

Esped. Zkia: **09/2022**

DONOSTIAKO UDALAREN SARERA SARTZEA KONTROLATZEKO (NAC) SISTEMA HARTZEKO PRESKRIPZIO TEKNIKOEN PLEGUA, SUSPERTZE, ERALDATZE ETA ERRESILENTZIA PLANAREN BARRUAN EUROPAR BATASUNAK NEXT GENERATION EU FUNTSEN BIDEZ FINANTZATUTA	PLIEGO DE PRESCRIPCIONES TECNICAS PARA EL SUMINISTRO DE UN SISTEMA DE CONTROL DE ACCESO A LA RED (NAC) PARA EL AYUNTAMIENTO DE SAN SEBASTIAN, ENMARcado EN EL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILENCIA – FINANCIADO POR LA UNION EUROPEA – NEXT GENERATION EU
<u>1.- XEDEA</u> Kontratu honen xedea da Udalaren sarera sartzea kudeatzeko eta kontrolatzeko NAC (Network Access Control) sistema bat (kable zein wireless sarek osatua) jartzeko behar diren hornidura, instalazioa, konfigurazioa eta abian jartzea. Helburua da sistema bat jartzea, alde batetik, Udalaren sarearekin zer gailu motak konektatu nahi duen ezagutzeko, eta, bestetik, begiratzeko ea gailu horrek Udalaren sarera sartzeko bete behar dituenak betetzen dituen, behin-behinean erremediatze sare batean utzi behar den edo beste zerbait egin behar den. Horretarako, honako hauek erabiliko dira: • Konektatutako gailuak ikusaraztea • Gailuen profila automatiko egitea • Politika granularrak egitea, segurtasun-irizpide mordo baten arabera • Gonbidatuak kudeatzea • Sarea segmentatzeko politikak egitea • Konexioen trazabilitatea • Gailuak erremediatzea	<u>1º.- OBJETO</u> El objeto del presente contrato es el suministro, instalación, configuración y puesta marcha precisos para la implantación de un sistema NAC (Network Access Control) para la gestión y control del acceso a la red corporativa municipal, formada tanto por la red cableada, como la wireless. La finalidad es la puesta en marcha de un sistema que permita identificar el tipo de dispositivo que se quiere conectar a la red del Ayuntamiento y evaluar si cumple con los requisitos definidos para determinar si debe tener acceso a la red local o debe ser ubicado en una red provisional de remedio u otras opciones, mediante: • Visibilización de dispositivos conectados • Perfilado automático de dispositivos • Políticas granulares en función de múltiples criterios de seguridad. • Gestión de invitados • Políticas de segmentación de red • Trazabilidad de las conexiones • Remediación de dispositivos
<u>2.- ABIAPUNTUKO EGOERA</u> I. eranskinean ikus daiteke sarearen osagaiek zer egoera duten orain.	<u>2º.- SITUACIÓN DE PARTIDA</u> En el ANEXO I se describe la situación actual de los componentes de la red.
<u>3.- SOLUZIO TEKNIKOAREN DEFINIZIOA</u> Sarera sartzea kontrolatzeko proposatutako sistemak eginkizun hauek egiteko gauza izan behar du: • Kable nahiz wireless sareari	<u>3º.- DEFINICIÓN SOLUCIÓN TÉCNICA</u> El sistema de control de acceso a la red propuesto debe tener las siguientes funcionalidades: • Visibilizar y categorizar todos los

konektatutako gailu guztiak (gailu klasikoak, iot, etab.) ikusteko moduan jartzea eta kategorizatzea, eta haien mota, marka eta ezaugarri batzuk identifikatzea, barrura sartutako guztiak monitorizatuta eduki ahal izateko.

- Gailuei eta erabiltzaileei sare korporatibora sartzen uztea edo blokeatzea, politika batzuen bidez.
- Sare korporatiboa segmentatzea, segurtasun-politika batzuk erabilita sarera sartzeko kontrolean (NAC), sarean diren gailuak baimendutako ekipoekin bakarrik komunika daitezkeela bermatzeko. Sarearen barruko alboetako mugimenduak blokeatzea.
- Gailuak erremediatzea. NACak kontrolatu egiten du gailuen osasun-egoera (health-check), badaki zer segurtasun-maila duten (partxeak, antibirusak, etab.), eta izan behar duena ez bada, partxeak eguneratu eta antibirusa instalatzeko gauza da, edota baita aplikazio batzuk exekutatzeko eragozteko ere.

3.1 Konponbideak bete behar dituen gutxieneko ezaugarri orokorrak:

3.1.1 Vmware ingurunean modu fisikoan edo birtualean Appliance hedatu behar da, eta beste sare-zunda batzuk ere zabaltzea behar izanez gero, oinarritzko lizentzian sartuta izango dira haiek ere.

3.1.2 Gailuen kontrola agentea instalatuta dela edo gabe egin ahal izango da.

3.1.3 Estandarretan oinarrituta izan behar du, sare-azpiegitura heterogeneoekin elkarrengatzen modua ere emanda, azpiegitura horien osagaien fabrikatzailea edozein dela ere. Zehatzago esanda, gutxienez I. eranskinean zehaztutako gailu guztiak elkarrengatzen modukoa eta bateragarria izan behar du soluzioak.

3.1.4 Kudeaketa guztia kontsola zentralizatu bakar batetik egin behar da:

- Kudeaketa-entzefak grafiko eta intuitiboak izan behar du, eta oso granulatu eta pertsonalizagarria. Era berean, soluzioa administratzeko erabiltzaile bat baino gehiago sortzeko modua ere eman behar du, bakoitza bere profil eta pribilegioekin. Erabiltzaile horiek lokalak edo

dispositibos (dispositibos klásikos, iot etc.) konektados tanto a la red cableada como wireless, identificando su tipo, marca y una serie de características para poder tener monitorizados todos los accesos internos.

- Permitir o bloquear en su caso, el acceso de los dispositivos y usuarios a la red corporativa mediante políticas.
- Segmentar la red corporativa mediante el uso de políticas de seguridad en el NAC, de forma que se garantice que los diferentes dispositivos de red solo pueden comunicarse con los equipos autorizados. Bloquear movimientos laterales dentro de la red.
- Remediación de dispositivos. El NAC controla el estado de salud de los dispositivos, (health-check) conoce el nivel de seguridad que tienen, (parches, antivirus etc) y en el caso de que no sea el correcto, puede actualizarlos los parches, instalar antivirus o incluso impedir que se ejecuten ciertas aplicaciones.

3.1 Características mínimas generales que debe cumplir la solución:

3.1.1 Debe desplegarse “on-premise” de manera física ó virtual Appliance en entorno Vmware, si hiciera falta desplegar sondas de red adicionales, estarán incluidas en la licencia base.

3.1.2 El control de los dispositivos se podrá realizar con o sin agente instalado.

3.1.3 Deberá estar basado en estándares permitiendo la interoperabilidad con infraestructuras de red heterogéneas, independientemente del fabricante de los componentes de estas infraestructuras. En concreto, la solución deberá soportar interacción y ser compatible al menos con todos los dispositivos detallados en el anexo I.

3.1.4 Toda la gestión deberá ser realizada desde una única consola de gestión centralizada:

- La interface de gestión deberá ser gráfica e intuitiva, y muy granular y personalizable. Permitirá además la creación de diferentes usuarios de administración de la solución con diferentes perfiles y privilegios. Estos usuarios podrán ser locales o de Directorio Activo.
- Dicha consola de gestión centralizada

direktorio aktibokoak izan daitezke. • Kudeaketa zentralizatuko kontsola horrek erabilgarritasun handia ere izan behar du, aukera gisa. • Autentifikazio-metodo bat baino gehiago izatea (direktorio aktiboa, LDAP, Kerberos) kudeaketa-kontsolara sartzeko. • Sarbidea mugatzeko modua izatea, IP bidez kudeaketa-kontsolara eta appliance edo makina birtualera sartzeko protokolo eta interfazeetara bideratuta. 3.1.5 CCNk NACtzat homologatuta izan behar du irtenbideak, eta CCN-STIC 105 gidan agertu ere egin behar du. 3.1.6 Irtenbideak reporting-sistema integratua eduki behar du; sareari, erabiltzaileei, gailuei eta autentifikazioei buruzko txosten programatuak eta eskaeraren araberakoak sortzeko. 3.1.7 NAC zerbitzua erortzen bada, sarerako sarbideak ez lirateke blokeatu behar, eta erabiltzaileek eta gailuek sarera sartzeko bidea izan behar lukete, orain den bezala. Proposatutako irtenbidea bandatik kanpo konfiguratu behar da, eta ez du akats-puntua izan behar. 3.1.8 Beste segurtasun funtzionalitate batzuk eransteko modua ere izatea, "plugin"en bidez. Plugin horiek ez diote sarrera kontrolatzeko zerbitzuari eragin behar akatsa izan edo gaizki eginda ere. 3.1.9 Switch ataka berean Voice VLAN eta access VLAN detektatzeko eta kudeatzeko gai izan behar du, eta bakoitza bere aldetik kontrolatzeko ere bai; adibidez, datuen VLAN bakarrik blokeatu edo aldatu eta ahotsarenari ez eragiteko, edo alderantziz. <u>3.2 Irtenbideak ikusmenaren funtzionaltasun aldetik gutxienez izan behar dituen ezaugarriak:</u> 3.2.1 Gutxienez 5.000 IP gailu kudeatzeko gai izan behar du, sare korporatibora denak batera konektatuta egonda gailu horiek denak. 3.2.2 Kategorizatutako gailuen datu-base handia izan behar du. 3.2.3 Aurkitu dituzun aktibo guztien inbentarioa egin behar du, automatiko, eta baita haien ezaugarriena, konexio motarena eta abarrena ere. – Sareko gailuen sailkapena (NAT gailuak, mugikorrak, Desktop Windows,	deberá disponer de alta disponibilidad como opción. • Acceso a la consola de Gestión por diferentes métodos de autenticación (Directorio Activo, LDAP, Kerberos) • Posibilidad de limitar el acceso mediante filtrado por direccionamiento IP a los diferentes protocolos e interfaces de acceso a la consola de Gestión y al appliance o maquina virtual. 3.1.5 La solución debe estar homologada como NAC por el CCN y aparecer en la guía CCN-STIC 105. 3.1.6 La solución debe contar con un sistema de reporting integrado para generar informes programados y bajo demanda sobre la red, usuarios, dispositivos y autenticaciones. 3.1.7 En el caso en el que caiga el servicio de NAC, los accesos a la red no deberían bloquearse, de forma que se pudiera tener acceso a la red por parte de los usuarios o dispositivos, tal y como se realizan actualmente. La solución propuesta ha de configurarse fuera de banda y no tiene que ser punto de fallo. 3.1.8 Posibilidad de añadir funcionalidades adicionales de seguridad a través de "plugins". Estos plugins no afectarán al servicio de control de acceso en caso de fallo o mal funcionamiento. 3.1.9 Debe ser capaz de detectar y gestionar Voice VLAN y access VLAN en el mismo puerto del switch, siendo capaz de controlar independientemente cada una, por ejemplo, bloqueando o cambiando solo la VLAN de Datos sin afectar a la de Voz o al contrario. <u>3.2 Características mínimas que debe cumplir la solución sobre la funcionalidad de Visibilidad:</u> 3.2.1 Debe ser capaz de gestionar al menos 5.000 dispositivos IPs conectados concurrentemente a la red corporativa. 3.2.2 Debe poseer una base de datos amplia de dispositivos categorizados. 3.2.3 Debe proporcionar un inventario automáticamente de todos los activos que haya descubierto así como de sus características, tipo de conexión, etc. – Clasificación de dispositivos en la red (Dispositivos NAT, Móviles, Desktop Windows, Impresoras, Dispositivos Linux/Unix,
--	--

inprimagailuak, Linux/Unix gailuak, Mac gailuak, VoIP gailuak, elektronikako gailuak, etab.). – PC bidez konektatutako kanpoko gailuen sailkapena (Wireless, USB, USB bidezko inprimagailuak, PCMIA, modemak, gailu infragorriak, eskanerrak, DVD/CD irakurgailuak, Bluetooth gailuak) – Makina birtualak sailkatzea. – Gailu korporatiboak eta gonbidatuak sailkatzea. – SNMPri eusten dion edozein gailu identifikatzea. – PCetan eta zerbitzarietan instalatuta diren edo exekutatzen ari diren aplikazioen inbentarioa. – Exekutatzen ari diren zerbitzuen inbentarioa. 3.2.4 Inbentario horretan, gailu bakoitzari buruzko informazio hau jaso behar da: - MAC helbidea - Hostname - IP Address - MAC-Vendor - Gailuaren kategoria, mota eta familia - Health Status - Konexioaren egoera - Username - Gailuaren kokapena: a) Kommutadorearen eta atakaren IPa b) AParen SSIDa eta izena 3.2.5 Baimendu gabeko gailuak (switches, Rogue AP, routerrak, etab.) azkar aurkitzeko gauza izan behar du. 3.2.6 Sarean baimendu gabeko zerbitzuak detektatzeko gai izan behar du; adibidez, baimendutakoak ez diren posta-zerbitzariak, DHCP zerbitzari faltsuak, baimendu gabeko web-zerbitzariak eta abar. Soluzioak administratzaileei alarmak bidaltzeko modua eman behar du, posta elektronikoz, behintzat. 3.2.7 SMB saioen Man-in-the-Middle erasoak hautematea egiaztatzeko garaian. 3.2.8 IP/Mac helbideetako spoofing saiakerak automatikoki hautematea, sarean ordeztu edo	Dispositivos Mac, Dispositivos VoIP, Dispositivos de Electrónica, etc). – Clasificación de dispositivos externos conectados via pc (Wireless , USB, Impresoras vía USB, PCMIA, Módems, Dispositivos infrarrojos, Scanners , Lectores de DVD/CD, Dispositivos Bluetooth) – Clasificación de máquinas virtuales. – Clasificación de dispositivos corporativos e invitados. – Identificación de cualquier dispositivo que soporte SNMP. – Inventario de aplicaciones instaladas/en ejecución en pcs y servidores. – Inventario de servicios en ejecución. 3.2.4 En este inventario se deberá recoger la siguiente información sobre cada dispositivo: - Dirección MAC - Hostname - IP Address - MAC-Vendor - Categoría, tipo y familia de dispositivo - Health Status - Estado de la conexión - Username - Localización del dispositivo: a) IP del switch y puerto b) SSID y nombre del AP 3.2.5 Debe poder descubrir de manera rápida dispositivos no autorizados como switches, Rogue AP, routers etc. 3.2.6 Debe poder detectar servicios no autorizados en la red, tales como servidores de correo distintos a los autorizados, servidores DHCP falsos, servidor Web no autorizado, etc. La solución debe poder enviar alarmas a los distintos administradores al menos a través de correo electrónico. 3.2.7 Detección de ataques Man-in-the-Middle de sesiones SMB durante la autenticación.
---	---

aldi berean gertatuz gero. Erasotzaileari sarera sartzeara automatikoki blokeatzeko gauza ere izan behar du.

3.2.9 Microsoft gailuetan X.509 ziurtagiriak identifikatzeko gai ere izan behar du.

3.2.10 Ekipo batek lehenetsitako pasahitza duen edo usu erabiltzen den pasahitza duen antz emateko gai izan behar du.

3.3 Irtenbideak sarbidea kontrolatzeko funtzionaltasun aldetik gutxienez izan behar dituen ezaugarriak:

3.3.1 Ezaugarri batzuen arabera sarbidea baimentzeko funtzionalitateak izan behar ditu sistemak. Ezaugarri hauek, esate baterako: erabiltzaile talde batekoa izatea, gailu mota, erabiltzaile aplikazioa, gailuaren kokapena, IP helbidea, MAC helbidea, gailuaren osasun-egoera (Health Check), etab. Soluzioak egiaztapen pertsonalizatuak onartu behar ditu Windowseko erregistro, artxibo, zerbitzu eta aplikazioetan. Eta iragazteko aukerak deskribatu ere bai.

3.3.2 Iragazketa horren arabera, ekintza batzuk egiteko modua izango da; konparazio baterako, Vlan jakin bati esleitzea, gonbidatuen Vlanari, sarbidea blokeatzea, ACLak erabiltzea, trafikoa injektatuz kontrolatzea, erabiltzaileak deskonektatzea, PCak itzaltzea, prozesuak eta aplikazioak itxi edo hiltzea, sarera sartzeara blokeatzea, USB gailuak desgaitzea (memoriak, modemak, etab.) eta sistema eragilearen komandoak exekutatzea. Konponbidean erabilgarri dauden ekintzak deskribatzea.

3.3.3 Sistemak protokolo estandarrak erabili behar ditu fabrikatzaile batzuen sarbide-ekipoekin (switchak, routerrak, firewallak, WLAN kontrolatzaileak, etab.) bateragarria dela bermatzeko; I. eranskineko ekipamenduarekin, zehazki.

3.3.4 Protokolo estandar horien bidez (SNMPren bidez, esate baterako) sareko gailuekin elkarreragiteko modua izan behar da; Vlan aldaketak, switcheko atakak desgaitu eta horrelako eragiketak egin ahal izateko.

3.3.5 Honako hauekin bateragarria izan behar du:

- Microsoft Active Directory
- RADIUS

3.2.8 Detección automática de intentos de spoofing de direcciones IP/Mac en caso de suplantación o de simultaneidad en la red. También debe poder bloquear automáticamente el acceso a la red para el atacante.

3.2.9 Debe ser capaz de identificar certificados X.509 en dispositivos Microsoft.

3.2.10 Debe ser capaz de detectar si un equipo tiene una contraseña por defecto o si tiene una password comúnmente utilizada.

3.3 Características mínimas que debe cumplir la solución sobre de la funcionalidad de Control de acceso:

3.3.1 El sistema tendrá funcionalidades de Autorización del acceso en función de características como pertenencia a un grupo de usuarios, tipo de dispositivo, aplicación utilizada, localización del dispositivo, dirección IP, dirección MAC, estado de salud (Health Check) del dispositivo, etc. La solución debe admitir comprobaciones personalizadas en el registro, archivos, servicios y aplicaciones de Windows. Describir las diferentes posibilidades de filtrado.

3.3.2 Según este filtrado, se podrán realizar diferentes acciones como: asignar a una vlan concreta, a la vlan de invitados, bloquear el acceso, uso de ACLs, control mediante inyección de tráfico, deberá permitir desconectar usuarios, apagar PCs, cerrar o matar procesos y aplicaciones, bloquear acceso a la red, deshabilitar dispositivos USB (como memorias, modems, etc) o ejecutar comandos del sistema operativo. Describir las diferentes acciones disponibles en la solución.

3.3.3 El sistema deberá utilizar protocolos estándar que garanticen su compatibilidad con distintos equipos de acceso (switches, routers, firewalls, controladores WLAN, etc) de distintos fabricantes, en concreto con el equipamiento del ANEXO I.

3.3.4 A través de estos protocolos estándar, como el SNMP, se debe poder interactuar con los dispositivos de red para operativas como cambios de Vlans, deshabilitar puertos en switch etc.

3.3.5 Debe ser compatible con:

- Microsoft Active Directory
- RADIUS
- S
- Directo

S o LDAP direktorioak 3.3.6 Ez da derrigorra 802.1x hedatzea, baina harekin integratzeko aukera izan behar du. Soluzioak atakara sartzea kontrolatzeko modua eman behar du, egiaztatze edo autentifikaziorako 802.1x izan beharrik gabe. 3.3.7 Atari gatibu bat izan behar du gonbidatuak sartzeko, eta gonbidatuaren datuak jaso ere egin behar du. Atari gatibuak funtzionalitate aurreratuak ere izan behar ditu sarera sartzeko eskatzekoan izateko. Atariak autentifikazio-faktore bikoitzeko soluzioekin integratzeko modua ere eman behar du. <u>3.4 Irtenbideak sarea zatitu edo segmentatzeko funtzionaltasun aldetik gutxienez izan behar ezaugarriak:</u> Sistemak aukera eman behar du sareen arteko trafiko politika edo arau batzuk definitzeko, gailuak baimendutako sareetara sartzeko eta gainerako sareetara sartzen ez uzteko. Arau horiek ukatzen dituzten sarbide-saiakerak sisteman trazatuta geratu behar dira. TTCP trafikoan, blokeo-funtzionalitate horrek ez lioke sareko elektronikari inola ere eragin behar; firewall birtual bat sortzeko gauza ere izan behar du-eta, TCP trafiko mota guztiak blokeatzeko modukoa, edozein gailutara edo edozein gailutatik datorrela ere trafiko hori. <u>3.5 Irtenbideak erremediatze aldetik gutxienez izan behar dituen ezaugarriak:</u> 3.5.1 Sarera konektatzen diren gailuen osasuna kontrolatzeko mekanismoak izan behar ditu. 3.5.2 Osasun-azterketa Windows eta Linux sistema eragileetan egin ahal izango da. 3.5.3 Sistema eragilearen adabakien, birusen kontrakoen, spywarearen kontrakoen eta abarren egoera eta eguneratzea egiaztatu behar du, eta gailuak politika korporatiboak urratzen baditu, automatiko egin behar ditu horiek konpontzeko egin behar diren ekintzak.	rios LDAP 3.3.6 No será obligatorio despliegue de 802.1x aunque debe tener la posibilidad de integración con el mismo. La solución deberá proporcionar control de acceso a nivel de puerto sin requerir 802.1x para la autenticación. 3.3.7 Deberá disponer para el acceso de invitados de un portal cautivo y recoger datos del invitado. El portal cautivo incluirá funcionalidades avanzadas para solicitar el acceso a la red. El portal permitirá integrarse con soluciones de doble factor de autenticación. <u>3.4 Características mínimas que debe cumplir la solución sobre de la funcionalidad de Segmentación de red:</u> El sistema deberá permitir la definición de políticas o reglas de tráfico entre redes, de forma que los dispositivos solo accedan a las redes permitidas impidiendo el acceso al resto de redes. Los intentos de accesos denegados por estas reglas deben de quedar trazados en el sistema. Esta funcionalidad de bloqueo en el caso del tráfico TCP no debería afectar para nada a la electrónica de red, ya que deberá poder crear un firewall virtual que permita bloquear cualquier tráfico TCP hacia o desde cualquier dispositivo. <u>3.5 Características mínimas que debe cumplir la solución sobre de la funcionalidad de Remediación:</u> 3.5.1 Deberá incorporar mecanismos para realizar el control de salud de los dispositivos que se conecten a la red. 3.5.2 El chequeo de salud deberá permitirse para los sistemas operativos Windows, Linux. 3.5.3 Se comprobará el estado y actualización de parches de sistema operativo, anti-virus, anti-spyware, etc, y en caso de que el dispositivo viole las políticas corporativas, se ejecutarán automáticamente las acciones necesarias para su remediación.
---	---

3.6 Hornitzeaz gainera, irtenbidea ezartzeko eta hedatzeko zerbitzu hauek ere egin behar dira:

- 3.6.1 – Instalatzea, konfiguratzea eta martxan jartzea, in situ.
- 3.6.2 – Sarera konektatutako gailuak identifikatzea eta kategorizatzea, in situ.
- 3.6.3 - Vlan-etan gailuak berrantolatzea eta segmentatzea.
- 3.6.4 – Atari gatibu bat sortzea.
- 3.6.5 – Sarera sartzeko oinarriko politikak definitzea, wifi sarean eta kable sarean.

Soluzioaren ezarpena eta konfigurazioa bat etorri beharko da eskainitako NACari lotutako konfigurazio seguruko CCN-STIC gidarekin (halakorik balego) eta lotutako guztiekin.

3.7 Eskainitako arkitekturaren eta egin beharreko zerbitzuen betekizunak

3.7.1 Irtenbideak bateragarria izan behar du I. eranskinean zehaztutako sare eta datu azpiegiturarekin eta egungo ingurunearekin. Eskainitako konponbideak bateraezintasunen bat badu orain den azpiegiturako elementuren batekin, enpresa esleipendunak ekarri beharko ditu bateraezintasun hori konpontzeko izan behar diren elementuak.

3.7.2 Irtenbideak ez du aldaketarik eginarazi behar ez instalatuta dauden aplikazioetan, ez eta haiek orain daukaten konfigurazioan ere.

3.7.3 Den-denak I. eranskinean eta agiri honetan adierazitako gainerako elementuetan zehaztutako sistemekin plataforma anitzean lan egiteko moduan ziurtatuta izan behar du.

3.7.4 Konponbidea ezartzeko eta hedatzeko lanek ez dute eraginik izango udal-sare korporatiboaren funtzionamendu normalean.

3.7.5 Kontratua indarrean den bitartean lantaldearen osaeran aldaketarik txikiena egiteak ere ez dauka Kaudimen Teknikoan aurkeztutako egiaztapena aldatzerik. Hori baino lehen, jakinarazi egin behar zaio DonostiaTIKi eta berariaz onartu behar du hark.

3.7.6 Eskainitako funtzionalitate eta/edo utilitate guztietan erabilera-lizentzia ere

3.6 Además del suministro, hay que realizar los siguientes servicios para la implantación de la solución y su despliegue:

- 3.6.1 – Instalación, configuración y puesta en marcha, in situ.
- 3.6.2 – Identificación y categorización de los dispositivos conectados a la red, in situ.
- 3.6.3 - Reorganización y segmentación de dispositivos en las diferentes Vlan's.
- 3.6.4 – Creación de un portal cautivo.
- 3.6.5 – Definición de políticas básicas de acceso a la red, tanto en red wifi como red cableada.

La implantación y configuración de la solución deberá ser acorde a la Guía CCN-STIC de configuración segura asociada al NAC ofertado si existiera y a todas aquellas relacionadas.

3.7 Requisitos de la arquitectura ofertada y los servicios a realizar

3.7.1 La solución debe ser compatible con la infraestructura de red y datos municipal y el entorno actual detallado en el anexo I. En caso de que la solución ofertada tenga alguna incompatibilidad con algún elemento de la infraestructura actual, la empresa adjudicataria suministrara los elementos necesarios para subsanar dicha incompatibilidad.

3.7.2 La solución no debe implicar el cambio de ninguna de las aplicaciones existentes ni de su configuración actual.

3.7.3 Todo deberá estar certificado para su funcionamiento multiplataforma bajo los sistemas especificados en el anexo I y el resto de elementos detallados en este pliego.

3.7.4 Los trabajos de implantación y despliegue de la solución no afectarán al funcionamiento normal de la red corporativa municipal.

3.7.5 Cualquier cambio en la composición del grupo de trabajo durante la vigencia del contrato no podrá variar la acreditación aportada en la Solvencia Técnica, debiendo notificarse previamente a DonostiaTIK y contar con su autorización expresa.

3.7.6 Para todas aquellas funcionalidades y/o utilidades ofertadas se entiende que la

sartuta dagoela jotzen da.	<u>licencia de uso está incluida.</u>
<u>4. SALMENTA OSTEO GORABEHREI ERANTZUTOKO BETEBEHARRAK</u> Softwarea eta hardwarea egin duen enpresak urtebeteko bermea eman behar du haientzat, eta han sartuta izan behar du: -Hornitutakoa appliance bada, pieza eta hardware originalez hornitzea, matxura edo beste zerbait izanez gero; NBDS (Next business day shipping) erantzuteko epean. -Softwarearekin lotutako akats arazo guztietan laguntza bermatzea. -Softwarearen azkeneko eginkizun eta eguneratzeetarako sarbidea ematea.	<u>4º.- OBLIGACIONES DE ATENCIÓN A INCIDENCIAS POST-VENTA DEL FABRICANTE</u> La empresa fabricante del software y hardware, debe ofrecer garantía de los mismos durante 1 año en el que: -En caso de que el suministro sea appliance, suministrar piezas y hardware, siempre originales, por avería u otros, con tiempo de respuesta NBDS (Next business day shipping) -Deberá garantizar la asistencia a todos los problemas de defecto relacionados con el software. -Deberá proveer acceso a las últimas funciones y actualizaciones de software.
<u>4. SALMENTA OSTEO GORABEHREI ERANTZUTOKO BETEBEHARRAK</u> 5.1 Enpresa esleipendunak lizentziak erregistratzeko izapidea egin beharko du enpresa fabrikatzaileak behar duen kontratatutako aldirako. 5.2 Fabrikatzailearen berme-aldian (urtebete), fabrikatzailearekin lehen eta bigarren mailako gorabeherak konpontzeko elkarriketa-zerbitzua eman beharko die DonostiaTIKeko teknikariei. Gai hauei buruz: • Aldi horretan izan daitezkeen gorabeherak aztertzea eta kudeatzea. • Kontratutako produktuari buruzko kontsultak • Bertsioaren eguneratze kritikoak • Irtenbidearen egoerari buruzko berrikuspenak eta txostenak, hiru hilean behin • Gutxienez 8x5-eko arreta (8 ordu asteleheneetik ostiralera) euskarri zerbitzu horietarako. • Gorabeherak eta matxura-abisuak jasotzeko eta konpontzeko eragiketa prozedura bat. Gorabeherak telefonoz eta on line jakinarazi ahal izateko modua izan dadin.	<u>5º.- OBLIGACIONES DE ATENCIÓN A INCIDENCIAS POST-VENTA DE LA EMPRESA ADJUDICATARIA</u> 5.1 La empresa adjudicataria tendrá que realizar el trámite de registro de las licencias para el periodo contratado que requiera la empresa fabricante. 5.2 Durante el periodo de garantía de fabricante, 1 año, deberá dar el servicio de interlocución con el fabricante para la resolución de incidencias de primer y segundo nivel para los técnicos de DonostiaTIK sobre: • Análisis y gestión de las incidencias que se puedan producir durante este periodo. • Consultas sobre el producto contratado • Actualizaciones críticas de versión • Revisiones e informes trimestrales del estado de la solución • Una atención como mínimo de 8x5 (8 horas de lunes a viernes) para estos servicios de soporte. • Un procedimiento operativo para recibir y resolver las incidencias y avisos de avería. De forma que haya posibilidad de notificar las incidencias vía telefónica y on line.
<u>6.- Proiektuaren hasierako dokumentazioa</u>	<u>6º.- Documentación al inicio del proyecto</u>

Dokumentazioa formatu digitalean aurkeztu behar da proiektuaren hasieran, eta hauek izan behar ditu: i. 6.1 Agiri honetan deskribatutako betekizun bakoitzari buruzko xehetasunak, han agertzen diren hurrenkera berean, eta argi eta garbi adierazita eskainitako irtenbideak 3. eta 5. blokeko betekizun horiek guztiak nola betetzen dituen. ii. 6.2 Ezarpen-plana aurkeztea, 3.6 atalean eskatutako zerbitzuei erantzungo dieten ekintzak zehaztuta, bai eta lanaldiak, ordu kopurua eta esleitutako pertsonak ere. Eta baita proiektuaren kronograma orokorra ere. iii. 6.3 Agirietan eskatutako beharrezko gainerako dokumentazioa.	La documentación, que se presentará en formato digital al inicio del proyecto, deberá incluir: i. 6.1 Detalle de cada uno de los requerimientos descritos en este pliego, explicitando en el mismo orden en el que <u>aparecen y detallando claramente como cumple la solución ofertada</u>, en todos los puntos de los bloques: 3 y 5. ii. 6.2 Se deberá aportar el plan de implantación detallando las acciones a realizar que den respuesta a los servicios solicitados en el apartado 3.6, incluyendo también las jornadas, número de horas total y personas asignadas. Así como el cronograma global del proyecto. iii. 6.3 El resto de documentación necesaria exigida en los pliegos.
<u>7.- Proiektuaren amaierako dokumentazioa</u> Irtenbidea martxan jarri ondoren, kontratatutako hornidura mantentzeko eta ondoren kudeatzeko beharrezko dokumentazioa eman beharko du esleipendunak, formatu elektronikoan; horretako dokumentuak honakoak izango dira gutxienez: 7.1 Proiektua azkenean <u>bezeroaren azpiegiturara egokituta ezarrita</u> geratu den moduari buruzko <u>dokumentazioa eta eskema grafikoak</u>. 7.2 Lehiaketa honen bidez hornitu diren hardware eta software produktu guztiei buruzko <u>dokumentuak eta fabrikatzailearen gidaliburuak</u>. 7.3 Soluzioaren <u>instalazio eta konfiguraziorako eskuliburuak</u>. 7.4 Hornitutako <u>hardware eta software produktuen zerrenda</u>, hala dagokionean horien serie zenbakiarekin, berme eta mantentze lanen iraupenarekin eta beharrezko lizentzien ziurtagiriek batera.	<u>7º.- Documentación final de proyecto</u> Tras la puesta en funcionamiento de la solución, el adjudicatario deberá aportar la documentación necesaria para el mantenimiento y posterior gestión del suministro contratado en formato electrónico, debiendo contener cuando menos los siguientes documentos: 7.1 Se deberá entregar la <u>documentación y esquemas gráficos</u> detallados de la implantación final del proyecto, <u>adaptada a la infraestructura del cliente</u>. 7.2 <u>Documentos y guías de fabricante</u> de todos los productos hardware y software suministrados como parte del presente concurso. 7.3 <u>Manual de instalación y configuración</u> de la solución. 7.4 <u>Listado productos</u> suministrados y cuando proceda con el nº de serie, duración de las garantías y mantenimientos y certificados con las licencias correspondientes.
<u>8.- Prestakuntza</u> Kontratuaren xede diren lanak gauzatu bitartean, esleipendunak konpromisoa hartzen du DonostiaTIKek horretarako izendatutako pertsonari eskatzen duten informazioa eta dokumentazioa guztia emateko, une oro. Horrela, pertsona horiek lanen nondik norakoan ezagutza tekniko osoa izango dute, eta ezagutuko dituzte, halaber, ezarpenaren ondorioz aldian behin sor daitezkeen arazoak,	<u>8º.- Formación</u> Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por DonostiaTIK a tales efectos, toda la información y documentación que éstas soliciten para disponer de un pleno conocimiento técnico de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse



baita horiek konpontzeko erabili beharreko tresnak, metodoak eta teknologiak ere. Bestalde, enpresa adjudikaziodunak ezagutzak helarazi beharko dizkie Dko langileei instalatutako plataforma osatzen duten elementu guztien konfigurazioari, kudeaketari eta mantentzeari buruz.	como consecuencia de la implantación y de las tecnologías, métodos y herramientas utilizadas para resolverlos. Por otra parte la empresa adjudicataria deberá transferir conocimientos al personal de DonostiaTIK sobre la configuración, gestión y mantenimiento de todos los elementos que formen la plataforma instalada.
I ERANSKINA - Hala eskatzen duten enpresen eskura egongo da I. eranskina. Eskuratu ahal izateko, eskatzailearen datuak erregistratu egin behar dira aurrena, nahitaez izan behar den isilpekotasuna izatea ziurtatzeko. Horretarako zerbitzuarekin harremanetan jarri beharko dira lizitatzailleak: donostiatik_administrazioa@donostia.eus Telefonoa: 943481824 Kontratazio-organoak I. Eranskineko informazioa eskuratzeko aukera ukatu ahal izango die enpresei, baldin eta, haien tipologia dela-eta, lizitazioan parte hartzeko interes legitimorik ez badute. Horretarako, interesa egiaztatzeke eskatu ahal izango du, interes hori justifikatzen duen dokumentazioa aurkeztuz.	ANEXO I - El Anexo I se encuentra a disposición de las empresas que así lo soliciten previo registro de los datos del solicitante a efectos de acreditar la confidencialidad requerida. Para ello tendrán que ponerse en contacto a través de: donostiatik_administrazioa@donostia.eus Teléfono: 943481824 El órgano de contratación podrá denegar el acceso a la información contenida en el Anexo I a empresas que por su tipología no tengan interés legítimo en participar en la licitación. A estos efectos, podrá solicitar que se acredite su interés mediante la aportación de la documentación que se estime que justifica dicho interés.

Sinaduraren datan/ En la fecha de la firma

Sistema eta Ustiapen Zerbitzuaren burua/ La Jefe del Servicio de Sistemas y Explotación

Lourdes Apeztegia Alzola

DonostiaTIKeko Kudeatzailea/ El Gerente de DonostiaTIK

Eduardo Fernández Rodríguez



Financiado por la Unión Europea

NextGenerationEU / Documento firmado digitalmente :
Lourdes Apeztegia Alzola (25/09/2022 13:42 CEST), Eduardo Fernandez Rodriguez (23/09/2022 13:42 CEST)Egiaztatzeko / Verificación : <https://www.donostia.eus/scve>
Eskara kodea / Código de petición : 8a10c104-bd5e-4ac5-8f32-325a893ccc44MINISTERIO
DE POLÍTICA TERRITORIAL
Y URBANISMOESPAÑA
PUEDEBerreskuratze,
Eraldaketa eta
Erresilientzia Plana