonts com a servidors, bases de dades, aplicacions, etc., així com consolidar aquestes dades i preservar la seva integritat davant de modificacions no autoritzades
- Correlació. Ha de tenir la capacitat de cercar atributs comuns i/o les relacions entre els fitxers de registre d'esdeveniments de totes les fonts fent servir la marca de temps com a eix per correlacionar les dades
- Serveis d'alertes. A partir de l'anàlisi automatitzada d'esdeveniments correlacionats, aquest producte ha de ser capaç de permetre la programació d'alertes per notificar als destinataris problemes o incidències de manera immediata. L'eina ha de permetre l'enviament d'alertes per diversos canals, a una consola específica, a correu electrònic, per SNMP, etc....

Repositori de dades sobre esdeveniments de seguretat. Aquesta eina ha de poder guardar la informació registrada sobre esdeveniments de seguretat dels sistemes que s'hi integren, i servir de gran ajuda a la investigació forense d'incidents de seguretat.

Caldrà que la solució proporcionada sigui escalable.

4.1.1.1 Requeriments generals

El producte ha de ser capaç de rebre, identificar i interpretar esdeveniments procedents de múltiples fonts. Ha de suportar, almenys, els protocols Syslog i SNMP (Simple Network Management Protocol) o connexió al registre d'events de Windows. També cal que sigui suficientment configurable per interpretar i normalitzar informació procedent d'aplicacions o eines propietàries, en particular, ha de permetre la integració amb les eines especificades al punt 3 del present document i amb les eines proposades a la licitació (NAC i WAF)

Per a la funcionalitat d'anàlisi i correlació d'esdeveniments, el producte facilitarà la creació d'alarmes o notificacions en el cas de detectar potencials riscos per a la seguretat.

El producte haurà de ser capaç d'analitzar les dades recollides en funció de regles definides, per identificar usos indeguts o activitats malicioses, registrant el resultat de les anàlisis.

El producte ha de protegir els esdeveniments emmagatzemats d'accessos, modificacions i esborrats no autoritzats, així com prevenir la pèrdua d'esdeveniments per omplir l'espai d'emmagatzematge.

Per a la seva integració a amb l'Agència de Ciberseguretat de Catalunya la solució disposarà d'una API per a la federació tant amb aquesta com amb el CCN, a fi de poder monitoritzar les alertes de seguretat de perillositat Alta, Molt Alta i Crítica, segons la norma CCN-STIC 817 de Gestió d'Incidents.

4.1.1.2 Requeriments de protecció Common Criteria

El producte ha d'estar certificat amb un dels perfils de protecció certificats següents d'acord amb la norma Common Criteria:

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

PERFILS DE PROTECCIÓ

Perfil de protecció	Versió	Data	Organisme responsable
Collaborative Protection Profile for Network Devices	2.2e	27/03/2022	CCDB
Collaborative Protection Profile for Network Devices	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices	2.0 + Errata 20190214	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices	1.0	27/02/2015	CCDB

Perfils de protecció Common Criteria – CCN STIC-140 Annex B.6 pt.4.1

En el cas que el producte no estigui certificat contra cap del perfils anteriors, caldrà acreditar una declaració de seguretat (Security Target) certificada amb un nivell de confiança EAL (Evaluation Assurance Level) EAL2 o superior. La declaració de seguretat ha d'implementar els SFR (Security Functional Requirements) apropiats per satisfer, almenys, els Objectius de Seguretat que es recullen a la taula següent:

Objectiu	**Descripció**
Auditoria: Registre d'esdeveniments I	El producte haurà de guardar un registre d'auditoria per a esdeveniments de seguretat rellevants que passin en el sistema
Auditoria: Registre d'esdeveniments II	Per a cada esdeveniment d'auditoria es registrarà, al menys, la següent informació: data/hora de l'esdeveniment, tipus d'esdeveniment, subjecte identificat (en el cas que correspongui) i el resultat de l'esdeveniment (èxit o fracàs)
Auditoria: Lectura de registres	El producte haurà de de protegir els registres d'auditoria guardats, d'accessos no autoritzats.
Auditoria: Modificació de registres	El producte haurà de de protegir els registres d'auditoria guardats, de modificacions i esborrat no autoritzats.
Auditoria: Prevenció de pèrdua de dades	El producte haurà de disposar de mecanismes apropiats per a prevenir la pèrdua de registres d'auditoria, en el cas de que l'espai d'emmagatzemament dels registres arribi al seu límit.
Auditoria: Transmissió segura de registres	En el cas que el producte tingui la capacitat de transmetre els registres d'auditoria a altres dispositius o serveis externs, haurà d'utilitzar un protocol segur per a la transmissió.

Control d'accés: Identificació i autenticació	El producte ha d'identificar de forma única als usuaris, i autenticar-los abans de donar-li's accés a funcions i dades del producte.
Gestió de la seguretat: funcions	El producte ha de proporcionar un conjunt de funcions de gestió que permetin el control adequat de les seves funcions i dades.
Gestió de la seguretat: permisos	El producte ha de garantir que només els usuaris amb els permisos adequats, puguin exercir el control de les dades i funcions del producte
Segellat de temps	El producte ha de proporcionar una font fiable de temps per als registres d'auditoria.

4.1.1.3 Requeriments de criptografia

El producte no emmagatzemarà cap credencial en clar en memòria no volàtil. El producte ha d'impedir l'accés en clar als paràmetres de seguretat crítics del sistema (claus simètriques i claus privades).

En cas que el producte utilitzi algorismes i funcions criptogràfiques, ha de suportar l'ús d'aquelles acceptades per a nivell Alt de l'ENS segons la guia CCN-STIC-807 amb les longituds de clau requerides, així com proporcionar capacitats de configuració que permetin obligar-ne l'ús d'aquests algorismes exclusivament.

4.1.1.4 Requeriments de confiabilitat

El producte utilitzarà protocols segurs (IPSec, TLS 1.2 o superior, etc.) per a l'establiment de canals de confiança per a l'intercanvi d'informació amb altres entitats TI autoritzades, l'administració remota o els usuaris remots.

4.1.1.5 Requeriments d'integració

L'eina haurà de ser integrable mitjançant API's i/o web services. L'existència d'integracions ja desenvolupades entre l'eina i les eines que empra a hores d'ara l'Ajuntament o la resta d'eines presents a l'oferta (WAF, NAC), seran tingudes en compte de cara a la valoració de les ofertes presentades.

En qualsevol cas, amb el SIEM s'hauran d'integrar la resta d'eines presents a l'oferta (WAF i NAC), així com les eines que empra a hores d'ara l'Ajuntament en matèria de seguretat (punt 3 del present document).

A efectes de volumetria, el SIEM haurà de rebre, registrar i processar events de les següents fonts de dades (17) :

- Mcafee ePO i EPP.
- Firewall perimetral Paloalto networks (clúster actiu-actiu)
- Symantec Messaging Gateway.
- Directori Actiu corporatiu de Microsoft, incloent DNS i DHCP
- Microsoft Exchange
- Servidors publicats a internet que presten servei a la ciutadania. (5 servidors Windows o Linux)
- Servidors crítics de la xarxa corporativa. (5 Servidors Windows o Linux)
- Xarxa de commutació Cisco.
- Controladora Wifi Aruba 7210

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

El proveïdor haurà de certificar que pot integrar les fonts detallades, sigui amb connector preexistent o amb integració a mida, amb una declaració responsable per a cada cas.

Els sistema SIEM haurà de disposar de la capacitat de rebre un mínim de 1250 Events per segon, i processar un mínim de 50GB diaris d'informació.

4.1.2 Web Application Firewall (WAF)

És objecte del contracte el subministrament de les llicències WAF (WEB APPLICATION FIREWALL) o Firewalls d'aplicacions web que analitzin i filtrin el transit adreçat a aplicacions web específiques.

La solució aportada haurà de gestionar el tràfic de 10 llocs web amb els seus corresponents certificats SSL durant un mínim de 24 mesos.

4.1.2.1 Requeriments de seguretat

El producte ha de proporcionar una política de seguretat WAF per governar el trànsit dirigit a les aplicacions i serveis web que protegeix. La política permetrà la configuració de regles per part dels administradors.

En funció de les regles configurades, es poden llençar les accions especificades per l'administrador. Dins de les accions possibles, es podrà alertar i/o bloquejar el trànsit sospitós.

El producte permetrà la creació de llistes blanques (explícitament autoritzades) i negres (explícitament denegades). Aquestes llistes es poden basar en adreces IP, protocol, servei, etc.

El producte s'ha de detectar i protegir davant, almenys, dels tipus d'atacs següents:

Tipus d'atac	Descripció
Atacs DoS i DDoS	Atacs de denegació de servei i denegació de servei distribuïda
Injecció	Consisteix en l'enviament a un intèrpret, de diverses dades malicioses com a part d'una ordre o consulta. El tipus de dades que se solen emprar són SQL, NoSQL, OS i LDAP. L'objectiu és que l'intèrpret executi les ordres no desitjades o proporcioni informació sense l'autorització adequada.
Debilitat d'autenticació	Un atacant s'aprofita de mecanismes d'autenticació i control de sessió febles, en l'aplicació o servei web. D'aquesta manera, pot comprometre credencials o tokens de

	sessió per assumir la identitat d'usuaris legítims, de forma temporal o permanent.
Espai de dades sensibles	Un atacant s'aprofita de mecanismes febles de protecció de dades sensibles (en repòs o en trànsit) en aplicacions i serveis web. D'aquesta manera, un atacant pot robar aquestes dades dèbilment protegides, per a realitzar fraus amb targetes de crèdit, robatori d'identitat o altres.
Entitats externes XML	Un atacant pot emprar entitats externes dins de documents XML, per revelar arxius íntegres, escaneig de ports interns, execució remota de codi i atacs de denegació de servei.
Debilitat de control d'accés	Un atacant s'aprofita de mecanismes de control d'accés febles en l'aplicació o servei web. D'aquesta manera, pot accedir a funcionalitats o dades no autoritzades.
Configuració de seguretat incorrecta	Un atacant s'aprofita d'una configuració de seguretat incompleta o incorrecta en l'aplicació o servei web. No únicament la configuració incorrecta d'opcions, funcions i paràmetres, sinó la falta de pegats de seguretat i actualització regular.
Cross-Site Scripting	Una atacant s'aprofita de febleses en aplicacions o serveis web, que recullen dades no confiables i els envien al navegador web sense una validació prèvia o codificació adequada. D'aquesta manera, un atacant pot executar ordres en el navegador de la víctima, segrestar una sessió, modificar els llocs web o redireccionar l'usuari cap un lloc maliciós.
Deserialització insegura	Un atacant s'aprofita de la feblesa d'algunes aplicacions i serveis web, que accepten objectes serialitzats maliciosos, els quals poden ser manipulats o esborrats per l'atacant, per realitzar atacs de repetició, injecció o escalat de privilegis. En el pitjor dels casos, la dessacralització insegura pot conduir a l'execució remota de codi en el servidor.
Us de components amb vulnerabilitats conegudes	Un atacant s'aprofita de components com llibreries, frameworks, i altres mòduls de software, que s'executen amb els mateixos privilegis que l'aplicació. D'aquesta manera, si algun dels components és vulnerable, l'atacant pot llançar atacs que provoquin pèrdua de dades o la presa de control del servidor.
Insuficient monitorització i logging	Un atacant s'aprofita d'una ineficient monitorització de les aplicacions i serveis web, juntament amb la falta d'un mecanisme de resposta a incidents adequat. D'aquesta manera, l'atacant pot llançar atacs al sistema de forma persistent i mantinguda en el temps, saltar a altres sistemes y manipular, extreure o destruir dades.

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

Altres atacs	Es podran declarar altre tipus d'atacs que siguin mitigats pel producte.

4.1.2.2 Requeriments d'administració

El producte ha de definir, almenys, el rol d'administrador i ser capaç d'associar usuaris a rols. A més, el producte ha de ser capaç de realitzar la gestió de les funcionalitats següents:

- Administració del producte de forma local i/o remota.
- Configuració del temps de terminació de sessió o bloqueig en detectar inactivitat.
- Altres paràmetres d'administració configurables.

  El producte ha d'assegurar que només un usuari amb permisos d'administrador serà capaç de fer les funcions descrites anteriorment.

4.1.2.3 Requeriments d'identificació

El producte haurà d'identificar i autenticar cada usuari abans d'atorgar-hi accés.

El producte haurà d'implementar mecanismes que impedeixin atacs d'autenticació per força bruta, a més de protegir les credencials d'autenticació de lectura i modificació no autoritzada.

El producte haurà de disposar de la capacitat de gestió de les contrasenyes, amb els següents criteris:

- La contrasenya ha de poder configurar-se amb una longitud mínima o igual a 12 caràcters.
- La contrasenya ha de ser capaç de compondre's per lletres minúscules, lletres majúscules, números i caràcters especials [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “* ”, “(“, “]

El producte ha de bloquejar o tancar la sessió d'un usuari després d'un període de temps d'inactivitat determinat.

4.1.2.4 Requeriments d'auditoria

El producte haurà de generar informació d'auditoria al començament i finalització de les funcions d'auditoria i quan es produeixi algun dels esdeveniments següents:

- Login i logout de personal autoritzat.
- Canvi a les credencials d'usuaris.
- Canvis en la configuració del producte.
- Esdeveniments relatius a la funcionalitat del producte.

Els registres d'auditoria contindran almenys la informació següent: data i hora de l'esdeveniment, tipus d'esdeveniment identificat, resultat de l'esdeveniment, usuari que produeix l'esdeveniment (si escau). Als registres d'auditoria se li aplicarà la política d'accés següent:

- Lectura: usuaris autoritzats.
- Modificació: cap usuari.
- Esborrat: administradors.

Si es tracta d'un producte appliance, haurà de ser capaç d'emmagatzemar la informació d'auditoria generada en si mateix o en una entitat externa. A més, aquest ha de ser capaç d'eliminar o sobreescriure registres anteriors d'auditoria quan l'espai d'emmagatzematge estigui ple.

4.1.2.5 Requeriments de canal segur

El TOE haurà d'establir canals segurs (HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, SSHv2, etc.) quan intercanviï informació sensible amb entitats autoritzades, o entre les diferents parts del producte, emprant funcions, algorismes i protocols que hi estiguin d'acord al que estableix la guia CCN-STIC-807 (p.ex.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

4.1.2.6 Requeriments d'instal·lació i actualització confiables

El producte oferirà la possibilitat de consultar la versió actual del firmware/software, iniciar actualitzacions manualment i comprovar si hi ha noves actualitzacions disponibles.

El producte haurà d'oferir mecanismes, d'acord amb la criptografia d'ocupació a l'ENS, a través de hashes o signatura digital per autenticar les actualitzacions de firmware/software abans d'instal·lar-les.

L'actualització del microprogramari/programari només es permet a usuaris amb rol d'administrador.

En cas de tractar-se d'un producte software, aquest haurà d'estar empaquetat de manera que, si s'elimina, no deixi rastre de la instal·lació (excepte per configuracions i fitxers de sortida o auditoria). A més, aquest no descarregarà ni modificarà el seu propi codi binari i únicament utilitzarà les biblioteques de terceres parts declarades pel fabricant.

4.1.2.7 Requeriments de criptografia

El TOE permetrà exclusivament l'ús de funcions, algorismes i protocols criptogràfics que estiguin inclosos entre les autoritzades per a Categoria ALTA de l'ENS, d'acord amb allò establert a la guia CCN-STIC-807.

El producte ha d'impedir l'accés en clar als paràmetres de seguretat crítics del sistema (claus simètriques i claus privades).

En cas de subministrar un servei de generació de bits aleatoris (RBG1) determinats, el producte haurà de:

- Utilitzar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
- Usar una llavor d'almenys una font d'entropia que acumuli entropia de diverses fonts o disposar d'una font d'entropia estudiada, amb un mínim de bits d'entropia almenys igual a la fortalesa més forta de seguretat de les claus i hashes que generarà, segons la ISO/IEC 18031:2011.

En cas de generar claus asimètriques, el producte podrà utilitzar els algorismes següents:

- ECC amb una longitud de clau de 256 o superior.
- FFC amb una longitud de clau de 3072 o superior.
- RSA amb una longitud de clau de 3072 o superior.

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

Per establir claus, el producte podrà utilitzar els algorismes següents:

- Esquemes basats en RSA amb una longitud de clau de 3072 o superior.
- Esquemes basats en FFC amb una longitud de clau de 3072 o superior.
- Esquemes basats en ECC amb una longitud de clau de 256 o superior.
- Esquemes basats en DH grups 15, 19, 20, 21, 28, 29 o 30.

Les funcions resum o HASH que utilitzi el producte han d'utilitzar els algoritmes SHA-22 i SHA-3 de longitud més gran o igual a 256.

Per als serveis de verificació de signatura digital, el producte haurà d'utilitzar un dels algorismes següents:

- Digital Signature Algorithm (DSA) amb una longitud de clau de 3072 bits o superior.
- Elliptic Curve Digital Signature Algorithm (ECDSA) amb una longitud de clau de 256 o superior.
- RSA amb una longitud de clau de 3072 o superior.

El producte implementarà xifratge de dades d'acord amb l'algorisme AES els modes CBC, GCM i longitud de claus 128 bits o superior.

Per als serveis d'autenticació de missatges, el producte podrà utilitzar HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA384, HMAC-SHA512.

El producte ha d'implementar els mètodes d'esborrament de claus següents:

- Per a memòria volàtil, la destrucció podrà ser realitzada utilitzant els mètodes següents:
  - Un patró de sobreescriptura d'una passada utilitzant un patró pseudoaleatori generat pel RBG del producte o algun valor que no contingui cap paràmetre de seguretat crític (PSC).
  - Destrucció de la referència a la clau directament seguida per una crida al "recol·lector d'escombraries" de la memòria.
- Per a memòria no volàtil:
  - Que utilitzi un algorisme de wear-leveling, la destrucció haurà de consistir en algun dels mètodes següents:
    - Una sola passada de sobreescriptura amb un nou valor de clau de la mateixa longitud o un altre valor que no contingui cap PSC.
    - Esborrat de bloc.
  - Que no utilitzi un algorisme wear-leveling, la destrucció s'haurà d'executar per:

- Una o més passades de sobreescriptura que no contingui cap PSC seguit d'una lectura de verificació.
- Esborrat de bloc.

Si la lectura de verificació de les dades sobreescrites falla, el procés haurà de ser repetit de nou fins a assolir un número N (N>1) d'intents en què es retorni un error.

L'eina haurà de ser integrable mitjançant API's i web services. L'existència d'integracions ja desenvolupades entre l'eina i les eines que empra a hores d'ara l'Ajuntament o la resta d'eines presents a l'oferta (SIEM, NAC), seran tingudes en compte de cara a la valoració de les ofertes presentades.

En qualsevol cas, l'eina haurà d'estar plenament integrada amb el SIEM ofert.

4.1.3 Network Acces Control (NAC)

És també objecte del contracte el subministrament d'una eina de Control d'Accés a Xarxa (NAC) mitjançant la qual es pugui controlar que només els usuaris i els equips/dispositius autoritzats tinguin accés als recursos i serveis de xarxa en funció del seu nivell i perfil d'accés.

Haurà de complir amb els següents requisits mínims:

- Ha de proporcionar serveis d'Authentication, Authorization and Accounting (AAA), Bring Your Own Device (BYOD), i accés de convidats, incorporant identitat, estat, informació física/dispositiu i polítiques d'accés a la xarxa.
- El sistema de control d'accés ha de suportar accessos de Remote Authentication Dial-In User Service (RADIUS) o de convidats a través d'un portal de manera concurrent i amb alta disponibilitat.
- Disposar de Certificació Common Criteria
- La solució ha de ser multifabricant
- La solució s'ha de poder implementar en appliances virtuals formant clúster de més de 2 equips per garantir alta disponibilitat en mode actiu/actiu amb failover automàtic. La configuració de la solució s'ha de poder implementar en un únic punt, que la replicarà a la resta del equipament.
- La solució en format virtual ha d'estar disponible a la plataforma VMware ESXi.
- La plataforma haurà d'operar totes les funcionalitats a qualsevol appliance d'un mateix clúster.
- Mètodes de perfilat de dispositius basats en NMAP, WMI, SNMP, SSH, sFLOW, NetFlow, IPFIX, DHCP Fingerprinting, HTTP User-Agent, MAC OUIs, …
- Aquesta informació de perfilat es pot utilitzar a les polítiques d'accés per permetre o denegar l'accés del dispositiu a la xarxa.
- El sistema disposarà de funcionalitats d'autorització del accés en funció de les característiques com pertinença a un grup, tipus de dispositiu mòbil, aplicació utilitzada, localització del dispositiu, estat de salut del equip client, etc...
- Autenticació i autorització d'accés utilitzant Directori actiu de Microsoft, Kerberos, directoris compatibles LDAP, bases de dades SQL, Token Servers, Google G Suite (via SAML o OAuth 2.0), Microsoft Azure Active Directory (via SAML o OAuth 2.0), …
- La solució ha de proporcionar un mètode de control d'accés i perfilat de dispositius sense la necessitat d'autenticació (802.1x o MAC Authentication), ni la instal·lació d'agents.

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

- El sistema ha de tenir inclosos a la plataforma de Gestió Web wizards de configuració i plantilles de polítiques d'accés prestades.
- Compatibilitat amb els estàndards definits per TNC (Trusted Network Connect) amb especial focus pel que fa a l'estàndard 802.1X
- El sistema ha de donar suport a autenticacions mitjançant 802.1X, autenticació MAC i amb portal captiu.
- El sistema ha de donar suport a autenticacions basades en SNMP amb commutadors de xarxa que no suportin protocols RADIUS.
- El sistema ha d'utilitzar protocols estàndard que garanteixin la seva compatibilitat amb diferents dispositius d'accés (switches, routers, firewalls, controladors WLAN, terminadors VPN) de diferents fabricants.
- El sistema ha d'incorporar eines per generar informes, anàlisis i troubleshooting, generar gràfiques i taules. S'ha de poder correlar i organitzar informació d'usuaris, informació d'autenticacions i informació del dispositiu alhora.
- Disponibilitat d'API-REST per estendre el sistema i suportar sistemes de seguretat i de TI de tercers.
- Se suportaran els següents mètodes de enforcement per al control d'accés a la xarxa:
    - VLAN steering via RADIUS IETF attributes and VSAs
    - VLAN steering and port bouncing via SNMP
    - Access control lists – tant estàtiques com dinàmiques i descarregables ACLs.
    - Rols o qualsevol altre atribut vendor-specific RADIUS suportat pel dispositiu de xarxa
- El sistema ha de ser capaç de facilitar autenticació 802.1x PEAP per a usuaris que pertanyin a múltiples directoris actius.
- Suport de serveis AAA de xarxa amb mètodes d'autenticació com:
    - RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
    - EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
    - PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
    - TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
    - EAP-TLS
    - EAP-TEAP (Tunneled EAP)
    - PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5

- Wireless and wired 802.1X and VPN
- OAuth2
- Microsoft NAP and NAC
- Windows machine authentication
- Online Certificate Status Protocol (OCSP)
- SNMP generic MIB, SNMP private MIB
- Common Event Format (CEF), Log Event Extended Format (LEEF)

- Possibilitat de separar els processos d'autenticació i autorització. Cada procés haurà de poder utilitzar bases de dades diferents.
- El sistema implementarà els últims estàndards RFC corresponents als protocols TLS, SNMP, MSCHAPv2, RADIUS amb totes les seves extensions, EAP, etc...
- La solució de NAC ha de poder integrar-se amb equipament Paloalto, McAfee Epo Agent, Aruba WLAN, Cisco Catalyst, SIEMs com RSA. Aquestes integracions no suposaran un cost addicional al sistema de gestió d'usuaris i control d'accés.
- La solució NAC haurà d'incorporar mecanismes per executar un control de salut de los dispositius que es connectin a la xarxa, sigui amb mecanismes basats en agent, sense agent, o utilitzant agents ja instal·lats als clients, com per exemple, McAfee.
- El sistema ha de generar missatges Syslog per a tercers.
- Els missatges syslog podran filtrar-se en funció dels diferents tipus d'events.
- Els missatges syslog es podran enviar simultàniament a diferents servidors, amb filtres independents.
- El sistema ha de suportar missatges syslog en formats: Standard, LEEF, CEF y RFC5424.
- Possibilitat de fer no només control d'accés a la xarxa sinó també aplicacions tant en local com en el núvol:
  - El sistema haurà de poder actuar com a Identity Provider de SAML 2.0
  - El sistema haurà de poder actuar com a Service Provider de SAML 2.0
- El sistema inclourà un portal captiu per a l'autenticació d'usuaris aliens a l'Ajuntament compatible amb les solucions WLAN més habituals dels diferents fabricants de la indústria.
- Aquest portal captiu inclourà funcionalitats avançades d'autoregistre, mitjançant les quals l'usuari aliè a l'Ajuntament podrà generar el seu compte de convidat sense comprometre la seguretat de la xarxa.
- El sistema ha de tenir capacitat per registrar la sessió d'usuari, evitant així que reaparegui el portal de convidats davant d'una suspensió del dispositiu client.
- El portal d'usuaris aliens a l'Ajuntament proporcionarà diversos mètodes per al lliurament de credencials: correu electrònic, SMS, impressió de tiquets.
- El temps d'expiració de les credencials de convidats ha de ser configurable.
- El portal proporcionarà informes d'activitat relativa al trànsit de convidats: número de visites, contingut multimèdia mostrat, número de SMS enviats amb credencials, etc.
- Possibilitat de personalització del portal de convidats:
  - Inclusió de menús que permetin registrar informació relativa al convidat (motiu de la visita, durada de la mateixa, persona a qui visita, etc.)

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

- Generació de portals HTML de diferent mida en funció de la mida i resolució de les pantalles dels dispositius mòbils.
- Possibilitat d'incloure tot tipus de contingut multimèdia al portal: imatges, àudio, vídeo, etc. que variï de forma dinàmica segons patrons establerts.

- El sistema ha de disposar d'un sistema de reporting, integrat, que permeti la generació d'informes programada o sota demanda sobre la xarxa, els usuaris, els dispositius connectats i les autenticacions. Han d'existir informes predeterminats i la possibilitat de definició d'informes personalitzats i filtrats.
- La solució NAC ha de disposar de les següents certificacions de Seguretat:
  - FIPS 140-2
  - Extended Package for Authentication Servers Version 1.
  - Collaborative Protection Profile for Network Devices Version 1.0.
  - Certificat pel CCN a la categoria de control d'accés amb nivell ENS ALT.

L'Ajuntament disposa d'una planta instal·lada de commutadors de xarxa Cisco Catalyst amb models 2960, 3560, 3750, 6509, 9200, 9500... Així mateix, es disposa d'una controladora WLAN Aruba 7210.

S'han de subministrar les llicències de programari amb totes les funcionalitats esmentades que siguin necessàries per implementar la solució NAC en un dels edificis municipals, on es disposa de 9 commutadors de xarxa amb un total de 432 ports cablejats i 7 punts d'accés wifi connectats a la controladora Aruba, amb un total de 500 equips connectats Es busca una solució escalable que permeti estendre's a tota la xarxa municipal.

L'eina haurà de ser integrable amb la resta d'eines de seguretat de l'Ajuntament, especialment amb el SIEM licitat al present plec. L'existència de connectors i/o d'integracions ja desenvolupades que s'ajustin a la infraestructura de l'Ajuntament seran tingudes en compte de cara a la valoració de les ofertes presentades.

4.1.4 Kaspersky Automated Security Awareness Platform – Conscienciació dels usuaris en ciberseguretat.

Per tal de garantir que tota l'organització municipal adquireix el nivell de seguretat òptim, el projecte contempla que el licitador haurà de subministrar una eina d'anàlisi, sensibilització i formació en seguretat per a 700 treballadors municipals. Aquest subministrament anirà acompanyat del servei de 10 píndoles formatives d'entre 5 minuts i 10 minuts adreçades als treballadors de l'Ajuntament per tal de sensibilitzar-los en la importància de l'ús segur de les eines informàtiques de l'Ajuntament, a executar durant un període de 12 mesos. La forma i el contingut d'aquestes píndoles seran tingudes en compte de cara a la valoració de l'oferta presentada i per tant el licitador haurà d'informar quines píndoles proposa desenvolupar, en quin format (vídeos, infografia, animacions, propostes d'activitats ...)

En relació a les activitats de de sensibilització, l'empresa haurà de subministrar les llicències necessàries de l'eina Kaspersky Automated Security Awareness Platform, que serà l'eina utilitzada per l'Ajuntament per tal que els treballadors es vagin entrenant i conscienciant amb pràctiques sobre la seguretat TIC.

L'empresa adjudicatària s'haurà de comprometre a:

- Dissenyar, planificar i documentar les 10 píndoles formatives.
- Proveir el programari de sensibilització Kaspersky Automated Security Awareness Platform i fer la instal.lació i configuració.
- Planificar les tasques de conscienciació associades sobre l'eina.
- Fer el seguiment de l'execució amb el primer grup d'usuaris.
- Formar als usuaris tècnics de l'Ajuntament en l'execució d'aquestes tasques de conscienciació un cop finalitzi el primer pilot, amb altres grups d'usuaris.
- Les llicencies hauran de ser activades per un període de 2 anys.

4.2 Fase d'instal·lació, configuració i integració

El projecte contemplarà, una vegada subministrades les eines, una **fase d'instal·lació de les eines, configuració d'aquestes i integració**, on es duran a terme la instal·lació i la configuració de les diferents eines contractades per part de l'Ajuntament i la integració d'aquestes amb la resta d'eines de seguretat de l'Ajuntament així com a les diferents fonts de dades que puguin subministrar informació clau en els processos de detecció d'atacs o de problemes de seguretat.

La instal·lació es realitzarà a la granja de servidors VMWare Vsphere als CPD de l'Ajuntament.

La instal·lació acabarà amb un ajust fi ("Fine tuning") de les eines instal·lades.

A més de l'anterior, la fase d'instal·lació, configuració i integració, contempla també:

- Donar suport a la instal·lació de **software del *Centro Criptológico Nacional* (CCN)**, en concret **LUCIA** i **microClaudia,** tasca que desenvoluparà al mateix Ajuntament.
- **Pla de proves** associat a la implantació. Per tal de garantir que els diferents components que integren el Centre s'ajusten a l'operativa definida prèviament, l'adjudicatari dissenyarà un Pla de proves complet. L'objectiu estratègic d'aquest pla serà el de constatar que les eines i la seva integració disposa d'un funcionament òptim. L'adjudicatari portarà un control documentat de totes les proves i tasques realitzades sobre els diferents components de la plataforma, que cristal·litzarà en un Informe de Pla de Proves.

4.3 Formació del personal tècnic de l'Ajuntament

Per garantir la correcta operativa de la plataforma, un cop finalitzades les fases anteriors del projecte, s'executarà una darrera fase de **transferència del coneixement**, que servirà per formar al personal responsable de l'Ajuntament.

Serà responsabilitat de l'adjudicatari garantir l'adient transferència del coneixement, sobre el muntatge, configuració i funcionalitat de les eines subministrades, envers l'equip tècnic de l'Ajuntament.

L'objectiu d'aquesta fase és garantir que l'equip tècnic de l'Ajuntament sigui capaç, un cop finalitzat el projecte, no únicament d'entendre el funcionament de les eines subministrades i de la seva interacció, sinó de poder entendre i modificar-ne l'operativitat, garantir un ús normal d'aquestes, dur a terme les tasques de desenvolupament sobre el disseny de la plataforma, etc. El licitador haurà de facilitar un **Pla de Formació**, en el qual s'identifiquin

CODI DE VERIFICACIÓ	321S 5E2E 5H16 5Q0F 119L				
EXPEDIENT NÚM.	TIC/2022/45	DOCUMENT NÚM.	TIC16I00L5	DATA	26-05-2022
ÀREA	Àrea de Desenvolupament Econòmic i Impuls Administratiu				
UNITAT	Tecnologia i Sistemes d'Informació				
ASSUMPTE	Centre d'Operacions de Ciberseguretat				

els cursos necessaris per dur a terme aquest objectiu, identificant-ne el contingut i especificant el número d'hores a executar.

Aquesta fase de transferència inclourà també el lliurament de **manuals sobre les eines subministrades**, tant pel seu ús com pel seu desenvolupament i configuració posterior.

A més del lliurament dels manuals, l'adjudicatari facilitarà a l'Ajuntament tot el material de suport que es faci servir durant els cursos formatius.

Es preveu un formació de 4 hores per eina als 7 integrants del Programa de Sistema i Tecnologia del Servei de Tecnologia i Sistemes d'Informació.

5 TERMINIS

El termini estàndard d'implantació serà de 18 mesos.

En qualsevol cas, el termini ha de contemplar com a mínim les següents fases:

1. Fase de subministrament de les eines: un mes.
2. Instal·lació eines de seguretat, 5 mesos desglossats en:
    a. Fase d'instal·lació bàsica de les eines: un mes
    b. Fase configuració i integració: tres mesos
    c. Fase de formació de l'equip de seguretat: un mes.
3. Fase de conscienciació en ciberseguretat als usuaris: 12 mesos

6 DOCUMENTACIÓ A LLIURAR

En acabar cadascuna de les fases dels treballs d'implantació de l'eina, el contractista haurà de lliurar a l'Ajuntament tota la documentació generada en format electrònic editable (Microsoft Office o LibreOffice) o en qualsevol altre format que sigui adequat.

Tota la documentació dels treballs d'implantació de l'eina es lliurarà en català i es conservarà de manera que garanteixi la transferència de coneixement des del contractista al personal de l'Ajuntament i també en cas de canvi en l'equip d'implantació o de manteniment i suport posterior.

Com a mínim es caldrà presentar la documentació següent:

- S'aportarà l'escandall complet del equipament i de les llicències subministrades
- Pla de treball detallat de les tasques realitzades.

- Actes de les reunions mantingudes en cadascuna de les fases de seguiment del projecte.
- Documentació d'anàlisi i disseny, incloent esquemes de l'arquitectura lògica i física.
- Documentació d'instal·lació, parametrització i configuració.
- Plans de proves realitzades i resultats.
- Manuals tècnics i funcionals de les eines subministrades.
- Manuals relacionats amb la transferència de coneixement
- La documentació corresponent a les 10 píndoles formatives.

Salvador Maza, Raimon
CAP PROGRAMA TECNOLOGIA I SISTEMA
23/06/2022 11:06